Configuración de certificados de servidor

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Configuración de certificados de servidor

Puede personalizar los certificados de servidor que utiliza el sistema StorageGRID.

El sistema StorageGRID utiliza certificados de seguridad para varios fines distintos:

- Certificados del servidor de la interfaz de gestión: Se utiliza para proteger el acceso al administrador de grid, al administrador de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos.
- Certificados de servidor de API de almacenamiento: Se utiliza para proteger el acceso a los nodos de almacenamiento y puerta de enlace, que las aplicaciones cliente API utilizan para cargar y descargar datos de objetos.

Puede utilizar los certificados predeterminados creados durante la instalación, o puede reemplazar, o ambos, estos tipos predeterminados de certificados por sus propios certificados personalizados.

Tipos admitidos de certificado de servidor personalizado

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

Para obtener más información sobre cómo protege StorageGRID las conexiones de cliente para la API REST, consulte las guías de implementación de S3 o Swift.

Certificados para extremos de equilibrador de carga

StorageGRID gestiona los certificados utilizados para los extremos del equilibrador de carga por separado. Para configurar certificados de equilibrador de carga, consulte las instrucciones para configurar los extremos de equilibrador de carga.

Información relacionada

"Use S3"

"Use Swift"

"Configuración de los extremos del equilibrador de carga"

Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos

Puede reemplazar el certificado de servidor StorageGRID predeterminado por un único certificado de servidor personalizado que permite a los usuarios acceder al Administrador de grid y al Administrador de inquilinos sin tener que encontrar advertencias de seguridad.

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 un solo certificado de servidor personalizado común y una clave privada correspondiente.

Dado que se utiliza un único certificado de servidor 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 CA raíz en el explorador Web que utilizarán para acceder a Grid Manager y al Gestor de inquilinos.

> Para garantizar que las operaciones no se interrumpen con un certificado de servidor fallido, la alarma **caducidad del certificado de servidor para la interfaz de administración** y la alarma de caducidad del certificado de interfaz de administración heredada (MCEP) se activan cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver el número de días hasta que caduque el certificado de servicio actual seleccionando **Soporte** > **Herramientas** > **Topología de cuadrícula**. A continuación, seleccione ***primary Admin Node*** > **CMN** > **Resources**.

> 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 del servidor de la interfaz de gestión personalizada caduca.
> - Se revierte de un certificado del servidor de interfaz de gestión personalizado al certificado de servidor predeterminado.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Certificado de servidor de la interfaz de administración, haga clic en **instalar certificado personalizado**.
3. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (`.crt`).
   - **Clave privada del certificado del servidor**: 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 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.
4. Haga clic en **Guardar**.

   Los certificados de servidor personalizados se utilizan para todas las conexiones de cliente nuevas posteriores.

   Seleccione una pestaña para mostrar información detallada sobre el certificado de servidor StorageGRID predeterminado o un certificado firmado de CA que se cargó.

Después de cargar un nuevo certificado, permita que se borren todas las alertas de caducidad de certificados (o alarmas heredadas) relacionadas.

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

Restauración de los certificados de servidor predeterminados para el administrador de grid y el administrador de inquilinos

Puede volver a utilizar los certificados de servidor predeterminados para el administrador de grid y el administrador de inquilinos.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Administrar certificado de servidor de interfaz, haga clic en **utilizar certificados predeterminados**.
3. Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

   Al restaurar los certificados de servidor predeterminados, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. Los certificados de servidor predeterminados se utilizan para todas las conexiones de cliente nuevas posteriores.

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

Configuración de un certificado de servidor personalizado para las conexiones al nodo de almacenamiento o al servicio CLB

Es posible reemplazar el certificado de servidor que se utiliza para las conexiones de clientes S3 o Swift al nodo de almacenamiento o al servicio CLB (obsoleto) en Gateway Node. 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 los usuarios también deban instalar el certificado de CA raíz en el cliente API S3 o Swift que utilizarán para acceder al sistema, según la entidad de certificación (CA) raíz que use.

Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alarma **caducidad del certificado de servidor para los extremos de la API de almacenamiento** y la alarma de caducidad del certificado de los extremos del servicio de la API de almacenamiento (SCEP) se activan cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver el número de días hasta que caduque el certificado de servicio actual seleccionando **Soporte** > **Herramientas** > **Topología de cuadrícula**. A continuación, seleccione ***primary Admin Node*** > **CMN** > **Resources**.

Los certificados personalizados solo se utilizan si los clientes se conectan a StorageGRID mediante el servicio CLB obsoleto en los nodos de puerta de enlace o si se conectan directamente a los nodos de almacenamiento. Los clientes S3 o Swift que se conectan a StorageGRID mediante el servicio Load Balancer en los nodos de administración o de puerta de enlace usan el certificado configurado para el extremo de balanceo de carga.

La alerta **caducidad del certificado de punto final de equilibrador de carga** se activa para los extremos de equilibrador de carga que caducarán pronto.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Object Storage API Service Endpoints Server Certificate, haga clic en **instalar certificado personalizado**.
3. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (`.crt`).
   - **Clave privada del certificado del servidor**: 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 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.
4. Haga clic en **Guardar**.

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

   Seleccione una pestaña para mostrar información detallada sobre el certificado de servidor StorageGRID predeterminado o un certificado firmado de CA que se cargó.

   Después de cargar un nuevo certificado, permita que se borren todas las alertas de caducidad de certificados (o alarmas heredadas) relacionadas.

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

Información relacionada

"Use S3"

"Use Swift"

"Configurar nombres de dominio de extremo de API de S3"

Restaurar los certificados de servidor predeterminados para los extremos de la API DE REST de S3 y Swift

Puede revertir a usar los certificados de servidor predeterminados para los extremos de la API DE REST de S3 y Swift.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Object Storage API Service Endpoints Server Certificate, haga clic en **utilizar certificados predeterminados**.
3. Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

   Cuando se restauran los certificados de servidor predeterminados para los extremos de API de almacenamiento de objetos, se eliminan los archivos de certificado de servidor personalizados que se configuraron y no se pueden recuperar desde el sistema. Los certificados de servidor predeterminados se utilizan para todas las conexiones de clientes API nuevas posteriores.

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

Copia del certificado de CA del sistema StorageGRID

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

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

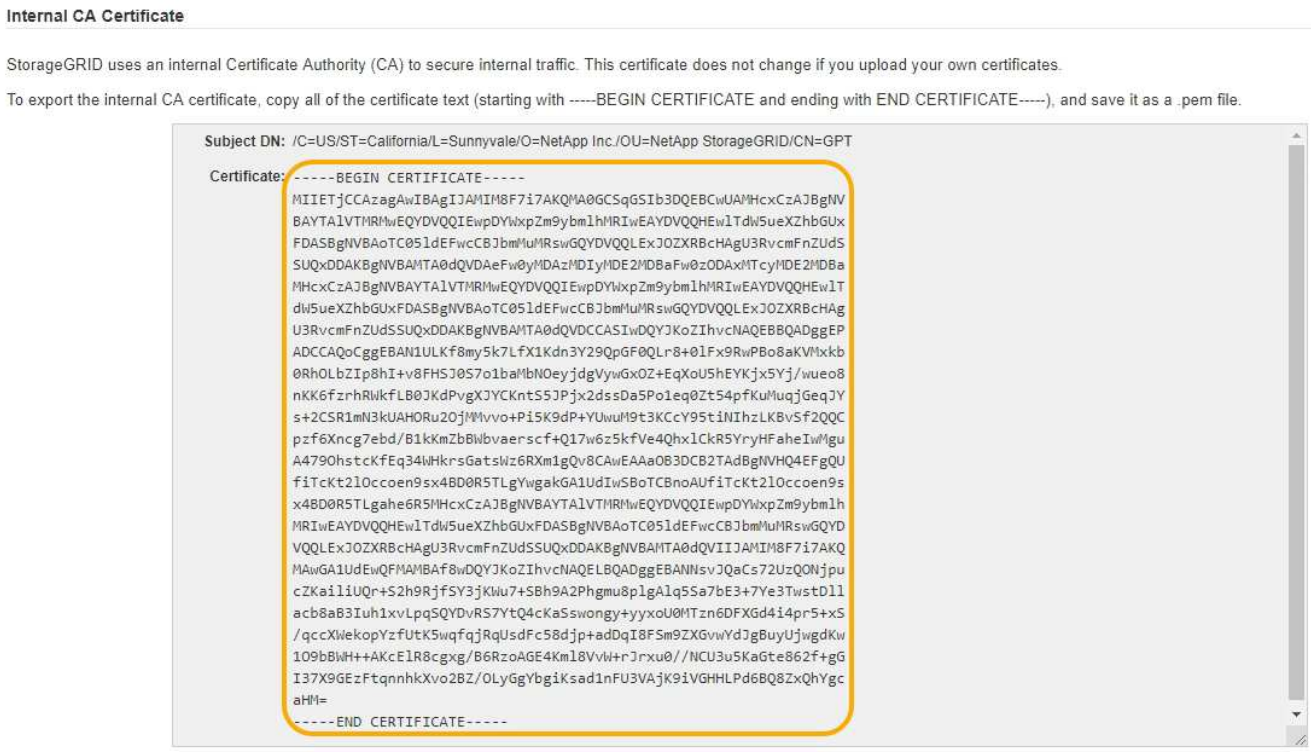
Acerca de esta tarea

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** > **Configuración de red** > **certificados de servidor**.
2. En la sección **Certificado CA interno**, seleccione todo el texto del certificado.

   Debe incluir `-----BEGIN CERTIFICATE-----` y.. `-----END CERTIFICATE-----` en su selección.



3. Haga clic con el botón derecho del ratón en el texto seleccionado y seleccione **Copiar**.
4. Pegue el certificado copiado en un editor de texto.
5. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

En el caso de clientes S3 que realizan una validación de nombre de host estricta y no admiten la deshabilitación de la validación estricta de nombre de host, como clientes ONTAP que utilizan FabricPool, puede generar o cargar un certificado de servidor al configurar el extremo del equilibrador de carga.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Acerca de esta tarea

Al crear un extremo de equilibrador de carga, 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 y procedimientos más detallados, consulte las instrucciones de configuración de StorageGRID para FabricPool.

El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y ya no se recomienda su uso con 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 equilibrador de carga HTTPS, se le solicita que cargue el certificado de servidor, la clave privada de certificado y el paquete de CA.

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.

Información relacionada

"Configure StorageGRID para FabricPool"

Generar un certificado de servidor autofirmado para la interfaz de gestión

Puede usar un script para generar un certificado de servidor autofirmado para los clientes API de gestión que requieren una validación de nombre de host estricta.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

En los entornos de producción, debe utilizar un certificado firmado por una entidad de certificación (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".

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 utilizado por 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 API 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 365
     ```

     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** > **certificados de servidor** > **Certificado de servidor de interfaz de administración**.
7. Configure el cliente de API de gestión para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.