# Administre StorageGRID

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-116/admin/index.html on April 10, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos


Administre StorageGRID . . . 1
- Administrar StorageGRID: Descripción general . . . 1
- Empiece a usar StorageGRID . . . 1
- Control del acceso a StorageGRID . . . 30
- Administrar la configuración de seguridad . . . 78
- Gestione inquilinos . . . 144
- Configure las conexiones de clientes S3 y Swift . . . 165
- Administrar redes y conexiones . . . 200
- Utilice AutoSupport . . . 220
- Gestione nodos de almacenamiento . . . 233
- Gestione los nodos de administrador . . . 257
- Gestione los nodos de archivado . . . 280
- Migrar datos a StorageGRID . . . 303

# Administre StorageGRID

## Administrar StorageGRID: Descripción general

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

### Acerca de estas instrucciones

Estas instrucciones describen cómo usar Grid Manager para configurar grupos y usuarios, crear cuentas de inquilino para permitir que las aplicaciones de cliente S3 y Swift almacenen y recuperen objetos, configurar y gestionar redes StorageGRID, configurar AutoSupport, gestionar los ajustes de nodo, etc.

Estas instrucciones están dirigidas al personal técnico que configurará, administre y prestará soporte técnico para un sistema StorageGRID después de que se haya instalado.

### Antes de empezar

- Tiene una visión general del sistema StorageGRID.
- Tiene un conocimiento muy detallado de los shell de comandos de Linux, las conexiones de red y la instalación y configuración del hardware de servidor.

# Empiece a usar StorageGRID

### Requisitos del navegador web

Debe utilizar un navegador web compatible.

| Navegador Web | Versión mínima admitida |
|---|---|
| Google Chrome | 96 |
| Microsoft Edge | 96 |
| Mozilla Firefox | 94 |

Debe establecer la ventana del navegador en un ancho recomendado.

| Ancho del navegador | Píxeles |
|---|---|
| Mínimo | 1024 |
| Óptimo | 1280 |

### Inicie sesión en Grid Manager

Para acceder a la página de inicio de sesión de Grid Manager, introduzca el nombre de dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de

direcciones de un explorador web compatible.

**Lo que necesitará**

- Tiene sus credenciales de inicio de sesión.
- Tiene la dirección URL de Grid Manager.
- Está utilizando un navegador web compatible.
- Las cookies están habilitadas en su navegador web.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

Cada sistema StorageGRID incluye un nodo de administrador primario y cualquier número de nodos de administrador que no son primarios. Puede iniciar sesión en Grid Manager en cualquier nodo de administrador para gestionar el sistema StorageGRID. Sin embargo, los nodos del administrador no son exactamente los mismos:

- Las confirmaciones de alarma (sistema heredado) realizadas en un nodo de administración no se copian en otros nodos de administración. Por este motivo, es posible que la información mostrada para las alarmas no tenga el mismo aspecto en cada nodo de administración.
- Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Si se incluyen nodos de administración en un grupo de alta disponibilidad (ha), puede conectarse mediante la dirección IP virtual del grupo de alta disponibilidad o un nombre de dominio completo que asigne la dirección IP virtual. El nodo de administración principal se debe seleccionar como la interfaz principal del grupo, de modo que al acceder a Grid Manager, se tiene acceso en el nodo de administración principal a menos que el nodo de administración principal no esté disponible.

**Pasos**

1. Inicie un explorador web compatible.
2. En la barra de direcciones del navegador, introduzca la dirección URL de Grid Manager:

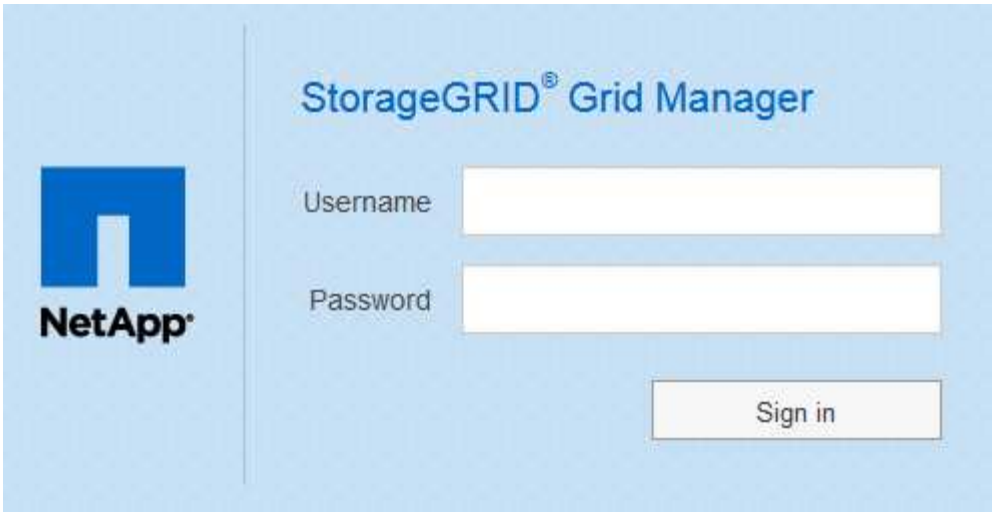
   `https://FQDN_or_Admin_Node_IP/`

   donde *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o la dirección IP de un nodo de administrador o la dirección IP virtual de un grupo ha de nodos de administrador.

   Si debe acceder a Grid Manager en un puerto distinto del puerto estándar para HTTPS (443), introduzca lo siguiente, donde *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o una dirección IP y el puerto es el número de puerto:

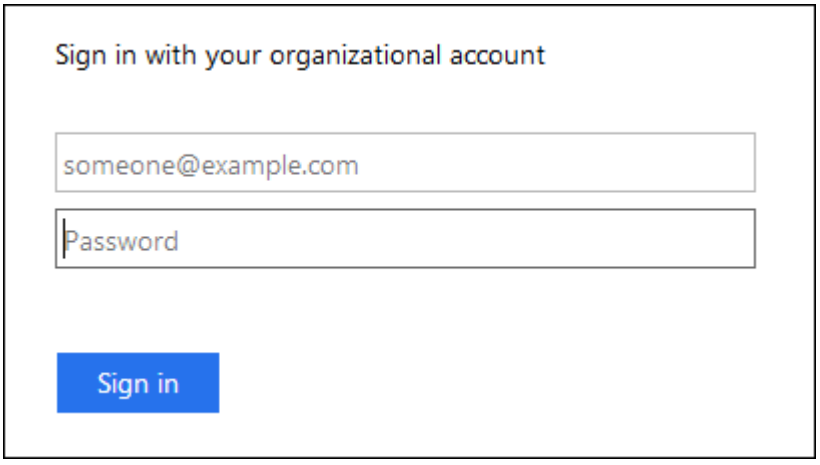
   `https://FQDN_or_Admin_Node_IP:port/`

3. Si se le solicita una alerta de seguridad, instale el certificado mediante el asistente de instalación del explorador (consulte Acerca de los certificados de seguridad).
4. Inicie sesión en Grid Manager:
   - Si su sistema StorageGRID no utiliza el inicio de sesión único (SSO):
     i. Introduzca su nombre de usuario y contraseña para el administrador de grid.
     ii. Seleccione **Iniciar sesión**.




- Si SSO está habilitado para el sistema StorageGRID y esta es la primera vez que accede a la URL en este navegador:
  i. Seleccione **Iniciar sesión**. Puede dejar el campo ID de cuenta en blanco.

  ii. Introduzca sus credenciales de SSO estándar en la página de inicio de sesión con SSO de su organización. Por ejemplo:

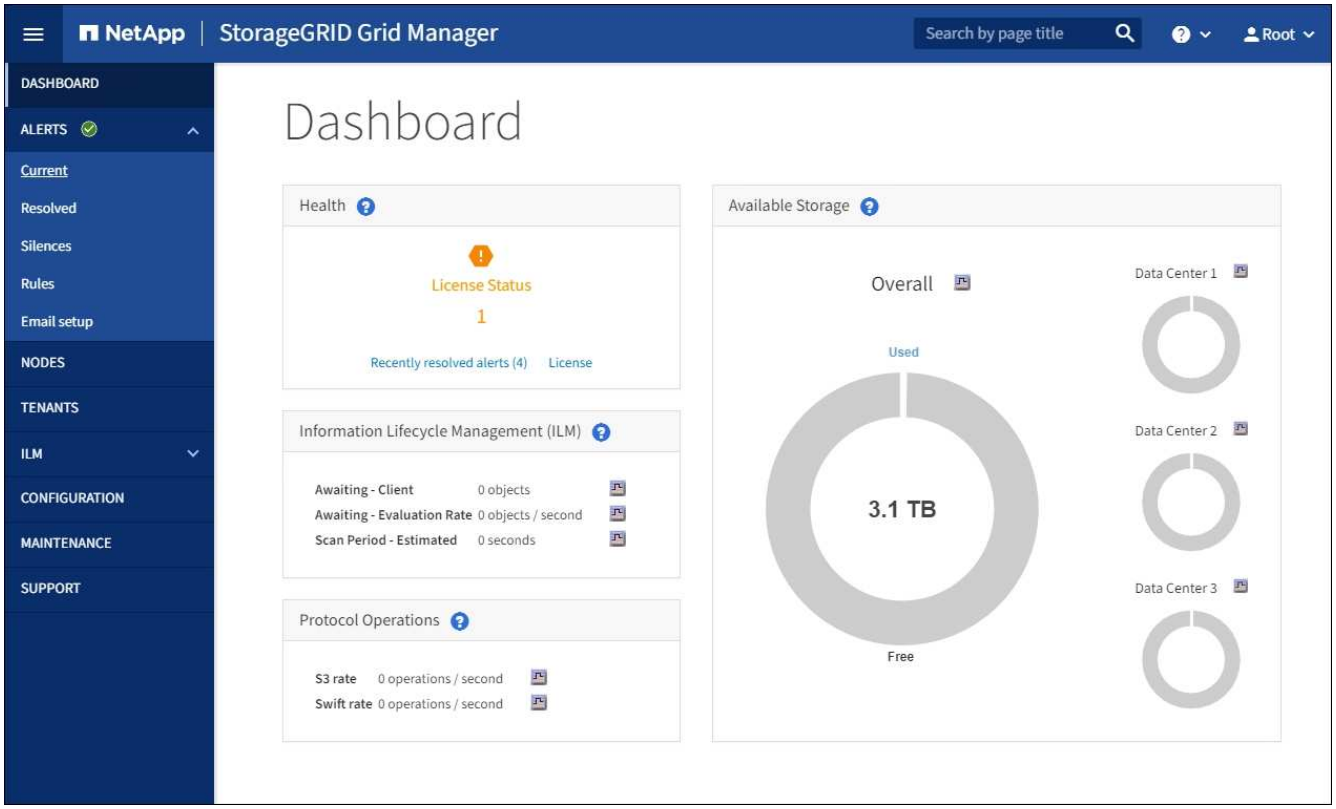



- Si SSO está habilitado para el sistema StorageGRID y ya ha accedido previamente a Grid Manager o a una cuenta de inquilino:

i. Realice una de las siguientes acciones:

- Introduzca **0** (el ID de cuenta de Grid Manager) y seleccione **Iniciar sesión**.
- Seleccione **Grid Manager** si aparece en la lista de cuentas recientes y seleccione **Iniciar sesión**.

ii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización. Cuando haya iniciado sesión, aparecerá la página de inicio de Grid Manager, que incluye el Panel. Para saber qué información se proporciona, consulte Consulte la consola.




5. Si desea iniciar sesión en otro nodo de administración:

| Opción | Pasos |
| --- | --- |
| SSO no está habilitado | a. En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración. Incluya el número de puerto según sea necesario.<br>b. Introduzca su nombre de usuario y contraseña para el administrador de grid.<br>c. Seleccione **Iniciar sesión**. |
| SSO habilitado | En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración.<br><br>Si inició sesión en un nodo de administrador, puede acceder a otros nodos de administrador sin tener que volver a iniciar sesión. Sin embargo, si su sesión SSO caduca, se le solicitará de nuevo sus credenciales.<br><br>**Nota:** SSO no está disponible en el puerto restringido de Grid Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único. |

**Información relacionada**

- Controlar el acceso mediante firewalls
- Configurar el inicio de sesión único
- Gestione los grupos de administradores
- Gestión de grupos de alta disponibilidad
- Usar una cuenta de inquilino
- Supervisión y solución de problemas

## Cierre la sesión en Grid Manager

Cuando haya terminado de trabajar con Grid Manager, deberá cerrar sesión para asegurarse de que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

**Pasos**

1. Seleccione su nombre de usuario en la esquina superior derecha.

2. Seleccione **Cerrar sesión**.

| Opción | Descripción |
| --- | --- |
| SSO no en uso | Ha cerrado sesión en el nodo de administrador.<br><br>Se muestra la página de inicio de sesión de Grid Manager.<br><br>**Nota:** Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo. |
| SSO habilitado | Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página de inicio de sesión de StorageGRID. **Grid Manager** aparece como el valor predeterminado en la lista desplegable **Cuentas recientes**, y el campo **ID de cuenta** muestra 0.<br><br>**Nota:** Si SSO está activado y también ha iniciado sesión en el Administrador de arrendatarios, también debe cerrar sesión en la cuenta de arrendatario para cerrar sesión en SSO. |

**Información relacionada**

- Configurar el inicio de sesión único
- Usar una cuenta de inquilino

## Cambie la contraseña

Si es un usuario local de Grid Manager, puede cambiar su propia contraseña.

**Lo que necesitará**

Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

**Acerca de esta tarea**

Si inicia sesión en StorageGRID como usuario federado o si está activado el inicio de sesión único (SSO), no podrá cambiar la contraseña en Grid Manager. En su lugar, debe cambiar la contraseña en el origen de identidad externo, por ejemplo, Active Directory u OpenLDAP.

**Pasos**

1. En el encabezado de Grid Manager, seleccione ***su nombre*** > **Cambiar contraseña**.
2. Introduzca su contraseña actual.
3. Escriba una nueva contraseña.

   La contraseña debe contener al menos 8 caracteres y no más de 32. Las contraseñas distinguen mayúsculas de minúsculas.

4. Vuelva a introducir la nueva contraseña.
5. Seleccione **Guardar**.

## Cambie el tiempo de espera de la sesión del explorador

Puede controlar si los usuarios de Grid Manager y de arrendatario Manager han cerrado la sesión si están inactivos durante más de un cierto período de tiempo.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

El valor predeterminado de tiempo de espera de inactividad de la interfaz gráfica de usuario es 900 segundos (15 minutos). Si la sesión del explorador de un usuario no está activa durante este período de tiempo, se agota el tiempo de espera de la sesión.

Según sea necesario, puede aumentar o reducir el tiempo de espera mediante la configuración de la opción de visualización tiempo de espera de inactividad de la interfaz gráfica de usuario.

Si se activa el inicio de sesión único (SSO) y se agota el tiempo de espera de la sesión del explorador de un usuario, el sistema se comporta como si el usuario seleccionara **Cerrar sesión** manualmente. El usuario debe volver a introducir sus credenciales de SSO para volver a acceder a StorageGRID. Consulte Configurar el inicio de sesión único.

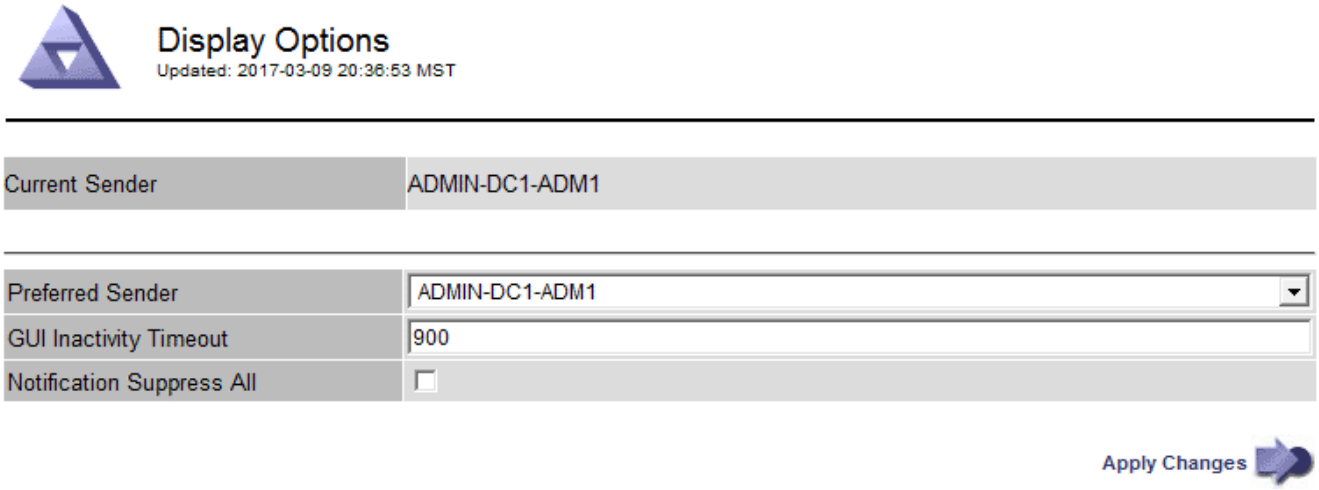
El tiempo de espera de la sesión de usuario también puede controlarse por lo siguiente:

- Temporizador StorageGRID independiente no configurable, que se incluye para la seguridad del sistema. De forma predeterminada, el token de autenticación de cada usuario caduca 16 horas después de que el usuario inicia sesión. Cuando caduca la autenticación de un usuario, ese usuario se cierra automáticamente, incluso si no se ha alcanzado el valor de tiempo de espera de inactividad de la interfaz gráfica de usuario. Para renovar el token, el usuario debe volver a iniciar sesión.
- Se ha agotado el tiempo de espera de la configuración del proveedor de identidades, suponiendo que SSO esté habilitado para StorageGRID.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. Para **tiempo de espera de inactividad de la GUI**, introduzca un período de tiempo de espera de 60 segundos o más.

   Configure este campo en 0 si no desea utilizar esta funcionalidad. Los usuarios se firman 16 horas después de iniciar sesión, cuando caducan sus tokens de autenticación.




3. Seleccione **aplicar cambios**.

   La nueva configuración no afecta a los usuarios que han iniciado sesión actualmente. Los usuarios deben iniciar sesión de nuevo o actualizar sus exploradores para que la nueva configuración de tiempo de espera tenga efecto.

## Consulte la información de licencia de StorageGRID

Puede ver la información de licencia del sistema StorageGRID, como la capacidad de almacenamiento máxima de su grid, cuando sea necesario.

### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

### Acerca de esta tarea

Si se produce un problema con la licencia de software para este sistema StorageGRID, el panel Estado del Panel incluye un icono de estado de licencia y un enlace **Licencia**. El número indica cuántos problemas relacionados con la licencia existen.

### Paso

Para ver la licencia, realice una de las siguientes acciones:

- En el panel Estado del panel, seleccione el icono de estado de la licencia o el enlace **Licencia**. Este vínculo sólo aparece si hay un problema con la licencia.

- Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.

Aparece la página Licencia y proporciona la siguiente información de sólo lectura acerca de la licencia actual:

- ID del sistema de StorageGRID, que es el número de identificación exclusivo para esta instalación de StorageGRID
- Número de serie de la licencia
- Capacidad de almacenamiento bajo licencia del grid
- Fecha de finalización de la licencia del software
- Fecha de finalización del contrato de servicio de soporte
- Contenido del archivo de texto de licencia

> Para las licencias emitidas antes de StorageGRID 10.3, la capacidad de almacenamiento con licencia no está incluida en el archivo de licencia y se muestra un mensaje "Ver acuerdo de licencia" en lugar de un valor.

## Actualice la información de licencia de StorageGRID

Debe actualizar la información de licencia del sistema de StorageGRID en cualquier momento que cambien las condiciones de su licencia. Por ejemplo, debe actualizar la información de la licencia si adquiere capacidad de almacenamiento adicional para su grid.

**Lo que necesitará**

- Tiene un nuevo archivo de licencia que se aplicará al sistema StorageGRID.
- Tiene permisos de acceso específicos.
- Tiene la clave de acceso de aprovisionamiento.

**Pasos**

1. Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.
2. Introduzca la frase de acceso de aprovisionamiento del sistema StorageGRID en el cuadro de texto **frase de paso** de aprovisionamiento.
3. Seleccione **examinar**.
4. En el cuadro de diálogo Abrir, busque y seleccione el nuevo archivo de licencia (`.txt`) Y seleccione **Abrir**.

   El nuevo archivo de licencia se valida y muestra.

5. Seleccione **Guardar**.

## Utilice la API

### Utilice la API de gestión de grid

Puede realizar tareas de administración del sistema mediante la API REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, se recomienda utilizar la API para automatizar operaciones o crear varias entidades, como

los usuarios, más rápidamente.

#### Recursos de alto nivel

La API de gestión de grid proporciona los siguientes recursos de nivel superior:

- `/grid`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`: Access está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener más información, consulte Usar una cuenta de inquilino.
- `/private`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados. Las API privadas están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

#### Emita solicitudes API

La API de gestión de grid utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores realizar operaciones en tiempo real en StorageGRID con la API.

La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

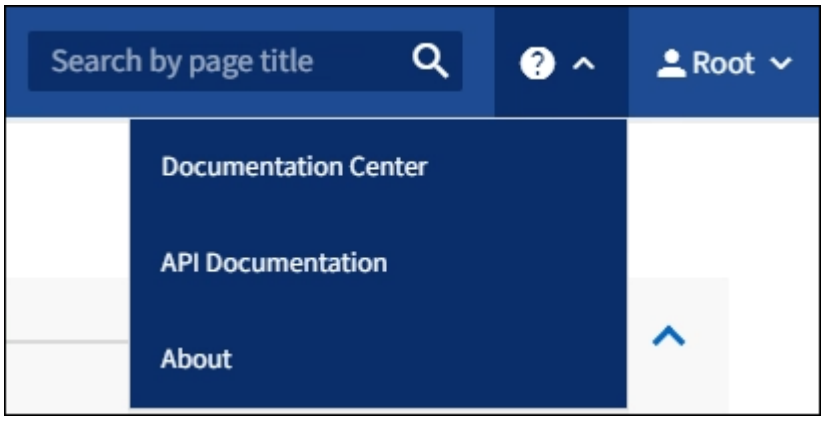
**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

> Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

**Pasos**

1. En el encabezado de Grid Manager, seleccione el icono de ayuda y seleccione **Documentación de API**.



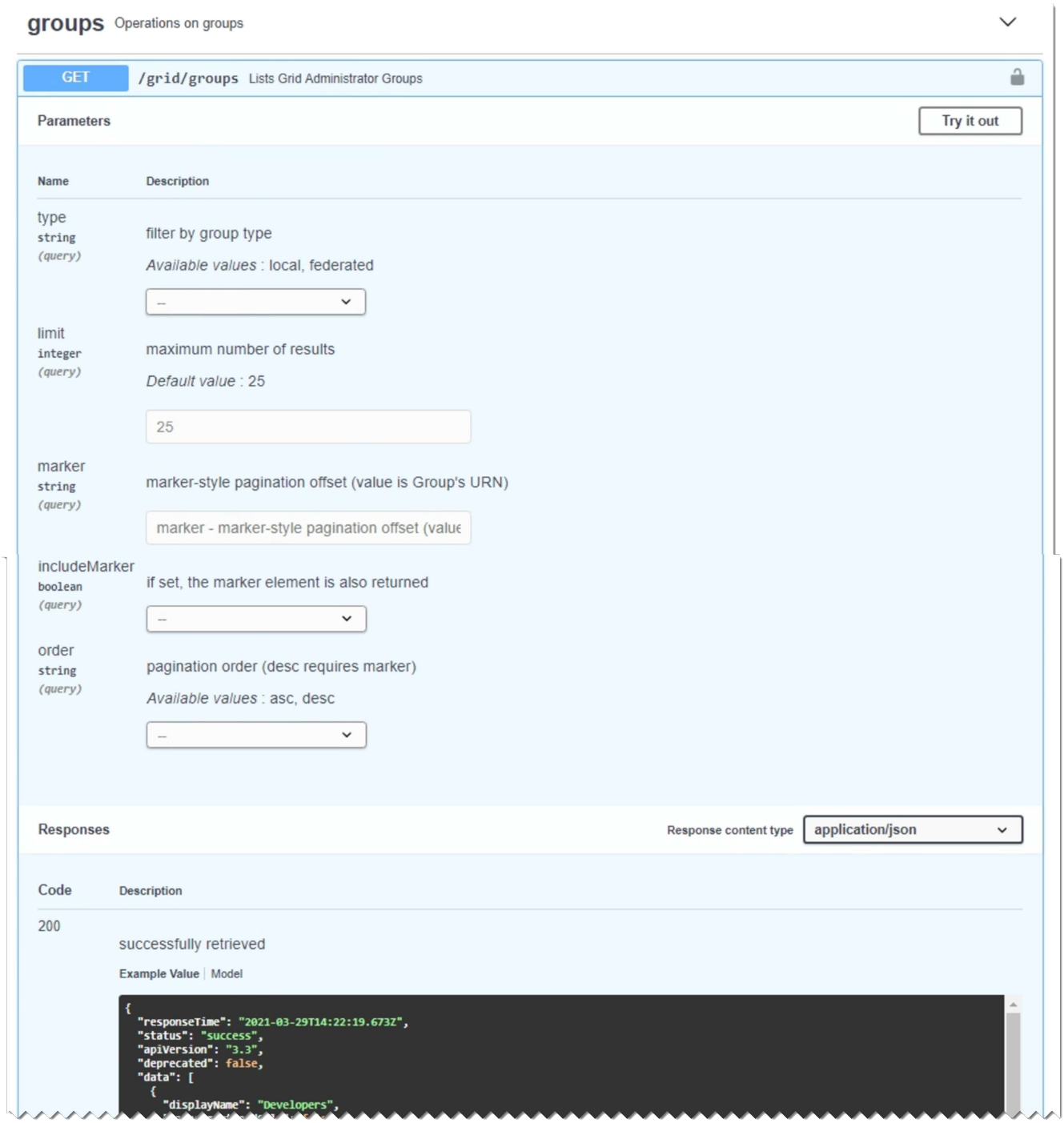

2. Para realizar una operación con la API privada, seleccione **Ir a documentación de API privada** en la página API de administración de StorageGRID.

   Las API privadas están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

3. Seleccione la operación deseada.

   Al expandir una operación de API, puede ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

4. Seleccione una acción HTTP para ver los detalles de la solicitud, incluida la dirección URL del extremo, una lista de los parámetros necesarios o opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.




5. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.

6. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **probar**.
8. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
9. Seleccione **Ejecutar**.
10. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

#### Operaciones de API de gestión de grid

La API de gestión de grid organiza las operaciones disponibles en las siguientes secciones.

> Esta lista solo incluye las operaciones disponibles en la API pública.

- **Cuentas** — Operaciones para administrar cuentas de arrendatarios de almacenamiento, incluyendo la creación de cuentas nuevas y la recuperación del uso del almacenamiento para una cuenta determinada.
- **Alarms** — Operaciones para enumerar las alarmas actuales (sistema heredado), y devolver información sobre el estado de la cuadrícula, incluyendo las alertas actuales y un resumen de los estados de conexión de los nodos.
- **Historial de alertas** — Operaciones en alertas resueltas.
- **ALERT-receptores** — Operaciones en receptores de notificación de alertas (correo electrónico).
- **Reglas de alerta** — Operaciones en reglas de alerta.
- **Silencios de alerta** — Operaciones en silencios de alerta.
- **Alertas** — Operaciones en alertas.
- **Audit** — Operaciones para enumerar y actualizar la configuración de auditoría.
- **Auth** — Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de grid admite el esquema de autenticación de token de Bearer. Para iniciar sesión, debe proporcionar un nombre de usuario y una contraseña en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token se debe proporcionar en el encabezado de las siguientes solicitudes de API ("autorización: Portador *token*").

  > Si el inicio de sesión único está habilitado para el sistema StorageGRID, debe realizar pasos diferentes para la autenticación. Consulte «"autenticación en la API si está activado el inicio de sesión único"."

  Consulte «"Protección contra la falsificación de solicitudes entre sitios"» para obtener información sobre la mejora de la seguridad de la autenticación.

- **Certificados cliente** — Operaciones para configurar certificados de cliente de modo que se pueda acceder a StorageGRID de forma segura utilizando herramientas de supervisión externas.
- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API de gestión de grid. Es posible mostrar la versión del producto y las versiones principales de la API de Grid Management compatibles con esta versión, así como deshabilitar las versiones obsoletas de la API.
- **Características desactivadas** — Operaciones para ver las funciones que podrían haberse desactivado.

- **servidores dns** — Operaciones para enumerar y cambiar los servidores DNS externos configurados.
- **Nombres-dominio-terminal** — Operaciones para enumerar y cambiar los nombres de dominio de punto final.
- **Codificación de borrado** — Operaciones en perfiles de codificación de borrado.
- **Expansión** — Operaciones de expansión (nivel de procedimiento).
- **Nodos de expansión** — Operaciones en expansión (a nivel de nodo).
- **Expansion-sites** — Operaciones en expansión (a nivel de sitio).
- **Grid-Networks** — Operaciones para enumerar y cambiar la Lista de redes Grid.
- **Grid-password** — Operaciones para la gestión de contraseñas de grid.
- **Grupos** — Operaciones para administrar grupos de administradores de grid locales y recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **Identity-source** — Operaciones para configurar un origen de identidad externo y sincronizar manualmente la información del grupo federado y del usuario.
- **ilm** — Operaciones en la gestión del ciclo de vida de la información (ILM).
- **Licencia** — Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **Logs** — Operaciones para recopilar y descargar archivos de registro.
- **Métricas** — Operaciones en métricas StorageGRID incluyendo consultas métricas instantáneas en un único punto en el tiempo y consultas métricas de rango en un intervalo de tiempo. La API de gestión de grid utiliza la herramienta de supervisión de sistemas Prometheus como origen de datos de back-end. Para obtener información sobre la construcción de consultas Prometheus, consulte el sitio web Prometheus.

> Métricas que incluyen `private` en sus nombres sólo se utilizan de forma interna. Estas métricas están sujetas a cambios entre las versiones de StorageGRID sin previo aviso.

- **Detalles del nodo** — Operaciones en los detalles del nodo.
- **Estado del nodo** — Operaciones en el estado del nodo.
- **ntp-Server** — Operaciones para enumerar o actualizar servidores de Protocolo de tiempo de redes (NTP) externos.
- **Objetos** — Operaciones en objetos y metadatos de objetos.
- **Recuperación** — Operaciones para el procedimiento de recuperación.
- **Paquete de recuperación** — Operaciones para descargar el paquete de recuperación.
- **Regiones** — Operaciones para ver y crear regiones.
- **s3-object-lock** — Operaciones en la configuración global de S3 Object Lock.
- **Server-certificate** — Operaciones para ver y actualizar certificados de servidor de Grid Manager.
- **snmp** — Operaciones en la configuración actual de SNMP.
- **Traffic-claes** — Operaciones para directivas de clasificación de tráfico.
- **Red-cliente-no confiable** — Operaciones en la configuración de Red cliente no confiable.
- **Usuarios** — Operaciones para ver y administrar usuarios de Grid Manager.

### Creación de versiones de la API de gestión de grid

## La API de gestión de grid utiliza versiones para permitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 3 de la API.

`https://hostname_or_ip_address/api/v3/authorize`

La versión principal de la API de administración de arrendatarios se bONTAP cuando se realizan cambios que son ***no compatibles*** con versiones anteriores. La versión menor de la API de administración de arrendatarios se bONTAP cuando se hacen cambios que ***are sea compatible*** con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos extremos o nuevas propiedades. En el ejemplo siguiente se muestra cómo la versión de API se bONTAP en función del tipo de cambios realizados.

| Tipo de cambio en la API | Versión anterior | Nueva versión |
|---|---|---|
| Compatible con versiones anteriores | 2.1 | 2.2 |
| No es compatible con versiones anteriores | 2.1 | 3.0 |

Al instalar el software StorageGRID por primera vez, sólo se activa la versión más reciente de la API de gestión de grid. Sin embargo, cuando actualice a una versión de función nueva de StorageGRID, seguirá teniendo acceso a la versión de API anterior para al menos una versión de función de StorageGRID.

Puede utilizar la API de gestión de grid para configurar las versiones compatibles. Consulte la sección «'config'» de la documentación de API de Swagger para obtener más información. Debe desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API de Grid Management para que utilicen la versión más reciente.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes formas:

- El encabezado de la respuesta es "Dedeprecated: True"
- El cuerpo de respuesta JSON incluye "obsoleto": TRUE
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

#### Determine qué versiones de API son compatibles con la versión actual

Utilice la siguiente solicitud de API para devolver una lista de las versiones principales de API admitidas:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

#### Especifique una versión API para una solicitud

Puede especificar la versión de API mediante un parámetro path (`/api/v3`) o un encabezado (`Api-Version: 3`). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

#### Protección contra falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitudes entre sitios (CSRF) contra StorageGRID mediante tokens CSRF para mejorar la autenticación que usa cookies. El administrador de grid y el administrador de inquilinos habilitan automáticamente esta característica de seguridad; otros clientes de API pueden elegir si habilitar la función cuando se conectan.

Un atacante que pueda activar una solicitud a un sitio diferente (por ejemplo, con UNA POST de formulario HTTP) puede provocar ciertas solicitudes mediante las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra ataques de CSRF mediante tokens CSRF. Cuando se activa, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro DE cuerpo DE POST específico.

Para habilitar la función, configure la `csrfToken` parámetro a. `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, un `GridCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en Grid Manager y en `AccountCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en el Administrador de inquilinos.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir una de las siguientes:

- La `X-Csrf-Token` Encabezado, con el valor del encabezado establecido en el valor de la cookie de token de CSRF.
- Para los extremos que aceptan un cuerpo codificado mediante formulario: A. `csrfToken` parámetro de cuerpo de solicitud codificado mediante formulario.

Consulte la documentación de API en línea para obtener detalles y ejemplos adicionales.

> Las solicitudes que tienen un conjunto de cookies de token CSRF también harán cumplir el `"Content-Type: application/json"` Encabezado para cualquier solicitud que espera un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

### Use la API si está activado el inicio de sesión único

#### Utilizar la API si está activado el inicio de sesión único (Active Directory)

Si lo tiene Inicio de sesión único configurado y habilitado (SSO) Además, se utiliza Active Directory como proveedor SSO, debe emitir una serie de solicitudes API para obtener un token de autenticación válido para la API de administración de grid o la API de administración de inquilinos.

#### Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO.

**Lo que necesitará**

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

**Acerca de esta tarea**

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de

instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).

- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

**Pasos**

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Introduzca ADFS o adfs.
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.

   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

> Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada `TENANTACCOUNTID`. Los resultados se pasan a. `python -m json.tool` Para quitar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenga una URL completa que incluya el ID de solicitud de cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión mediante la URL de la respuesta anterior.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La respuesta incluye el ID de solicitud del cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Guarde el ID de solicitud de cliente de la respuesta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envíe sus credenciales a la acción de formulario de la respuesta anterior.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS devuelve un redireccionamiento 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para el sistema SSO, la entrada del formulario también contendrá la segunda contraseña u otras credenciales.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Guarde la `MSISAuth` cookie de la respuesta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envíe una solicitud GET a la ubicación especificada con las cookies de LA PUBLICACIÓN de autenticación.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Los encabezados de respuesta contendrán información de sesión de AD FS para el uso posterior del cierre de sesión y el cuerpo de respuesta contiene el SAMLResponse en un campo de formulario oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Guarde la `SAMLResponse` en el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

   Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

   La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

   Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

### Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos. Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO

#### Acerca de esta tarea

Si es necesario, puede cerrar la sesión de la API de StorageGRID simplemente cerrando la sesión en la página única de cierre de sesión de su empresa. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

#### Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true"` En la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si `cookie "sso=true"` No proporciona, el usuario cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

#### Use la API si el inicio de sesión único está habilitado (Azure)

Si lo tiene Inicio de sesión único configurado y habilitado (SSO) Además, utilice Azure como proveedor SSO, puede utilizar dos scripts de ejemplo para obtener un token de autenticación válido para la API de gestión de grid o la API de gestión de inquilinos.

##### Inicie sesión en la API si el inicio de sesión único de Azure está habilitado

Estas instrucciones se aplican si utiliza Azure como proveedor de identidades de SSO

**Lo que necesitará**

- Conoce la dirección de correo electrónico y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

**Acerca de esta tarea**

Para obtener un token de autenticación, puede utilizar las siguientes secuencias de comandos de ejemplo:

- La `storagegrid-ssoauth-azure.py` Guión Python
- La `storagegrid-ssoauth-azure.js` Secuencia de comandos Node.js

Ambos scripts se encuentran en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).

Para escribir su propia integración de API con Azure, consulte `storagegrid-ssoauth-azure.py` guión. El script de Python hace dos solicitudes a StorageGRID directamente (primero para obtener el SAMLRequest, y más tarde para obtener el token de autorización), y también llama al script Node.js para interactuar con Azure para realizar las operaciones de SSO.

Las operaciones SSO se pueden ejecutar mediante una serie de solicitudes API, pero hacerlo no es sencillo. El módulo Puppeteer Node.js se utiliza para raspar la interfaz SSO de Azure.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

**Pasos**

1. Instale las dependencias necesarias de la siguiente manera:
   a. Instale Node.js (consulte "https://nodejs.org/en/download/").

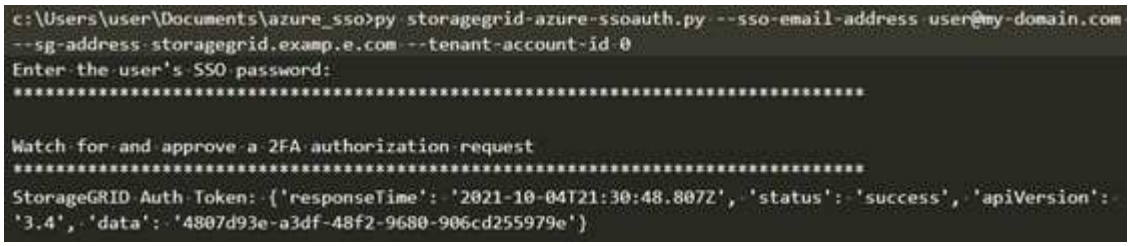
b. Instale los módulos Node.js necesarios (tippeteer y jsdom):

```
npm install -g <module>
```

2. Pase la secuencia de comandos de Python al intérprete de Python para ejecutar la secuencia de comandos.

   La secuencia de comandos Python llamará al script Node.js correspondiente para realizar las interacciones de SSO de Azure.

3. Cuando se le solicite, introduzca valores para los siguientes argumentos (o bien, pasarlos mediante parámetros):
   - La dirección de correo electrónico de SSO que se utiliza para iniciar sesión en Azure
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos
4. Cuando se le solicite, introduzca la contraseña y esté preparado para proporcionar una autorización de MFA para Azure si así se lo solicita.




> La secuencia de comandos asume que la MFA se realiza utilizando Microsoft Authenticator. Es posible que deba modificar el script para admitir otras formas de MFA (como introducir un código recibido a través de un mensaje de texto).

El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

#### Utilizar la API si está activado el inicio de sesión único (PingFederate)

Si lo tiene Inicio de sesión único configurado y habilitado (SSO) Además, debe utilizar PingFederate como proveedor SSO, para obtener un token de autenticación válido para la API de gestión de grid o la API de gestión de inquilinos, debe emitir una serie de solicitudes API.

#### Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

#### Lo que necesitará

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

#### Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).
- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

  Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

**Pasos**

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Puede introducir cualquier variación de "'pingfederate'" (PINGFEDERATE, pingfederate, etc.).
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puede dejarlo en blanco o introducir cualquier valor.
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.
3. Si desea usar solicitudes curl, use el siguiente procedimiento.
   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan a python -m json.tool para quitar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exporte la respuesta y el cookie y añada la respuesta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporte el valor 'pf.adapterId' y añada la respuesta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporte el valor 'href' (retire la barra diagonal inversa /) y añada la respuesta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporte el valor de 'acción':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies junto con credenciales:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Guarde la `SAMLResponse` en el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

### Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos. Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

#### Acerca de esta tarea

Si es necesario, puede cerrar la sesión de la API de StorageGRID simplemente cerrando la sesión en la página única de cierre de sesión de su empresa. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

#### Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true"` En la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si `cookie "sso=true"` No proporciona, el usuario cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

# Control del acceso a StorageGRID

## Cambie la clave de acceso del aprovisionamiento

Use este procedimiento para cambiar la clave de acceso de aprovisionamiento de StorageGRID. La frase de acceso es necesaria para los procedimientos de recuperación, expansión y mantenimiento. La clave de acceso también se requiere para descargar los backups del paquete de recuperación que incluyen la información de topología de la cuadrícula, las contraseñas de la consola del nodo de la cuadrícula y las claves de cifrado del sistema StorageGRID.

### Lo que necesitará

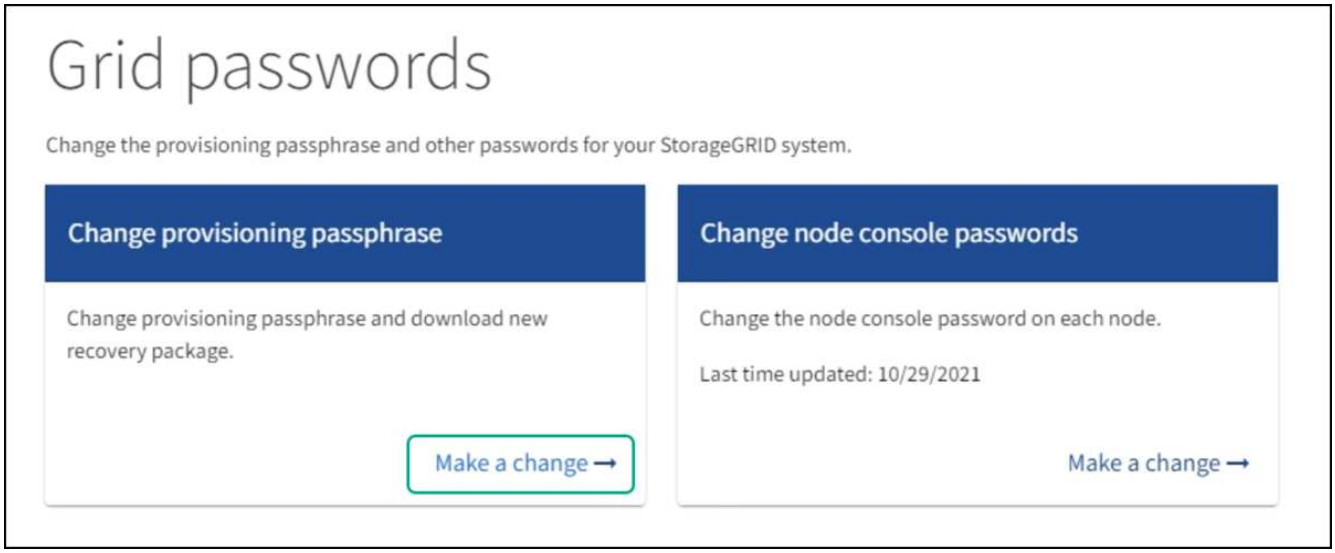
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene la clave de acceso de aprovisionamiento actual.

### Acerca de esta tarea

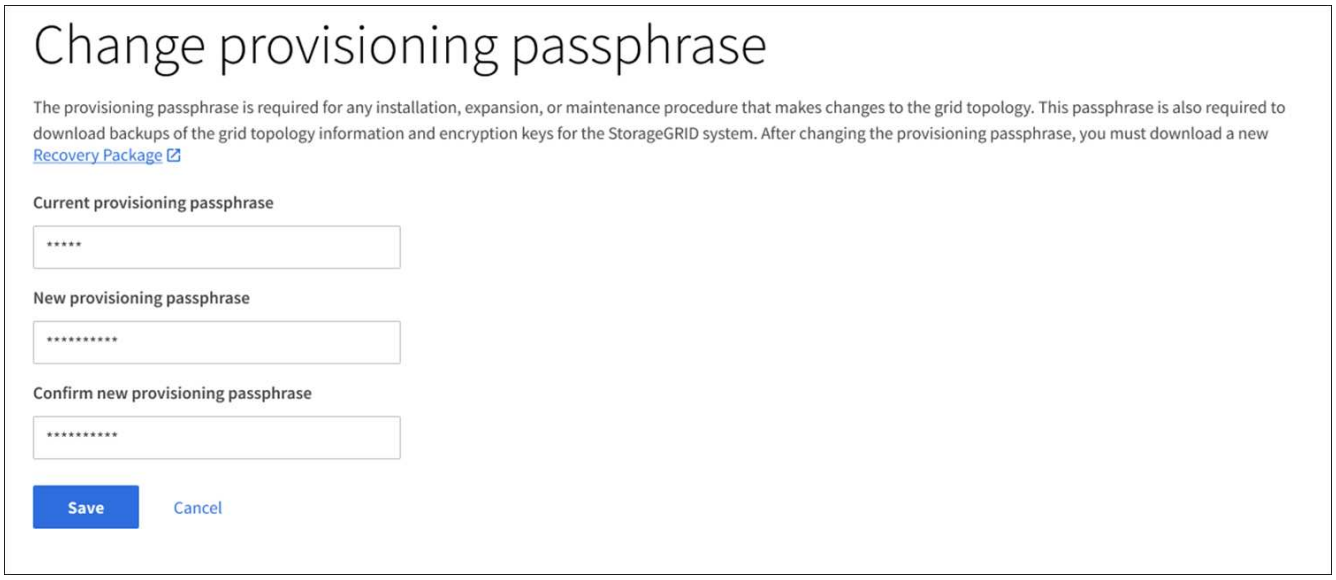
La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para Descarga del paquete de recuperación. La clave de acceso de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la frase de acceso de aprovisionamiento y mantenerla en una ubicación segura.

### Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **contraseñas de cuadrícula**.

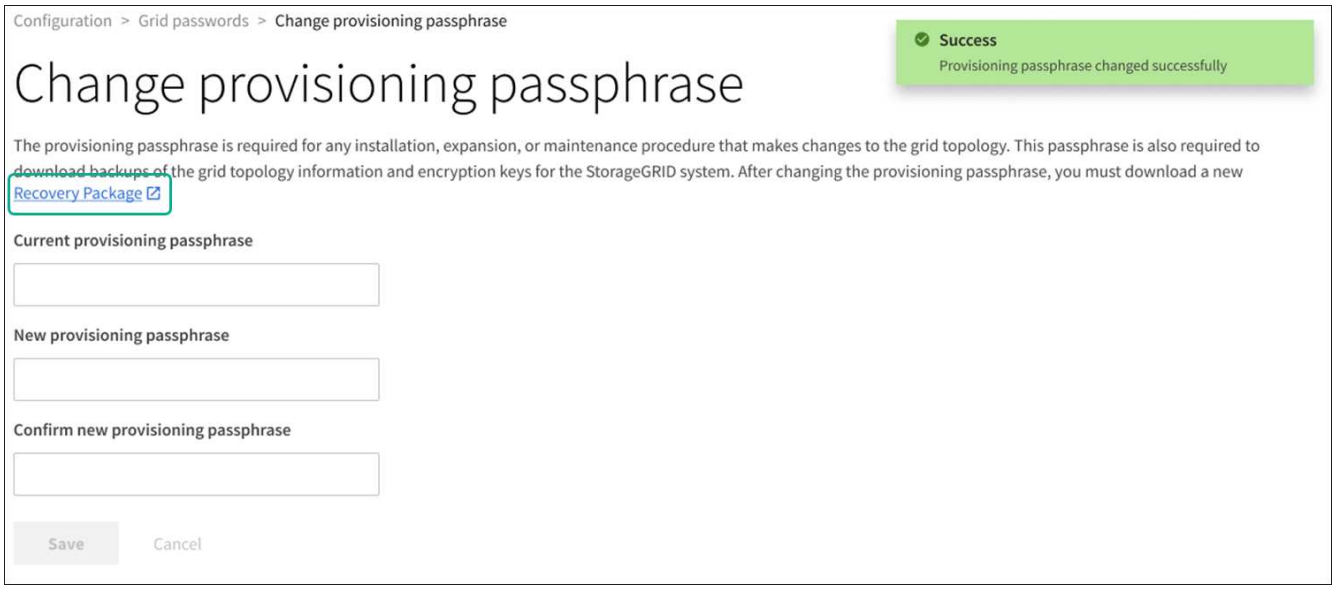



2. Seleccione **hacer un cambio** en **Cambiar contraseña de aprovisionamiento**.




3. Introduzca la clave de acceso de aprovisionamiento actual.
4. Introduzca la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.
5. Almacene la nueva clave de acceso de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.
6. Vuelva a introducir la nueva contraseña y seleccione **Guardar**.

   El sistema muestra un banner verde de éxito cuando se completa el cambio de la clave de acceso de aprovisionamiento.




7. Seleccione **paquete de recuperación**.
8. Introduzca la nueva clave de acceso de aprovisionamiento para descargar el nuevo paquete de recuperación.

> Después de cambiar la contraseña de aprovisionamiento, debe descargar inmediatamente un nuevo paquete de recuperación. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

## Cambie las contraseñas de la consola de los nodos

Cada nodo de su grid tiene una contraseña de consola de nodo única, que necesita iniciar sesión en el nodo. Siga estos pasos para cambiar cada contraseña de la consola de nodos única para cada nodo de la cuadrícula.

### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso de mantenimiento o acceso raíz.
- Tiene la clave de acceso de aprovisionamiento actual.

### Acerca de esta tarea

Utilice la contraseña de la consola del nodo para iniciar sesión en un nodo como “admin” mediante SSH o en el usuario root en una conexión de la consola física/VM. El proceso de cambiar la contraseña de la consola del nodo crea nuevas contraseñas para cada nodo de la cuadrícula y almacena las contraseñas en una actualización `Passwords.txt` En el paquete de recuperación. Las contraseñas figuran en la columna Password de la `Passwords.txt` archivo.

> Hay contraseñas de acceso SSH separadas para las claves SSH que se usan para la comunicación entre nodos. Este procedimiento no cambia las contraseñas de acceso SSH.

### Acceda al asistente

### Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **contraseñas de cuadrícula**.
2. En **Cambiar contraseñas de consola de nodo**, selecciona **Hacer un cambio**.

### Introduzca la clave de acceso de aprovisionamiento

### Pasos

1. Introduzca la clave de acceso de aprovisionamiento para el grid.
2. Seleccione **continuar**.

### Descargue el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola de nodos, descargue el paquete de recuperación actual. Puede usar las contraseñas de este archivo si el proceso de cambio de contraseña falla en cualquier nodo.

### Pasos

1. Seleccione **Descargar paquete de recuperación**.
2. Copie el archivo del paquete de recuperación (`.zip`) a dos ubicaciones seguras, seguras y separadas.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

3. Seleccione **continuar**.
4. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para empezar a cambiar las contraseñas de la consola del nodo.

No puede cancelar este proceso una vez que se inicia.

### Cambie las contraseñas de la consola de los nodos

Cuando se inicia el proceso de contraseña de la consola del nodo, se genera un nuevo paquete de recuperación que incluye las nuevas contraseñas. A continuación, las contraseñas se actualizan en cada nodo.

**Pasos**

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Seleccione **Descargar nuevo paquete de recuperación**.
3. Cuando finalice la descarga:

   a. Abra el `.zip` archivo.

   b. Confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo, que contiene las nuevas contraseñas de la consola del nodo.

   c. Copie el nuevo archivo de Recovery Package (`.zip`) a dos ubicaciones seguras, seguras y separadas.

   > No sobrescriba el paquete de recuperación antiguo.

   El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

4. Active la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y que ha verificado el contenido.
5. Seleccione **Cambiar contraseñas de consola de nodos** y espere a que todos los nodos se actualicen con las nuevas contraseñas. Esto puede tardar varios minutos.

   Si se modifican contraseñas para todos los nodos, se muestra un banner verde de éxito. Vaya al paso siguiente.

   Si se produce un error durante el proceso de actualización, un mensaje de banner enumera la cantidad de nodos que no pudieron cambiar sus contraseñas. El sistema volverá a intentar automáticamente el proceso en cualquier nodo que no haya cambiado su contraseña. Si el proceso finaliza con algunos nodos que aún no han cambiado la contraseña, aparece el botón **Reintentar**.

   Si la actualización de la contraseña falló para uno o más nodos:

   a. Revise los mensajes de error que aparecen en la tabla.

   b. Resuelva los problemas.

   c. Seleccione **Reintentar**.

   > Al volver a intentar solo se cambian las contraseñas de la consola de nodos en los nodos que fallaron durante los intentos anteriores de cambio de contraseña.

6. Después de cambiar las contraseñas de la consola de nodos para todos los nodos, elimine el Primer paquete de recuperación descargado.
7. Opcionalmente, utilice el enlace **paquete de recuperación** para descargar una copia adicional del nuevo

paquete de recuperación.

## Controlar el acceso mediante firewalls

Cuando desee controlar el acceso a través de firewalls, puede abrir o cerrar puertos específicos en el firewall externo.

### Controlar el acceso al firewall externo

Puede controlar el acceso a las interfaces de usuario y las API de los nodos de administrador de StorageGRID. Para ello, abra y cierre puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse a Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

| Puerto | Descripción | Si el puerto está abierto… |
|---|---|---|
| 443 | Puerto HTTPS predeterminado para nodos de administración | Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager, a la API de gestión de grid, al administrador de inquilinos y a la API de gestión de inquilinos.<br><br>**Nota:** el puerto 443 también se utiliza para tráfico interno. |
| 8443 | Puerto de Grid Manager restringido en nodos de administración | • Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager y a la API de gestión de grid mediante HTTPS.<br>• Los exploradores web y los clientes de API de gestión no pueden acceder al administrador de inquilinos ni a la API de gestión de inquilinos.<br>• Se rechazarán las solicitudes de contenido interno. |
| 9443 | Puerto de administrador de inquilinos restringido en los nodos de administrador | • Los exploradores web y los clientes de API de gestión pueden acceder al administrador de inquilinos y a la API de gestión de inquilinos mediante HTTPS.<br>• Los exploradores web y los clientes de la API de administración no pueden acceder a Grid Manager ni a la API de gestión de grid.<br>• Se rechazarán las solicitudes de contenido interno. |

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

**Información relacionada**

- Inicie sesión en Grid Manager

- Cree una cuenta de inquilino
- Comunicaciones externas

## Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de grupos y usuarios y permite a los usuarios iniciar sesión en StorageGRID utilizando credenciales conocidas.

### Configurar la federación de identidades para Grid Manager

Puede configurar la federación de identidades en Grid Manager si desea que los grupos y usuarios de administración se gestionen en otro sistema como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

> Si desea utilizar un servicio LDAP v3 que no esté en la lista, póngase en contacto con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar un servidor OpenLDAP.
- Si tiene pensado habilitar el inicio de sesión único (SSO), ha revisado el requisitos para usar el inicio de sesión único.
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades usa TLS 1.2 o 1.3. Consulte Cifrados compatibles para conexiones TLS salientes.

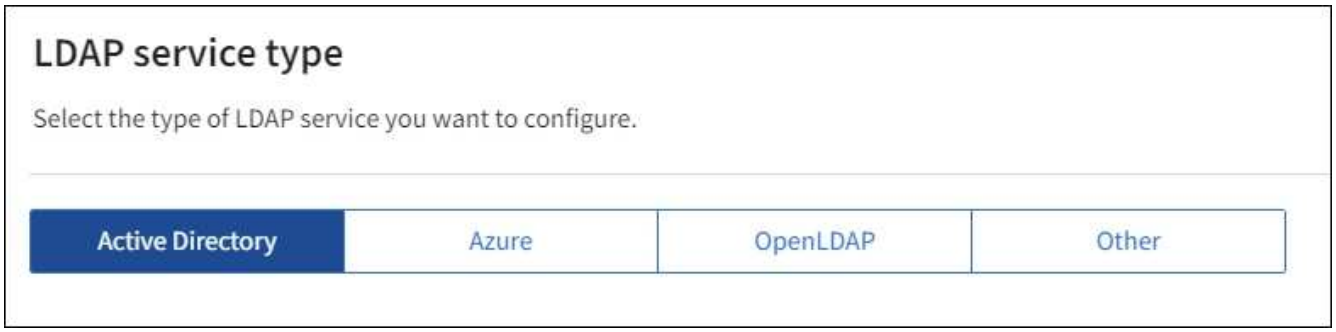
#### Acerca de esta tarea

Puede configurar un origen de identidades para Grid Manager si desea importar grupos de otro sistema, como Active Directory, Azure AD, OpenLDAP u Oracle Directory Server. Puede importar los siguientes tipos de grupos:

- Grupos de administración. Los usuarios de los grupos de administración pueden iniciar sesión en Grid Manager y realizar tareas basándose en los permisos de administración asignados al grupo.
- Grupos de usuarios de inquilinos para inquilinos que no utilizan su propio origen de identidad. Los usuarios de grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, en función de los permisos asignados al grupo en el Administrador de inquilinos. Consulte Cree una cuenta de inquilino y.. Usar una cuenta de inquilino para obtener más detalles.

#### Introduzca la configuración

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.




Seleccione **otros** para configurar valores para un servidor LDAP que utilice Oracle Directory Server.

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
   - **Nombre único de usuario**: Nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `uid` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `uid`.
   - **UUID de usuario**: Nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único del grupo**: Nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `cn` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `cn`.
   - **UUID de grupo**: Nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.
   - **Hostname**: El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.

   - **Nombre de usuario**: La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP.

     Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

     El usuario especificado debe tener permiso para enumerar grupos y usuarios y para tener acceso a los siguientes atributos:

     - `sAMAccountName` o. `uid`

- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure**: `accountEnabled` y.. `userPrincipalName`

◦ **Contraseña**: La contraseña asociada al nombre de usuario.

◦ **DN base de grupo**: La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com).

> Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.

◦ **DN base de usuario**: La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.

> Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

◦ **Formato de nombre de usuario Bind** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe utilizar si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario Bind** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazar con la cuenta de servicio.

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (Active Directory y Azure)**: `[USERNAME]@*example*.com`
- **Patrón de nombre de inicio de sesión de nivel inferior (Active Directory y Azure)**: `*example*\[USERNAME]`
- **Patrón de nombre completo**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Incluya **[USERNAME]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   ◦ **Use STARTTLS**: Utilice STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.
   ◦ **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
   ◦ **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

> El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA del sistema operativo**: Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

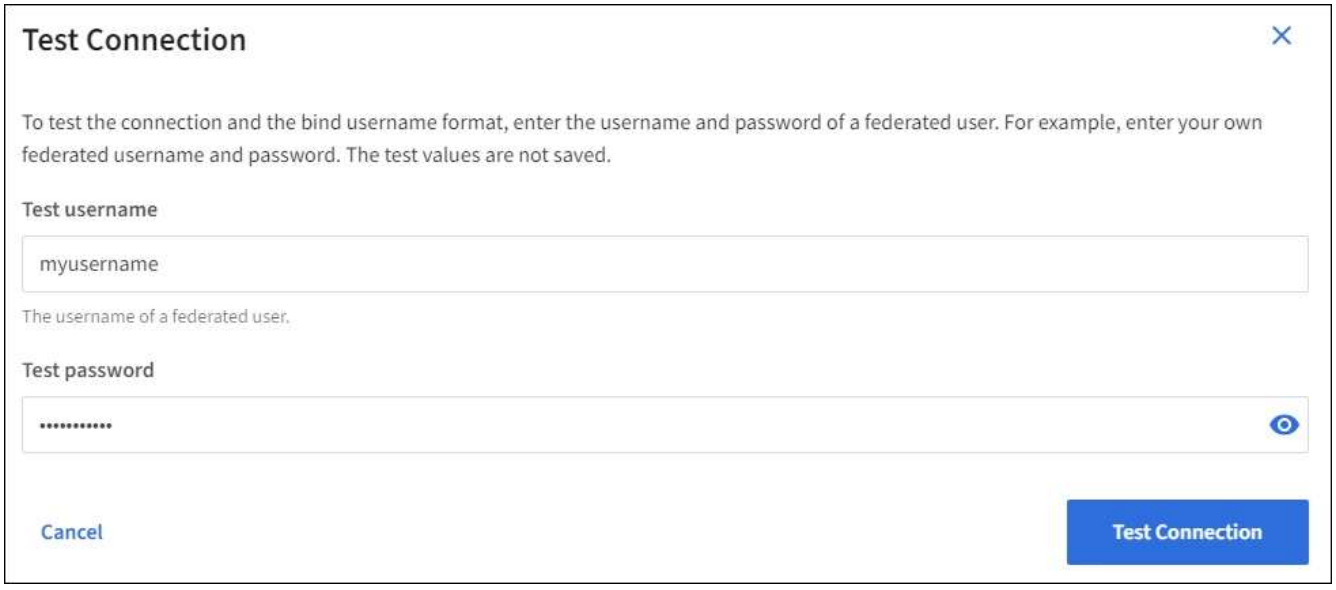
     Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

#### Pruebe la conexión y guarde la configuración

Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
   - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
   - Aparece el mensaje «"no se ha podido establecer la conexión de prueba"» si los ajustes de conexión no son válidos. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduzca su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.




   - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
   - Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

### Forzar la sincronización con el origen de identidades

El sistema StorageGRID sincroniza periódicamente grupos federados y usuarios del origen de identidades. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo antes posible.

**Pasos**

1. Vaya a la página federación de identidades.
2. Seleccione **servidor de sincronización** en la parte superior de la página.

   El proceso de sincronización puede tardar bastante tiempo en función del entorno.

> La alerta **fallo de sincronización de la federación de identidades** se activa si hay un problema al sincronizar grupos federados y usuarios del origen de identidades.

### Deshabilitar la federación de identidades

Puede deshabilitar temporalmente o de forma permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está deshabilitada, no existe comunicación entre StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

**Acerca de esta tarea**

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- No se realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Activar federación de identidades** está desactivada si el inicio de sesión único (SSO) está establecido en **activado** o **modo Sandbox**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades. Consulte Desactive el inicio de sesión único.

**Pasos**

1. Vaya a la página federación de identidades.
2. Desactive la casilla de verificación **Activar federación de identidades**.

### Instrucciones para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar ajustes específicos en el servidor OpenLDAP.

> Para los orígenes de identidad que no son ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 del usuario y quite el usuario de todos los grupos.

#### Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso enhttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^].

#### Indización

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de pertenencia a grupos inversa en lahttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^].

## Gestione los grupos de administradores

Es posible crear grupos de administración para gestionar los permisos de seguridad de uno o más usuarios de administrador. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

### Cree un grupo de administración

Los grupos de administración permiten determinar a qué usuarios se puede acceder a qué características y operaciones en Grid Manager y en la API de gestión de grid.

#### Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **grupos de administración**.
2. Seleccione **Crear grupo**.

#### Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a los usuarios locales.

- Cree un grupo federado para importar usuarios desde el origen de identidades.

**Grupo local**

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que puede actualizar más adelante si es necesario. Por ejemplo, «usuarios de mantenimiento» o «Administradores de ILM».
3. Introduzca un nombre único para el grupo, que no se podrá actualizar más adelante.
4. Seleccione **continuar**.

**Grupo federado**

1. Seleccione **Grupo federado**.
2. Introduzca el nombre del grupo que desea importar, exactamente como aparece en el origen de identidad configurado.
   - Para Active Directory y Azure, utilice sAMAccountName.
   - Para OpenLDAP, utilice CN (Nombre común).
   - Para otro LDAP, utilice el nombre exclusivo adecuado para el servidor LDAP.
3. Seleccione **continuar**.

#### Administrar permisos de grupo

1. En **modo de acceso**, seleccione si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en Grid Manager y la API de gestión de grid o si sólo pueden ver la configuración y las características.
   - **Read-write** (predeterminado): Los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o en la API de gestión de grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

   > ⓘ Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione uno o varios Permisos de grupo.

   Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenezcan al grupo no podrán iniciar sesión en StorageGRID.

3. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

#### Añadir usuarios (sólo grupos locales)

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

   Si todavía no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página usuarios. ConsulteGestionar usuarios para obtener más detalles.

2. Seleccione **Crear grupo** y **Finalizar**.

### Consulte y edite los grupos de administración

Puede ver los detalles de los grupos existentes, modificar un grupo o duplicar un grupo.

- Para ver información básica de todos los grupos, revise la tabla de la página grupos.
- Para ver todos los detalles de un grupo específico o editar un grupo, utilice el menú **acciones** o la página de detalles.

| Tarea | Menú Actions | Detalles |
|---|---|---|
| Ver detalles del grupo | a. Seleccione la casilla de verificación del grupo.<br>b. Seleccione **acciones** > **Ver detalles del grupo**. | Seleccione el nombre del grupo en la tabla. |
| Editar nombre para mostrar (sólo grupos locales) | a. Seleccione la casilla de verificación del grupo.<br>b. Seleccione **acciones** > **Editar nombre de grupo**.<br>c. Introduzca el nuevo nombre.<br>d. Seleccione **Guardar cambios**. | a. Seleccione el nombre del grupo para mostrar los detalles.<br>b. Seleccione el icono de edición .<br>c. Introduzca el nuevo nombre.<br>d. Seleccione **Guardar cambios**. |
| Edite el modo de acceso o los permisos | a. Seleccione la casilla de verificación del grupo.<br>b. Seleccione **acciones** > **Ver detalles del grupo**.<br>c. Si lo desea, cambie el modo de acceso del grupo.<br>d. Opcionalmente, seleccione o anule la selección Permisos de grupo.<br>e. Seleccione **Guardar cambios**. | a. Seleccione el nombre del grupo para mostrar los detalles.<br>b. Si lo desea, cambie el modo de acceso del grupo.<br>c. Opcionalmente, seleccione o anule la selección Permisos de grupo.<br>d. Seleccione **Guardar cambios**. |

### Duplicar un grupo

1. Seleccione la casilla de verificación del grupo.
2. Seleccione **acciones** > **Duplicar grupo**.
3. Complete el asistente para grupos duplicados.

### Eliminar un grupo

Es posible eliminar un grupo de administración cuando se desea quitar el grupo del sistema y quitar todos los permisos asociados con el grupo. Al eliminar un grupo de administración, se quitan todos los usuarios del grupo, pero no se eliminan los usuarios.

1. En la página grupos, active la casilla de verificación de cada grupo que desee quitar.

2. Seleccione **acciones** > **Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

### Permisos de grupo

Al crear grupos de usuarios de administrador, debe seleccionar uno o más permisos para controlar el acceso a funciones específicas de Grid Manager. A continuación, puede asignar cada usuario a uno o varios de estos grupos de administración para determinar qué tareas puede realizar el usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios pertenecientes a ese grupo no podrán iniciar sesión en Grid Manager o en la API de gestión de grid.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Inicie sesión en Grid Manager
- Consulte la consola
- Puede ver las páginas Nodes
- Supervise la topología de grid
- Ver las alertas actuales y resueltas
- Ver alarmas actuales e históricas (sistema heredado)
- Cambiar su propia contraseña (sólo usuarios locales)
- Vea cierta información en las páginas Configuración y Mantenimiento

#### Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas. Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

En las siguientes secciones se describen los permisos que se pueden asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se haya mencionado explícitamente requiere el permiso **acceso raíz**.

#### Acceso raíz

Este permiso proporciona acceso a todas las funciones de administración de grid.

#### Confirmar alarmas (heredadas)

Este permiso proporciona acceso para reconocer y responder a alarmas (sistema heredado). Todos los usuarios que han iniciado sesión pueden ver las alarmas actuales e históricas.

Si desea que un usuario supervise la topología de la cuadrícula y reconozca únicamente las alarmas, debe asignar este permiso.

#### Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Este permiso

también se usa para migrar claves S3 cuando se habilita la función de importación de claves S3. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.

> Para conceder acceso a la página arrendatarios, que contiene la opción **Cambiar contraseña root**, también asigne el permiso **Cuentas de arrendatario**.

#### Configuración de la página de topología de grid

Este permiso permite acceder a las fichas Configuración de la página **SUPPORT** > **Tools** > **Topología de cuadrícula**.

#### ILM

Este permiso permite acceder a las siguientes opciones del menú **ILM**:

- Bases de datos
- Normativas
- Codificación de borrado
- Regiones
- Pools de almacenamiento

> Los usuarios deben tener los permisos **Other grid Configuration** y **Grid Topology page Configuration** para administrar los grados de almacenamiento.

#### Mantenimiento

Los usuarios deben tener permiso de mantenimiento para utilizar estas opciones:

- **CONFIGURACIÓN** > **Control de acceso**:
  - Contraseñas de grid
- **MANTENIMIENTO** > **tareas**:
  - Retirada
  - Expansión
  - Comprobación de existencia de objeto
  - Recuperación
- **MANTENIMIENTO** > **sistema**:
  - Paquete de recuperación
  - Actualización de software
- **SOPORTE** > **Herramientas**:
  - Registros

Los usuarios que no tienen permiso de mantenimiento pueden ver, pero no editar, estas páginas:

- **MANTENIMIENTO** > **Red**:
  - Servidores DNS
  - Red Grid

    - Servidores NTP
- **MANTENIMIENTO** > **sistema**:
    - Licencia
- **CONFIGURACIÓN** > **Seguridad**:
    - Certificados
    - Nombres de dominio
- **CONFIGURACIÓN** > **Supervisión**:
    - Servidor de auditoría y syslog

#### Gestionar alertas

Este permiso proporciona acceso a opciones para gestionar alertas. Los usuarios deben tener este permiso para gestionar las silencios, las notificaciones de alerta y las reglas de alerta.

#### Consulta de métricas

Este permiso permite acceder a la página **SUPPORT** > **Tools** > **Metrics**. Este permiso también proporciona acceso a consultas de métricas Prometheus personalizadas mediante la sección **Metrics** de la API de gestión de grid.

#### Búsqueda de metadatos de objetos

Este permiso proporciona acceso a la página **ILM** > **Búsqueda de metadatos de objetos**.

#### Otra configuración de cuadrícula

Este permiso proporciona acceso a opciones de configuración de cuadrícula adicionales.

> Para ver estas opciones adicionales, los usuarios también deben tener el permiso **Configuración de página de topología de cuadrícula**.

- **ILM**:
    - Grados de almacenamiento
- **CONFIGURACIÓN** > **Red**:
    - Coste del enlace
- **CONFIGURACIÓN** > **sistema**:
    - Opciones de visualización
    - Opciones de cuadrícula
    - Opciones de almacenamiento
- **SOPORTE** > **Alarmas (heredado)**:
    - Eventos personalizados
    - Alarmas globales
    - Configuración de correo electrónico heredado

#### Administrador de dispositivos de almacenamiento

Este permiso proporciona acceso al System Manager de SANtricity E-Series en dispositivos de almacenamiento a través de Grid Manager.

#### Cuentas de inquilino

Este permiso proporciona acceso a la página arrendatarios, donde puede crear, editar y quitar cuentas de arrendatario. Este permiso también permite a los usuarios ver las directivas de clasificación de tráfico existentes.

## Desactivar las funcionalidades con la API

Puede utilizar la API de gestión de grid para desactivar por completo determinadas funciones del sistema StorageGRID. Cuando se desactiva una función, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

#### Acerca de esta tarea

El sistema de funciones desactivadas le permite impedir el acceso a determinadas funciones del sistema StorageGRID. La desactivación de una característica es la única forma de impedir que el usuario raíz o los usuarios que pertenecen a grupos de administración con permiso **acceso raíz** puedan utilizar esa función.

Para comprender cómo puede ser útil esta funcionalidad, considere el siguiente escenario:

*Company A es un proveedor de servicios que arrienda la capacidad de almacenamiento de su sistema StorageGRID mediante la creación de cuentas de inquilino. Para proteger la seguridad de los objetos de sus arrendatarios, la Compañía A desea asegurarse de que sus propios empleados nunca tengan acceso a ninguna cuenta de arrendatario después de que se haya implementado la cuenta.*

*La empresa A puede lograr este objetivo mediante el sistema Desactivar características en la API de gestión de grid. Al desactivar completamente la característica **Cambiar contraseña raíz de arrendatario** en Grid Manager (tanto la interfaz de usuario como la API), la Compañía A puede garantizar que ningún usuario de administrador (incluido el usuario raíz y los usuarios pertenecientes a grupos con el permiso **acceso raíz**) puede cambiar la contraseña para el usuario raíz de cualquier cuenta de arrendatario.*

#### Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management. Consulte Utilice la API de gestión de grid.
2. Busque el extremo Desactivar funciones.
3. Para desactivar una función, como Cambiar contraseña raíz de inquilino, envíe un cuerpo a la API de este modo:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Cuando se completa la solicitud, la función Cambiar contraseña raíz de inquilino está desactivada. El permiso de administración **Cambiar contraseña raíz de arrendatario** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino fallará con "'403 Prohibido".

### Reactivar las funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de grid para reactivar una función que se

haya desactivado. Sin embargo, si desea evitar que alguna vez se reactiven las funciones desactivadas, puede desactivar la propia función **activateFeatures**.

> La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar otras funciones desactivadas. Para restaurar cualquier funcionalidad perdida, debe ponerse en contacto con el soporte técnico.

**Pasos**

1. Acceda a la documentación de Swagger para la API de Grid Management.
2. Busque el extremo Desactivar funciones.
3. Para reactivar todas las funciones, envíe un cuerpo a la API de este modo:

```
{ "grid": null }
```

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar contraseña raíz del inquilino. El permiso de administración **Cambiar contraseña raíz de arrendatario** aparece ahora en la interfaz de usuario y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino se realizará correctamente, suponiendo que el usuario tenga el permiso de administración **acceso raíz** o **Cambiar contraseña raíz de inquilino**.

> El ejemplo anterior hace que se reactiven las funciones *all* desactivadas. Si se han desactivado otras funciones que deben permanecer desactivadas, debe especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar contraseña raíz de arrendatario y continuar desactivando la función de confirmación de alarma, envíe esta solicitud DE ENVÍO:
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

## Gestionar usuarios

Es posible ver usuarios locales y federados. También puede crear usuarios locales y asignarles grupos de administración locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

### Cree un usuario local

Es posible crear uno o varios usuarios locales y asignar cada usuario a uno o varios grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y la API de gestión de grid puede acceder el usuario.

Solo es posible crear usuarios locales. Utilice el origen de identidades externo para administrar grupos y usuarios federados.

Grid Manager incluye un usuario local predefinido denominado «'root'». No puede quitar el usuario raíz.

Si está habilitado el inicio de sesión único (SSO), los usuarios locales no podrán iniciar sesión en StorageGRID.

#### Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **usuarios de administración**.
2. Seleccione **Crear usuario**.

#### Introduzca las credenciales de usuario

1. Introduzca el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Opcionalmente, seleccione **Sí** si este usuario no debe tener acceso a Grid Manager o a la API de gestión de grid.
3. Seleccione **continuar**.

#### Asignar a grupos

1. Opcionalmente, asigne el usuario a uno o más grupos para determinar los permisos del usuario.

   Si aún no ha creado grupos, puede guardar el usuario sin seleccionar grupos. Puede agregar este usuario a un grupo en la página grupos.

   Si un usuario pertenece a varios grupos, los permisos son acumulativos. ConsulteGestione los grupos de administradores para obtener más detalles.

2. Seleccione **Crear usuario** y seleccione **Finalizar**.

### Ver y editar usuarios locales

Es posible ver detalles de los usuarios locales y federados existentes. Es posible modificar un usuario local para cambiar el nombre completo, la contraseña o la pertenencia a grupos del usuario. También puede impedir temporalmente que un usuario acceda a Grid Manager y a la API de gestión de grid.

Solo puede editar usuarios locales. Utilice el origen de identidad externo para administrar usuarios federados.

- Para ver la información básica de todos los usuarios locales y federados, revise la tabla en la página Users.
- Para ver todos los detalles de un usuario específico, editar un usuario local o cambiar la contraseña de un usuario local, utilice el menú **acciones** o la página de detalles.

  Las modificaciones se aplican la próxima vez que el usuario cierre sesión y vuelva a acceder al Gestor de cuadrícula.

  Los usuarios locales pueden cambiar sus propias contraseñas mediante la opción **Cambiar contraseña** del banner de Grid Manager.

| Tarea | Menú Actions | Detalles |
| --- | --- | --- |
| Ver los detalles del usuario | a. Seleccione la casilla de verificación del usuario.<br>b. Seleccione **acciones** > **Ver detalles del usuario**. | Seleccione el nombre del usuario en la tabla. |
| Editar nombre completo (sólo usuarios locales) | a. Seleccione la casilla de verificación del usuario.<br>b. Seleccione **acciones** > **Editar nombre completo**.<br>c. Introduzca el nuevo nombre.<br>d. Seleccione **Guardar cambios**. | a. Seleccione el nombre del usuario para mostrar los detalles.<br>b. Seleccione el icono de edición .<br>c. Introduzca el nuevo nombre.<br>d. Seleccione **Guardar cambios**. |
| Denegar o permitir el acceso a StorageGRID | a. Seleccione la casilla de verificación del usuario.<br>b. Seleccione **acciones** > **Ver detalles del usuario**.<br>c. Seleccione la pestaña Access.<br>d. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione **no** para permitir que el usuario inicie sesión.<br>e. Seleccione **Guardar cambios**. | a. Seleccione el nombre del usuario para mostrar los detalles.<br>b. Seleccione la pestaña Access.<br>c. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione **no** para permitir que el usuario inicie sesión.<br>d. Seleccione **Guardar cambios**. |
| Cambiar contraseña (solo usuarios locales) | a. Seleccione la casilla de verificación del usuario.<br>b. Seleccione **acciones** > **Ver detalles del usuario**.<br>c. Seleccione la ficha Contraseña.<br>d. Introduzca una contraseña nueva.<br>e. Seleccione **Cambiar contraseña**. | a. Seleccione el nombre del usuario para mostrar los detalles.<br>b. Seleccione la ficha Contraseña.<br>c. Introduzca una contraseña nueva.<br>d. Seleccione **Cambiar contraseña**. |

| Tarea | Menú Actions | Detalles |
| --- | --- | --- |
| Cambiar grupos (sólo usuarios locales) | a. Seleccione la casilla de verificación del usuario.<br>b. Seleccione **acciones** > **Ver detalles del usuario**.<br>c. Seleccione la ficha grupos.<br>d. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador.<br>e. Seleccione **Editar grupos** para seleccionar diferentes grupos.<br>f. Seleccione **Guardar cambios**. | a. Seleccione el nombre del usuario para mostrar los detalles.<br>b. Seleccione la ficha grupos.<br>c. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador.<br>d. Seleccione **Editar grupos** para seleccionar diferentes grupos.<br>e. Seleccione **Guardar cambios**. |

#### Duplique un usuario

Puede duplicar un usuario existente para crear un nuevo usuario con los mismos permisos.

1. Seleccione la casilla de verificación del usuario.
2. Seleccione **acciones** > **Duplicar usuario**.
3. Complete el asistente Duplicar usuario.

#### Eliminar un usuario

Puede eliminar un usuario local para eliminar de forma permanente ese usuario del sistema.

No puede eliminar el usuario raíz.

1. En la página Users (usuarios), seleccione la casilla de verificación de cada usuario que desee quitar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

## Utilizar inicio de sesión único (SSO)

#### Configurar el inicio de sesión único

Cuando se habilita el inicio de sesión único (SSO), los usuarios solo pueden acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid o a la API de gestión de inquilinos si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por la organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

##### Cómo funciona el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) con el estándar de lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0).

Antes de habilitar el inicio de sesión único (SSO), revise cómo se ven afectados los procesos de inicio de sesión y cierre de sesión de StorageGRID cuando se habilita SSO.

### Inicie sesión cuando SSO esté habilitado

Cuando se habilita SSO y usted inicia sesión en StorageGRID, se le redirigirá a la página SSO de su organización para validar sus credenciales.

**Pasos**

1. Introduzca el nombre de dominio o la dirección IP completos de cualquier nodo de administración de StorageGRID en un navegador web.

   Aparece la página Inicio de sesión de StorageGRID.

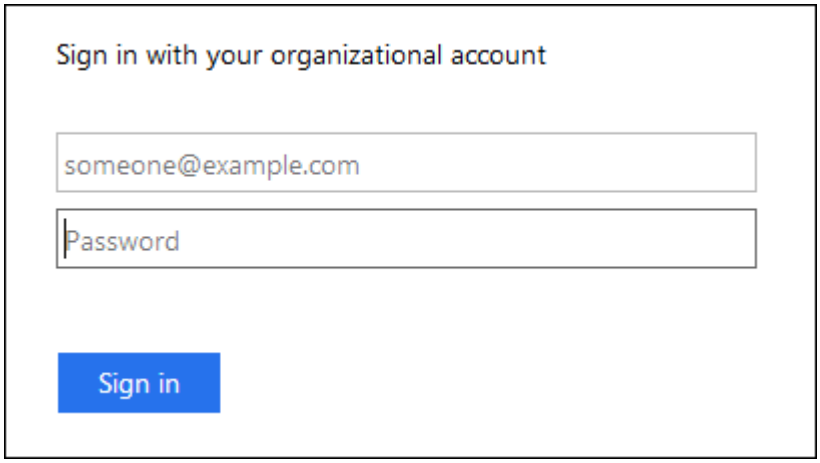
   - Si es la primera vez que accede a la URL en este navegador, se le pedirá un ID de cuenta:

   - Si anteriormente ha accedido al administrador de grid o al administrador de inquilinos, se le pedirá que seleccione una cuenta reciente o que introduzca un ID de cuenta:

> La página de inicio de sesión de StorageGRID no se muestra cuando introduce la URL completa de una cuenta de inquilino (es decir, un nombre de dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, se le redirige inmediatamente a la página de inicio de sesión con SSO de su organización, en la que puede hacerlo Inicie sesión con sus credenciales de SSO.

2. Indique si desea acceder al administrador de grid o al responsable de inquilinos:
   - Para acceder a Grid Manager, deje el campo **ID de cuenta** en blanco, introduzca **0** como ID de cuenta o seleccione **Gestor de cuadrícula** si aparece en la lista de cuentas recientes.
   - Para acceder al Administrador de arrendatarios, introduzca el ID de cuenta de arrendatario de 20 dígitos o seleccione un arrendatario por nombre si aparece en la lista de cuentas recientes.
3. Seleccione **Iniciar sesión**

   StorageGRID le redirige a la página de inicio de sesión con SSO de su organización. Por ejemplo:




4. inicia sesión con sus credenciales de SSO.

   Si sus credenciales de SSO son correctas:

   a. El proveedor de identidades (IDP) ofrece una respuesta de autenticación a StorageGRID.
   b. StorageGRID valida la respuesta de autenticación.
   c. Si la respuesta es válida y pertenece a un grupo federado con permisos de acceso a StorageGRID, se ha iniciado sesión en el Gestor de grid o el Gestor de inquilinos, según la cuenta seleccionada.

   > Si no se puede acceder a la cuenta de servicio, puede iniciar sesión siempre que sea un usuario existente que pertenezca a un grupo federado con permisos de acceso StorageGRID.

5. Opcionalmente, acceda a otros nodos de administración o acceda al administrador de grid o al administrador de inquilinos, si dispone de los permisos adecuados.

   No es necesario volver a introducir sus credenciales de SSO.

### Cierre sesión cuando SSO esté habilitado

Cuando se habilita SSO en StorageGRID, lo que sucede cuando se inicia sesión depende de lo que se haya iniciado sesión y del lugar en el que se está cerrando sesión.

**Pasos**

1. Busque el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
2. Seleccione **Cerrar sesión**.

   Aparece la página Inicio de sesión de StorageGRID. La lista desplegable **Cuentas recientes** se actualiza

para incluir **Grid Manager** o el nombre del inquilino, por lo que puede acceder a estas interfaces de usuario más rápidamente en el futuro.

| Si ha iniciado sesión en… | Y salir de… | Se ha cerrado sesión en… |
|---|---|---|
| Grid Manager en uno o varios nodos de administrador | Grid Manager en cualquier nodo de administrador | Grid Manager en todos los nodos de administración<br><br>**Nota:** Si utiliza Azure para SSO, es posible que tarde unos minutos en salir de todos los nodos de administración. |
| Administrador de inquilinos en uno o varios nodos de administrador | Inquilino Manager en cualquier nodo de administrador | Administrador de inquilinos en todos los nodos de administrador |
| Tanto Grid Manager como Inquilino Manager | Administrador de grid | Sólo Grid Manager. También debe cerrar sesión en el Administrador de inquilinos para cerrar la sesión de SSO. |

La tabla resume lo que sucede cuando se inicia sesión si está utilizando una sola sesión del navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de explorador, debe cerrar la sesión en todas las sesiones de explorador por separado.

### Requisitos para usar el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID, revise los requisitos en esta sección.

#### Requisitos del proveedor de identidades

StorageGRID admite los siguientes proveedores de identidad de SSO (IDP):

- Servicio de Federación de Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

Debe configurar la federación de identidades para el sistema StorageGRID antes de poder configurar un proveedor de identidades SSO. El tipo de servicio LDAP que utiliza para controlar la federación de identidades qué tipo de SSO puede implementar.

| Se ha configurado el tipo de servicio LDAP | Opciones para el proveedor de identidades SSO |
|---|---|
| Active Directory | • Active Directory<br>• Azure<br>• PingFederate |

| Se ha configurado el tipo de servicio LDAP | Opciones para el proveedor de identidades SSO |
| --- | --- |
| Azure | Azure |

### Requisitos DE AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 debe utilizar "Actualización KB3201845", o superior.

- AD FS 3.0, incluido con la actualización de Windows Server 2012 R2 o superior.

### Requisitos adicionales

- Seguridad de la capa de transporte (TLS) 1.2 ó 1.3
- Microsoft .NET Framework, versión 3.5.1 o posterior

#### Requisitos de certificado de servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de gestión en cada nodo de administración para garantizar el acceso a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos. Cuando configura confianzas de partes confiadas (AD FS), aplicaciones empresariales (Azure) o conexiones de proveedores de servicio (PingFederate) para StorageGRID, utilizará el certificado de servidor como certificado de firma para las solicitudes StorageGRID.

Si aún no lo ha hecho se configuró un certificado personalizado para la interfaz de gestión, usted debe hacerlo ahora. Cuando instala un certificado de servidor personalizado, se utiliza para todos los nodos de administrador y puede usarlo en todas las confianzas de parte que dependen de StorageGRID, aplicaciones de empresa o conexiones del SP.

> No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en la confianza de una parte que confía, la aplicación de empresa o la conexión de SP. Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte que confía, la aplicación de empresa o la conexión del SP con el nuevo certificado.

Para acceder a la certificación de servidor de un nodo de administrador, inicie sesión en el shell de comandos del nodo y vaya al `/var/local/mgmt-api` directorio. Se denomina certificado de servidor personalizado `custom-server.crt`. El certificado de servidor predeterminado del nodo se denomina `server.crt`.

#### Requisitos de puertos

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único. Consulte Controlar el acceso mediante firewalls.

### Confirmar que los usuarios federados pueden iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar que al menos un usuario federado puede iniciar sesión en Grid Manager y en el Gestor de inquilinos para cualquier cuenta de inquilino existente.

**Lo que necesitará**

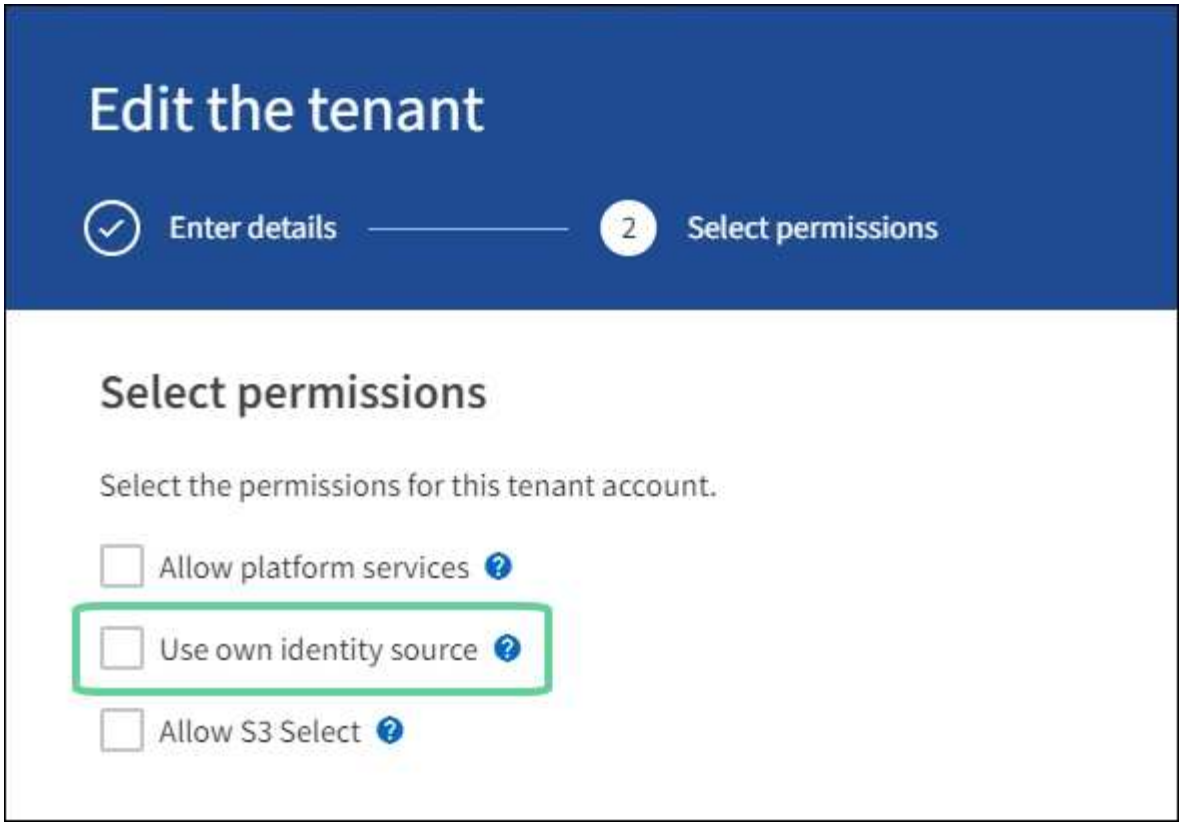
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ya ha configurado la federación de identidades.

**Pasos**

1. Si hay cuentas de inquilino existentes, confirme que ninguno de los inquilinos utiliza su propio origen de identidad.

   > Al habilitar SSO, el origen de identidad configurado en el Administrador de inquilinos se anula mediante el origen de identidades configurado en Grid Manager. Los usuarios que pertenezcan al origen de identidad del arrendatario ya no podrán iniciar sesión a menos que tengan una cuenta con el origen de identidad de Grid Manager.

   a. Inicie sesión en el Administrador de arrendatarios para cada cuenta de arrendatario.
   b. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
   c. Confirme que la casilla de verificación **Activar federación de identidades** no está activada.
   d. Si es así, confirme que los grupos federados que podrían estar en uso para esta cuenta de arrendatario ya no son necesarios, anule la selección de la casilla de verificación y seleccione **Guardar**.
2. Confirme que un usuario federado puede acceder a Grid Manager:
   a. En Grid Manager, seleccione **CONFIGURACIÓN** > **Control de acceso** > **grupos de administración**.
   b. Asegúrese de que al menos un grupo federado se ha importado del origen de identidad de Active Directory y de que se le ha asignado el permiso acceso raíz.
   c. Cierre la sesión.
   d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario en el grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado con permiso de acceso raíz puede iniciar sesión:
   a. En Grid Manager, seleccione **ARRENDATARIOS**.
   b. Seleccione la cuenta de arrendatario y seleccione **acciones** > **Editar**.
   c. En la ficha introducir detalles, seleccione **continuar**.
   d. Si la casilla de verificación **usar origen de identidad propio** está activada, desactive la casilla y seleccione **Guardar**.




Aparece la página inquilino.

a. Seleccione la cuenta de arrendatario, seleccione **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
b. En el Administrador de inquilinos, seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
c. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso de acceso raíz para este arrendatario.
d. Cierre la sesión.
e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

**Información relacionada**

- Requisitos para usar el inicio de sesión único
- Gestione los grupos de administradores
- Usar una cuenta de inquilino

### Utilizar el modo de recinto de seguridad

Es posible utilizar el modo de recinto de seguridad para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID. Una vez que se habilita SSO, es posible volver al modo Sandbox cada vez que sea necesario cambiar o volver a probar la configuración.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

- Configuró la federación de identidades para el sistema StorageGRID.
- Para la federación de identidades **Tipo de servicio LDAP**, ha seleccionado Active Directory o Azure, basándose en el proveedor de identidades SSO que planea utilizar.

| Se ha configurado el tipo de servicio LDAP | Opciones para el proveedor de identidades SSO |
|---|---|
| Active Directory | • Active Directory<br>• Azure<br>• PingFederate |
| Azure | Azure |

**Acerca de esta tarea**

Cuando se habilita el inicio de sesión único y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidades de SSO. A su vez, el proveedor de identidades SSO envía una respuesta de autenticación a StorageGRID para indicar si la solicitud de autenticación se ha realizado correctamente. Para solicitudes correctas:

- La respuesta de Active Directory o PingFederate incluye un identificador único universal (UUID) para el usuario.
- La respuesta de Azure incluye un nombre principal de usuario (UPN).

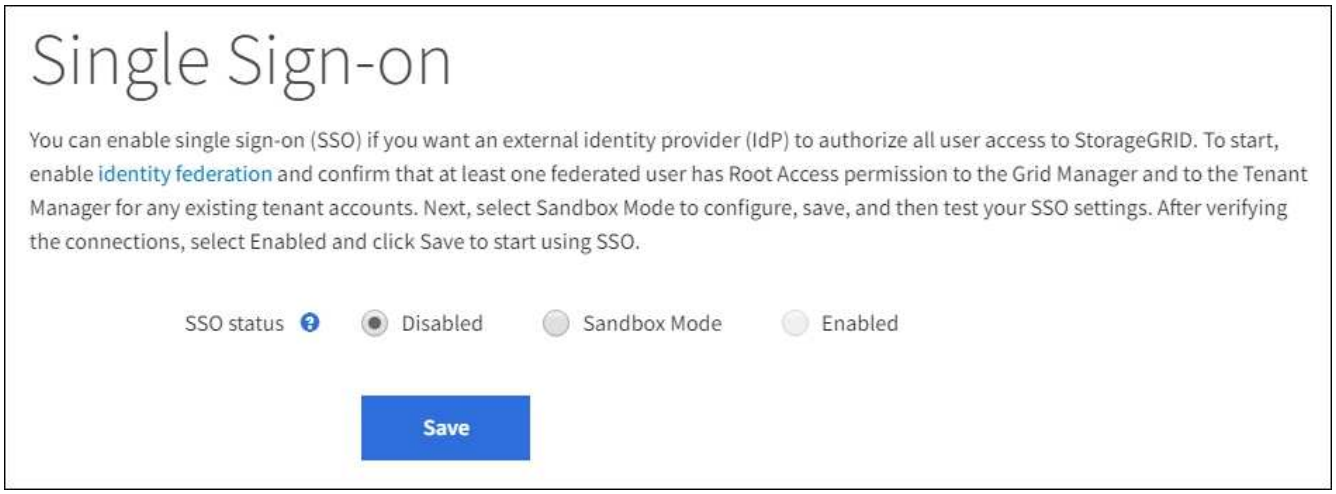
Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidades SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar determinados ajustes en StorageGRID. A continuación, debe utilizar el software del proveedor de identidades SSO para crear una confianza de parte fiable (AD FS), una aplicación empresarial (Azure) o un proveedor de servicios (PingFederate) para cada nodo de administración. Por último, debe volver a StorageGRID para habilitar SSO.

El modo de recinto de seguridad facilita la realización de esta configuración de fondo y la realización de pruebas de todos los ajustes antes de habilitar SSO. Cuando se utiliza el modo Sandbox, los usuarios no pueden iniciar sesión mediante SSO.

#### Acceder al modo de recinto de seguridad

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.

   Aparece la página Inicio de sesión único, con la opción **Desactivado** seleccionada.




Si no aparecen las opciones de estado de SSO, confirme que ha configurado el proveedor de identidades como origen de identidad federado. Consulte Requisitos para usar el inicio de sesión único.

2. Seleccione **modo Sandbox**.

   Aparece la sección Proveedor de identidades.

#### Introduzca los detalles del proveedor de identidades

1. Seleccione **Tipo SSO** en la lista desplegable.
2. Complete los campos de la sección Proveedor de identidades según el tipo de SSO seleccionado.

**Active Directory**

1. Introduzca el **nombre del servicio de Federación** para el proveedor de identidades, exactamente como aparece en el Servicio de Federación de Active Directory (AD FS).

   Para buscar el nombre del servicio de federación, vaya al Administrador de Windows Server. Seleccione **Herramientas** > **Administración AD FS**. En el menú Acción, seleccione **Editar propiedades del servicio de Federación**. El nombre del servicio de Federación se muestra en el segundo campo.

2. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

     Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

   - **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.
3. En la sección parte que confía, especifique el identificador * de parte que confía* para StorageGRID. Este valor controla el nombre que utiliza para cada confianza de parte que confía en AD FS.
   - Por ejemplo, si el grid solo tiene un nodo de administrador y no prevé añadir más nodos de administrador en el futuro, introduzca `SG` o. `StorageGRID`.
   - Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]`. De este modo, se genera una tabla que muestra el identificador de la parte que confía para cada nodo de administrador del sistema en función del nombre de host del nodo.

   Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

4. Seleccione **Guardar**.

   Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

**Azure**

1. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.

- **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

  Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

- **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

2. En la sección aplicación de empresa, especifique **Nombre de aplicación de empresa** para StorageGRID. Este valor controla el nombre que se utiliza para cada aplicación empresarial en Azure AD.

   - Por ejemplo, si el grid solo tiene un nodo de administrador y no prevé añadir más nodos de administrador en el futuro, introduzca `SG` o. `StorageGRID`.
   - Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]`. De este modo, se genera una tabla que muestra el nombre de una aplicación empresarial para cada nodo de administrador del sistema en función del nombre de host del nodo.

   > Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

3. Siga los pasos de Cree aplicaciones empresariales en Azure AD Para crear una aplicación de empresa para cada nodo de administración que se muestra en la tabla.
4. Desde Azure AD, copie la URL de metadatos de federación para cada aplicación empresarial. A continuación, pegue esta URL en el campo **URL** de metadatos de Federación correspondiente de StorageGRID.
5. Después de copiar y pegar una dirección URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar**.

   Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

**PingFederate**

1. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.

   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

     Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

   - **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

2. En la sección Proveedor de servicios (SP), especifique **ID de conexión SP** para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.
   - Por ejemplo, si el grid solo tiene un nodo de administrador y no prevé añadir más nodos de administrador en el futuro, introduzca `SG` o. `StorageGRID`.
   - Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]`. De este modo, se genera una tabla que muestra el ID de conexión del SP para cada nodo de administrador del sistema, según el nombre de host del nodo.

   > Debe crear una conexión de SP para cada nodo de administrador en el sistema StorageGRID. Tener una conexión de SP para cada nodo de administrador garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administrador.

3. Especifique la dirección URL de metadatos de federación para cada nodo de administración en el campo **URL de metadatos de Federación**.

   Utilice el siguiente formato:

   ```
   https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
   ```

4. Seleccione **Guardar**.

   Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

#### Configurar las confianzas de partes de confianza, las aplicaciones de la empresa o las conexiones de SP

Cuando se guarde la configuración, aparecerá el aviso de confirmación del modo Sandbox. Este aviso confirma que el modo de recinto de seguridad está ahora activado y proporciona instrucciones de descripción general.

StorageGRID puede permanecer en modo de recinto limitado siempre que sea necesario. Sin embargo, cuando se selecciona **modo Sandbox** en la página Single Sign-On, SSO está desactivado para todos los usuarios de StorageGRID. Solo los usuarios locales pueden iniciar sesión.

Siga estos pasos para configurar trusting Party trusts (Active Directory), completar aplicaciones empresariales (Azure) o configurar conexiones SP (PingFederate).

**Active Directory**

1. Vaya a Servicios de Federación de Active Directory (AD FS).
2. Cree una o varias confianzas de parte que dependan para StorageGRID, utilizando cada identificador de parte que dependa que se muestra en la tabla de la página StorageGRID Single Sign-On.

   Debe crear una confianza para cada nodo de administrador que se muestra en la tabla.

   Para obtener instrucciones, vaya a. Crear confianzas de parte de confianza en AD FS.

**Azure**

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
   a. Inicie sesión en el nodo.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya al portal de Azure.
4. Siga los pasos de Cree aplicaciones empresariales en Azure AD Para cargar el archivo de metadatos SAML para cada nodo de administrador en la aplicación empresarial de Azure correspondiente.

**PingFederate**

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
   a. Inicie sesión en el nodo.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya a PingFederate.
4. Cree una o varias conexiones de proveedor de servicios (SP) para StorageGRID. Utilice el ID de conexión del SP para cada nodo de administrador (que se muestra en la tabla de la página StorageGRID Single Sign-On) y los metadatos SAML que ha descargado para ese nodo de administrador.

   Debe crear una conexión de SP para cada nodo de administrador que se muestra en la tabla.

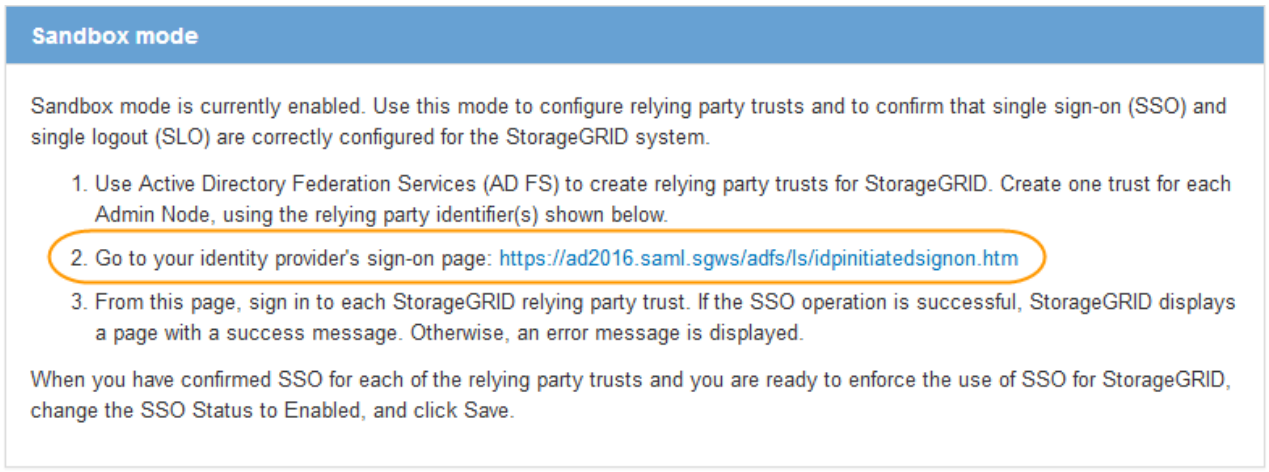
#### Probar conexiones SSO

Antes de aplicar el uso del inicio de sesión único para todo el sistema StorageGRID, debe confirmar que el inicio de sesión único y el cierre de sesión único están correctamente configurados para cada nodo de administración.

**Active Directory**

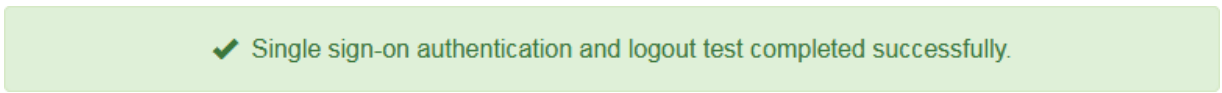
1. En la página Inicio de sesión único de StorageGRID, localice el vínculo en el mensaje modo Sandbox.

   La dirección URL se deriva del valor introducido en el campo **Nombre de servicio de Federación**.




2. Seleccione el enlace, o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión del proveedor de identidades.
3. Para confirmar que puede utilizar SSO para iniciar sesión en StorageGRID, seleccione **Iniciar sesión en uno de los siguientes sitios**, seleccione el identificador de la parte que confía para su nodo de administración principal y seleccione **Iniciar sesión**.

4. Introduzca el nombre de usuario y la contraseña federados.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.




   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

**Azure**

1. Vaya a la página Single Sign-On del portal de Azure.
2. Seleccione **probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.

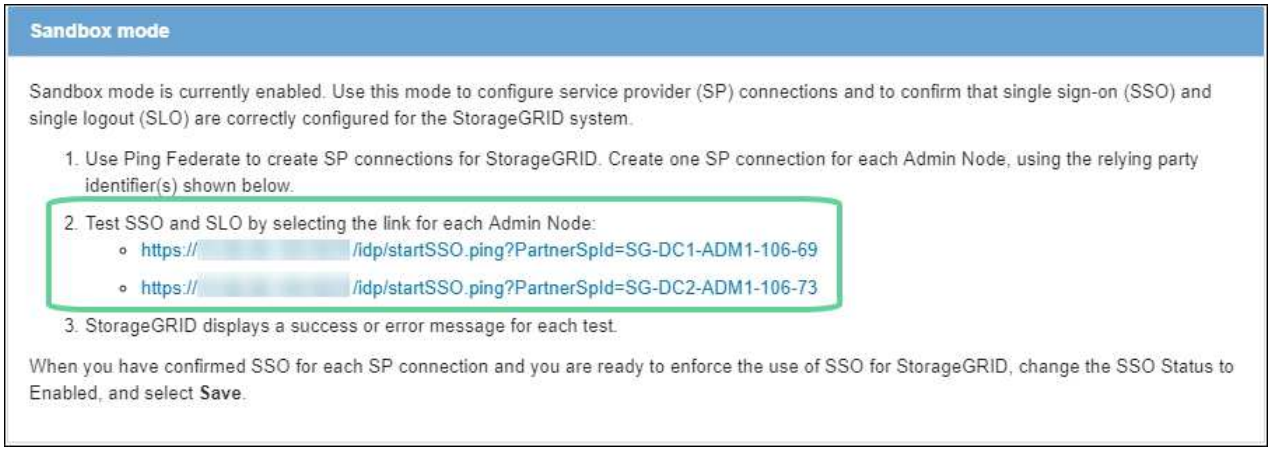
     ✔ Single sign-on authentication and logout test completed successfully.

   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

**PingFederate**

1. En la página Inicio de sesión único de StorageGRID, seleccione el primer enlace en el mensaje modo Sandbox.

   Seleccione y pruebe un enlace cada vez.




2. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
3. Seleccione el siguiente enlace para verificar la conexión de SSO para cada nodo de administrador de la cuadrícula.

   Si ve un mensaje Página caducada, seleccione el botón **Atrás** de su explorador y vuelva a enviar sus credenciales.

#### Active el inicio de sesión único

Una vez que haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, puede habilitar SSO en todo el sistema StorageGRID.

> Cuando SSO está habilitado, todos los usuarios deben utilizar SSO para acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de gestión de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
2. Cambie el estado de SSO a **habilitado**.
3. Seleccione **Guardar**.
4. Revise el mensaje de advertencia y seleccione **Aceptar**.

   El inicio de sesión único ahora está activado.

> Si utiliza el portal de Azure y accede a StorageGRID desde el mismo equipo que utiliza para acceder a Azure, asegúrese de que el usuario del portal de Azure también sea un usuario de StorageGRID autorizado (un usuario de un grupo federado que se ha importado a StorageGRID) O cierre la sesión en Azure Portal antes de intentar iniciar sesión en StorageGRID.

#### Crear confianzas de parte de confianza en AD FS

Debe utilizar los Servicios de Federación de Active Directory (AD FS) para crear una confianza de parte de confianza para cada nodo de administración del sistema. Puede crear confianzas de parte confiando mediante comandos de PowerShell, importando los metadatos de SAML desde StorageGRID o introduciendo los datos manualmente.

**Lo que necesitará**

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **AD FS** como tipo SSO.
- **Modo Sandbox** está seleccionado en la página Single Sign-On de Grid Manager. Consulte Utilizar el modo de recinto de seguridad.
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administración del sistema. Puede encontrar estos valores en la tabla de detalles Admin Nodes en la página StorageGRID Single Sign-On.

> Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

- Tiene experiencia en la creación de confianzas de parte de confianza en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.
- Si crea la confianza de la parte de confianza manualmente, tiene el certificado personalizado que se cargó para la interfaz de gestión de StorageGRID, o sabe cómo iniciar sesión en un nodo de administrador desde el shell de comandos.

**Acerca de esta tarea**

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si está utilizando una versión diferente de AD FS, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

#### Cree una confianza de parte de confianza mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más confianzas de parte que dependan.

**Pasos**

1. En el menú de inicio de Windows, seleccione con el botón derecho el icono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, introduzca el siguiente comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para *Admin_Node_Identifier*, Escriba el identificador de parte que confía para el nodo de administración, exactamente como aparece en la página Single Sign-On. Por ejemplo: `SG-DC1-ADM1`.
   - Para *Admin_Node_FQDN*, Escriba el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)
3. En Windows Server Manager, seleccione **Herramientas** > **Administración de AD FS**.

   Aparece la herramienta de administración de AD FS.
4. Seleccione **AD FS** > **fideicomisos de la parte**.

   Aparece la lista de confianzas de parte de confianza.
5. Agregar una directiva de control de acceso a la confianza de parte de confianza recién creada:
   a. Busque la parte de confianza que acaba de crear.
   b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de control de acceso**.
   c. Seleccione una Política de control de acceso.
   d. Seleccione **aplicar** y seleccione **Aceptar**
6. Agregar una política de emisión de reclamaciones a la nueva confianza de parte de confianza creada:
   a. Busque la parte de confianza que acaba de crear.
   b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
   c. Seleccione **Agregar regla**.
   d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
   e. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

      Por ejemplo, **ObjectGUID to Name ID**.

f. Para el almacén de atributos, seleccione **Active Directory**.

g. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.

h. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.

i. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Confirme que los metadatos se han importado correctamente.

a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.

b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

Si faltan metadatos, confirme que la dirección de metadatos de la Federación es correcta o simplemente introduzca los valores manualmente.

8. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.

9. Cuando haya terminado, vuelva a StorageGRID y pruebe todos los fideicomisos de las partes que dependan para confirmar que están configurados correctamente. Consulte Utilice el modo Sandbox si desea obtener instrucciones.

#### Cree una confianza de parte de confianza importando metadatos de federación

Puede importar los valores de cada una de las partes que confía mediante el acceso a los metadatos de SAML de cada nodo de administrador.

**Pasos**

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.

2. En acciones, seleccione **Agregar confianza de parte de confianza**.

3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.

4. Seleccione **Importar datos sobre la parte que confía publicada en línea o en una red local**.

5. En **Dirección de metadatos de Federación (nombre de host o URL)**, escriba la ubicación de los metadatos SAML para este nodo de administración:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *`Admin_Node_FQDN`*, Escriba el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

6. Complete el asistente Trust Party Trust, guarde la confianza de la parte que confía y cierre el asistente.

> Al introducir el nombre para mostrar, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página Single Sign-On en Grid Manager. Por ejemplo: `SG-DC1-ADM1`.

7. Agregar una regla de reclamación:

a. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de**

**reclamaciones**.

b. Seleccione **Agregar regla**:

c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.

d. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

   Por ejemplo, **ObjectGUID to Name ID**.

e. Para el almacén de atributos, seleccione **Active Directory**.

f. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.

g. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.

h. Seleccione **Finalizar** y seleccione **Aceptar**.

8. Confirme que los metadatos se han importado correctamente.

   a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.

   b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

      Si faltan metadatos, confirme que la dirección de metadatos de la Federación es correcta o simplemente introduzca los valores manualmente.

9. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.

10. Cuando haya terminado, vuelva a StorageGRID y pruebe todos los fideicomisos de las partes que dependan para confirmar que están configurados correctamente. Consulte Utilice el modo Sandbox si desea obtener instrucciones.

#### Cree una confianza de parte de confianza manualmente

Si elige no importar los datos de las confianzas de la pieza de confianza, puede introducir los valores manualmente.

**Pasos**

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, seleccione **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.
4. Seleccione **introducir datos sobre la parte que confía manualmente** y seleccione **Siguiente**.
5. Complete el asistente Trust Party Trust:

   a. Introduzca un nombre de visualización para este nodo de administración.

      Para obtener coherencia, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página de inicio de sesión único en Grid Manager. Por ejemplo: `SG-DC1-ADM1`.

   b. Omitir el paso para configurar un certificado de cifrado de token opcional.

   c. En la página Configurar URL, active la casilla de verificación **Activar compatibilidad con el**

**protocolo WebSSO** de SAML 2.0.

d. Escriba la URL del extremo de servicio SAML para el nodo de administración:

`https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, Escriba el nombre de dominio completo para el nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

e. En la página Configurar identificadores, especifique el identificador de parte que confía para el mismo nodo de administración:

*Admin_Node_Identifier*

Para *Admin_Node_Identifier*, Escriba el identificador de parte que confía para el nodo de administración, exactamente como aparece en la página Single Sign-On. Por ejemplo: `SG-DC1-ADM1`.

f. Revise la configuración, guarde la confianza de la parte que confía y cierre el asistente.

Aparecerá el cuadro de diálogo Editar directiva de emisión de reclamaciones.

> Si el cuadro de diálogo no aparece, haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de emisión de reclamaciones**.

6. Para iniciar el asistente para reglas de reclamación, seleccione **Agregar regla**:
   a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
   b. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

      Por ejemplo, **ObjectGUID to Name ID**.

   c. Para el almacén de atributos, seleccione **Active Directory**.
   d. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.
   e. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
   f. Seleccione **Finalizar** y seleccione **Aceptar**.
7. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
8. En la ficha **endpoints**, configure el extremo para un único cierre de sesión (SLO):
   a. Seleccione **Añadir SAML**.
   b. Seleccione **Tipo de extremo** > **SAML Logout**.
   c. Seleccione **enlace** > **Redirigir**.
   d. En el campo **Trusted URL**, introduzca la dirección URL utilizada para cerrar sesión único (SLO) desde este nodo de administración:

      `https://Admin_Node_FQDN/api/saml-logout`

Para *Admin_Node_FQDN*, Escriba el nombre de dominio completo del nodo de administración. (Si es

necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

   a. Seleccione **OK**.

9. En la ficha **firma**, especifique el certificado de firma para esta confianza de parte de confianza:

   a. Agregue el certificado personalizado:

      - Si posee el certificado de gestión personalizado cargado en StorageGRID, seleccione ese certificado.
      - Si no tiene el certificado personalizado, inicie sesión en el nodo de administrador, vaya al `/var/local/mgmt-api` directorio del nodo Admin y añada el `custom-server.crt` archivo de certificado.

        **Nota:** utilizando el certificado predeterminado del nodo de administración (`server.crt`) no es recomendable. Si falla el nodo de administración, el certificado predeterminado se regenerará al recuperar el nodo y deberá actualizar la confianza de la parte de confianza.

   b. Seleccione **aplicar** y seleccione **Aceptar**.

      Las propiedades de la parte de confianza se guardan y cierran.

10. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
11. Cuando haya terminado, vuelva a StorageGRID y pruebe todos los fideicomisos de las partes que dependan para confirmar que están configurados correctamente. Consulte Utilizar el modo de recinto de seguridad si desea obtener instrucciones.

#### Cree aplicaciones empresariales en Azure AD

Puede usar Azure AD para crear una aplicación empresarial para cada nodo de administrador del sistema.

**Lo que necesitará**

- Ha empezado a configurar el inicio de sesión único para StorageGRID y ha seleccionado **Azure** como tipo de SSO.
- **Modo Sandbox** está seleccionado en la página Single Sign-On de Grid Manager. Consulte Utilizar el modo de recinto de seguridad.
- Tiene el **Nombre de la aplicación de empresa** para cada nodo de administración de su sistema. Se pueden copiar estos valores de la tabla de detalles Admin Node en la página StorageGRID Single Sign-On.

> Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de aplicaciones empresariales en Azure Active Directory.
- Tiene una cuenta de Azure con una suscripción activa.
- Tiene uno de los siguientes roles en la cuenta de Azure: Administrador global, administrador de

aplicaciones de cloud, administrador de aplicaciones o propietario del director del servicio.

#### Acceda a Azure AD

1. Inicie sesión en el "Portal de Azure".
2. Vaya a. "Active Directory para Azure".
3. Seleccione "Aplicaciones de negocio".

#### Creación de aplicaciones empresariales y guardado de la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Azure en StorageGRID, debe utilizar Azure para crear una aplicación empresarial para cada nodo de administración. Copiará las URL de metadatos de federación de Azure y las pegará en los campos de la URL* de metadatos de Federación correspondientes de la página de inicio de sesión único de StorageGRID.

1. Repita los siguientes pasos para cada nodo de administrador.
   a. En el panel aplicaciones de Azure Enterprise, seleccione **Nueva aplicación**.
   b. Seleccione **Crear su propia aplicación**.
   c. Para el nombre, introduzca el **Nombre de la aplicación de empresa** que ha copiado de la tabla de detalles del nodo de administración en la página Inicio de sesión único de StorageGRID.
   d. Deje seleccionada la opción **integrar cualquier otra aplicación que no encuentre en la galería (no galería)**.
   e. Seleccione **Crear**.
   f. Seleccione el enlace **Get Started** en **2. Configure el cuadro de inicio de sesión único en** o seleccione el enlace **Single Sign-On** en el margen izquierdo.
   g. Seleccione el cuadro **SAML**.
   h. Copie la URL * metadatos de Federación de aplicaciones*, que puede encontrar en **Paso 3 Certificado de firma SAML**.
   i. Vaya a la página Inicio de sesión único de StorageGRID y pegue la dirección URL en el campo **URL** de metadatos de Federación que corresponda al **Nombre de aplicación de empresa** que ha utilizado.
2. Una vez que haya pegado una URL de metadatos de federación para cada nodo de administración y realizado todos los demás cambios necesarios en la configuración de SSO, seleccione **Guardar** en la página Inicio de sesión único de StorageGRID.

#### Descargue los metadatos de SAML para cada nodo de administración

Una vez guardada la configuración de SSO, puede descargar un archivo de metadatos SAML para cada nodo de administrador del sistema StorageGRID.

Repita estos pasos para cada nodo de administrador:

1. Inicie sesión en StorageGRID desde el nodo de administrador.
2. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
3. Seleccione el botón para descargar los metadatos de SAML de ese nodo de administración.
4. Guarde el archivo, que cargará en Azure AD.

#### Cargue metadatos de SAML en cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administrador de StorageGRID, siga estos pasos en Azure AD:

1. Vuelva al portal de Azure.
2. Repita estos pasos con cada aplicación de empresa:

   > Es posible que deba actualizar la página aplicaciones de empresa para ver las aplicaciones que ha agregado anteriormente en la lista.

   a. Vaya a la página Propiedades de la aplicación de empresa.
   b. Establezca **asignación requerida** en **no** (a menos que desee configurar las asignaciones por separado).
   c. Vaya a la página Single Sign-On.
   d. Complete la configuración de SAML.
   e. Seleccione el botón **Upload metadata file** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
   f. Después de cargar el archivo, seleccione **Guardar** y, a continuación, seleccione **X** para cerrar el panel. Volverá a la página Set up Single Sign-On with SAML.
3. Siga los pasos de Utilizar el modo de recinto de seguridad para probar cada aplicación.

#### Cree conexiones de proveedores de servicios (SP) en PingFederate

Puede utilizar PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración del sistema. Para acelerar el proceso, importe los metadatos SAML de StorageGRID.

**Lo que necesitará**

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **Ping federate** como tipo de SSO.
- **Modo Sandbox** está seleccionado en la página Single Sign-On de Grid Manager. Consulte Utilizar el modo de recinto de seguridad.
- Tiene el **ID de conexión SP** para cada nodo de administración de su sistema. Puede encontrar estos valores en la tabla de detalles Admin Nodes en la página StorageGRID Single Sign-On.
- Ha descargado los **metadatos SAML** de cada nodo de administración del sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Usted tiene lahttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["Guía de referencia del administrador"^] Para PingFederate Server. La documentación de PingFederate proporciona instrucciones detalladas paso a paso y explicaciones.
- Tiene el permiso Admin para PingFederate Server.

**Acerca de esta tarea**

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como un proveedor SSO para StorageGRID. Si está utilizando otra versión de PingFederate, puede que necesite adaptar estas instrucciones. Consulte la documentación de PingFederate Server para obtener instrucciones detalladas para su publicación.

#### Complete los requisitos previos en PingFederate

Antes de poder crear las conexiones SP que utilizará para StorageGRID, debe completar las tareas previas en PingFederate. Utilizará la información de estos requisitos previos al configurar las conexiones del SP.

##### Crear almacén de datos

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utilice los valores que utilizó cuando configurando la federación de identidades En StorageGRID.

- **Tipo**: Directorio (LDAP)
- **Tipo LDAP**: Active Directory
- **Nombre del atributo binario**: Introduzca **objectGUID** en la ficha atributos binarios LDAP exactamente como se muestra.

##### Crear validador de credenciales de contraseña

Si todavía no lo ha hecho, cree un validador de credencial de contraseña.

- **Tipo**: Validador de credenciales de nombre de usuario de LDAP
- **Almacén de datos**: Seleccione el almacén de datos que creó.
- **Search base**: Introduzca la información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda**: SAMAccountName=${username}
- **Ámbito**: Subárbol

##### Crear instancia de adaptador IDP[[instancia de adaptador]]

Si todavía no lo ha hecho, cree una instancia de adaptador de IDP.

1. Vaya a **autenticación** > **integración** > **Adaptadores IDP**.
2. Seleccione **Crear nueva instancia**.
3. En la ficha Tipo, seleccione **adaptador IDP de formulario HTML**.
4. En la ficha adaptador IDP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione la validador de credenciales de contraseña que haya creado.
6. En la ficha atributos del adaptador, seleccione el atributo **nombre de usuario** para **seudónimo**.
7. Seleccione **Guardar**.

##### Crear o importar un certificado de firma[[certificado de firma]]

Si todavía no lo ha hecho, cree o importe el certificado de firma.

1. Vaya a **Seguridad** > **claves y certificados de firma y descifrado**.
2. Cree o importe el certificado de firma.

#### Cree una conexión SP en PingFederate

Cuando crea una conexión del SP en PingFederate, importe los metadatos SAML que ha descargado de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos necesarios.

Debe crear una conexión de SP para cada nodo de administrador en su sistema de StorageGRID, de modo que los usuarios puedan iniciar sesión desde y hacia cualquier nodo de forma segura. Utilice estas instrucciones para crear la primera conexión del SP. A continuación, vaya a. Cree conexiones adicionales del SP para crear las conexiones adicionales que necesite.

### Elija el tipo de conexión del SP

1. Vaya a **aplicaciones** > **integración** > **conexiones SP**.
2. Seleccione **Crear conexión**.
3. Seleccione **no utilice una plantilla para esta conexión**.
4. Seleccione **Examinador SSO Profiles** y **SAML 2.0** como protocolo.

### Importe los metadatos de SP

1. En la ficha Importar metadatos, seleccione **Archivo**.
2. Seleccione el archivo de metadatos de SAML que descargó de la página de inicio de sesión único de StorageGRID para el nodo de administrador.
3. Revise el Resumen de metadatos y la información de la ficha Información general.

   El ID de entidad del partner y el nombre de conexión se establecen en el ID de conexión de StorageGRID SP. (Por ejemplo, 10.96.105.200-DC1-ADM1-105-200). La URL base es la IP del nodo de administrador de StorageGRID.

4. Seleccione **Siguiente**.

### Configure el SSO del explorador IDP

1. En la ficha SSO del explorador, seleccione **Configurar SSO del explorador**.
2. En la ficha Perfiles de SAML, seleccione las opciones **SSO iniciado por el SP**, **SLO inicial de SP**, **SSO iniciado por IDP** y **SLO iniciado por IDP**.
3. Seleccione **Siguiente**.
4. En la ficha ciclo de vida de las aserción, no realice cambios.
5. En la ficha creación de aserción, seleccione **Configurar creación de aserción**.
   a. En la ficha asignación de identidades, seleccione **Estándar**.
   b. En la ficha Contrato de atributo, utilice el formato **SAML_SUBJECT** como atributo Contract y el formato de nombre no especificado que se importó.
6. Para extender el contrato, seleccione **Eliminar** para eliminar `urn:oid`, que no se utiliza.

### Asigne la instancia del adaptador

1. En la ficha asignación de origen de autenticación, seleccione **asignar nueva instancia de adaptador**.
2. En la ficha instancias del adaptador, seleccione instancia del adaptador que haya creado.
3. En la ficha método de asignación, seleccione **recuperar atributos adicionales de un almacén de datos**.
4. En la ficha origen del atributo y Búsqueda del usuario, seleccione **Agregar origen del atributo**.
5. En la ficha almacén de datos, proporcione una descripción y seleccione almacén de datos usted agregó.

6. En la ficha Búsqueda de directorios LDAP:
   - Introduzca el **DN base**, que debe coincidir exactamente con el valor especificado en StorageGRID para el servidor LDAP.
   - Para el ámbito de búsqueda, seleccione **Subtree**.
   - Para la clase de objeto raíz, busque el atributo **objectGUID** y añádalo.
7. En la ficha tipos de codificación de atributos binarios LDAP , seleccione **Base64** para el atributo **objectGUID** .
8. En la ficha filtro LDAP, introduzca **sAMAccountName=${username}**.
9. En la ficha cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en la lista desplegable origen y seleccione **objectGUID** en la lista desplegable valor.
10. Revise y, a continuación, guarde el origen del atributo.
11. En la ficha origen del atributo Failsave, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **hecho**.
13. Seleccione **Listo**.

### Configure los ajustes de protocolo

1. En la ficha **Conexión SP** > **SSO del navegador** > **Configuración de protocolo**, seleccione **Configurar ajustes de protocolo**.
2. En la ficha URL del servicio de consumidor de aserción , acepte los valores predeterminados que se importaron desde los metadatos SAML de StorageGRID (**POST** para el enlace y. `/api/saml-response` Para la URL del extremo).
3. En la ficha direcciones URL del servicio SLO , acepte los valores predeterminados, que se importaron desde los metadatos SAML de StorageGRID (**REDIRECT** para el enlace y. `/api/saml-logout` Para la dirección URL del extremo.
4. En la ficha vinculaciones SAML permitidas, anule la selección de **ARTEFACTO** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la ficha Directiva de firma, deje las casillas de verificación **requerir firma de solicitudes** y **siempre firmar confirmación** activadas.
6. En la ficha Directiva de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **hecho** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **hecho** para guardar la configuración de SSO del explorador.

### Configurar credenciales

1. En la ficha Conexión SP, seleccione **credenciales**.
2. En la ficha credenciales, seleccione **Configurar credenciales**.
3. Seleccione la certificado de firma ha creado o importado.
4. Seleccione **Siguiente** para ir a **gestionar ajustes de verificación de firma**.
   a. En la ficha Modelo de confianza, seleccione **sin anclar**.
   b. En la pestaña Certificado de verificación de firma, revise la información de certificación de firma, que se importó de los metadatos SAML de StorageGRID.
5. Revise las pantallas de resumen y seleccione **Guardar** para guardar la conexión SP.

### Cree conexiones adicionales del SP

Puede copiar la primera conexión de SP para crear las conexiones de SP que necesita para cada nodo de administrador de su grid. Se cargan metadatos nuevos para cada copia.

> Las conexiones SP para diferentes nodos de administración utilizan valores idénticos, a excepción del ID de entidad del partner, la URL base, el ID de conexión, el nombre de conexión, la verificación de firma, Y URL de respuesta de SLO.

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Introduzca el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Elija el archivo de metadatos que corresponde al nodo de administración:
   a. Seleccione **Acción** > **Actualizar con metadatos**.
   b. Seleccione **elegir archivo** y cargue los metadatos.
   c. Seleccione **Siguiente**.
   d. Seleccione **Guardar**.
4. Resuelva el error debido al atributo no utilizado:
   a. Seleccione la nueva conexión.
   b. Seleccione **Configurar SSO del explorador > Configurar creación de aserción > Contrato de atributo**.
   c. Elimine la entrada para **urn:oid**.
   d. Seleccione **Guardar**.

### Desactive el inicio de sesión único

Si ya no desea usar esta funcionalidad, puede deshabilitar el inicio de sesión único (SSO). Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidades.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

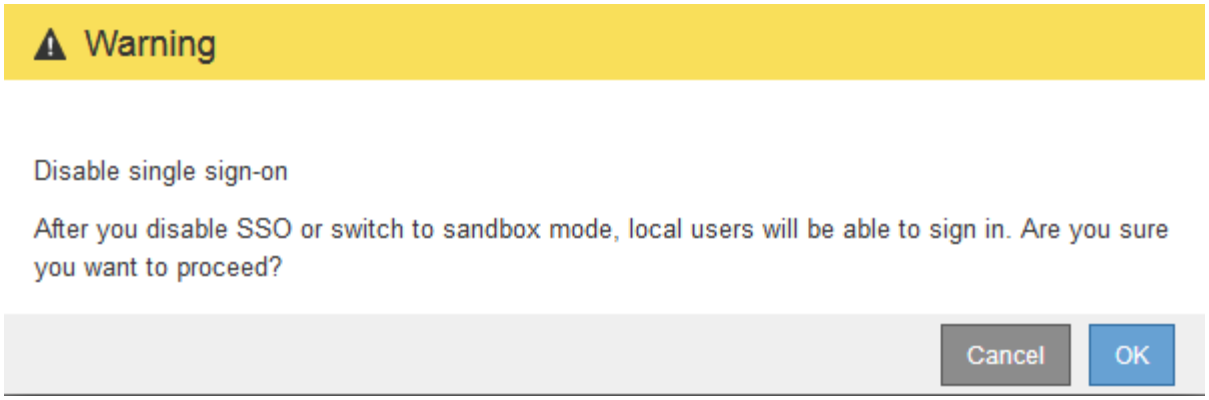
#### Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.

   Aparece la página Single Sign-On.

2. Seleccione la opción **Desactivado**.
3. Seleccione **Guardar**.

   Aparece un mensaje de advertencia que indica que los usuarios locales podrán iniciar sesión.




4. Seleccione **OK**.

   La próxima vez que inicie sesión en StorageGRID, aparecerá la página Inicio de sesión en StorageGRID, donde deberá introducir el nombre de usuario y la contraseña de un usuario de StorageGRID local o federado.

### Desactive y vuelva a habilitar temporalmente el inicio de sesión único para un nodo de administración

Es posible que no pueda iniciar sesión en Grid Manager si se desactiva el sistema de inicio de sesión único (SSO). En este caso, puede deshabilitar y volver a habilitar SSO para un nodo de administración. Para deshabilitar y, a continuación, volver a habilitar SSO, debe acceder al shell de comandos del nodo.

#### Lo que necesitará

- Tiene permisos de acceso específicos.
- Usted tiene la `Passwords.txt` archivo.
- Conoce la contraseña del usuario raíz local.

#### Acerca de esta tarea

Después de deshabilitar SSO para un nodo de administración, puede iniciar sesión en Grid Manager como usuario raíz local. Para proteger el sistema StorageGRID, tiene que utilizar el shell de comandos del nodo para volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.

> La deshabilitación de SSO para un nodo de administrador no afecta la configuración de SSO para ningún otro nodo de administrador que esté en el grid. La casilla de verificación **Activar SSO** de la página de inicio de sesión único de Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que se actualicen.

#### Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@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 `#`.

2. Ejecute el siguiente comando:`disable-saml`

   Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

3. Confirme que desea deshabilitar SSO.

   Un mensaje indica que el inicio de sesión único está deshabilitado en el nodo.

4. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.

   Ahora se muestra la página de inicio de sesión de Grid Manager porque SSO se ha desactivado.

5. Inicie sesión con la raíz del nombre de usuario y la contraseña del usuario raíz local.
6. Si deshabilitó temporalmente SSO debido a que debe corregir la configuración de SSO:
   a. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   b. Cambie la configuración incorrecta o obsoleta de SSO.
   c. Seleccione **Guardar**.

      Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a activar SSO automáticamente para toda la cuadrícula.

7. Si ha desactivado SSO temporalmente porque necesita acceder a Grid Manager por algún otro motivo:
   a. Realice cualquier tarea o tarea que necesite realizar.
   b. Seleccione **Cerrar sesión** y cierre Grid Manager.
   c. Vuelva a habilitar SSO en el nodo de administrador. Puede realizar cualquiera de los siguientes pasos:

      - Ejecute el siguiente comando: `enable-saml`

        Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

      Confirme que desea habilitar SSO.

   Un mensaje indica que el inicio de sesión único está habilitado en el nodo.

      - Reinicie el nodo de cuadrícula: `reboot`

8. Desde un explorador web, acceda a Grid Manager desde el mismo nodo de administración.
9. Confirme que aparece la página de inicio de sesión de StorageGRID y que debe introducir sus credenciales de SSO para acceder a Grid Manager.

# Administrar la configuración de seguridad

## Gestionar certificados

### Acerca de los 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 de servidor, que contiene una clave pública. El cliente verifica este certificado comparando 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 incluye una entidad de certificación (CA) integrada que genera un certificado de CA de grid interno durante la instalación del sistema. El certificado de CA de cuadrícula se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una entidad de certificación externa (CA) puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de su empresa. Aunque se puede utilizar el certificado de CA de cuadrícula para un entorno que no sea de producción, la práctica recomendada para un entorno de producción es utilizar certificados personalizados firmados por una entidad de certificación externa. Las conexiones no seguras que no tienen ningún certificado también se admiten, pero no se recomienda.

- Los certificados de CA personalizados no quitan 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 optimización del sistema para certificados de servidor.
- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).

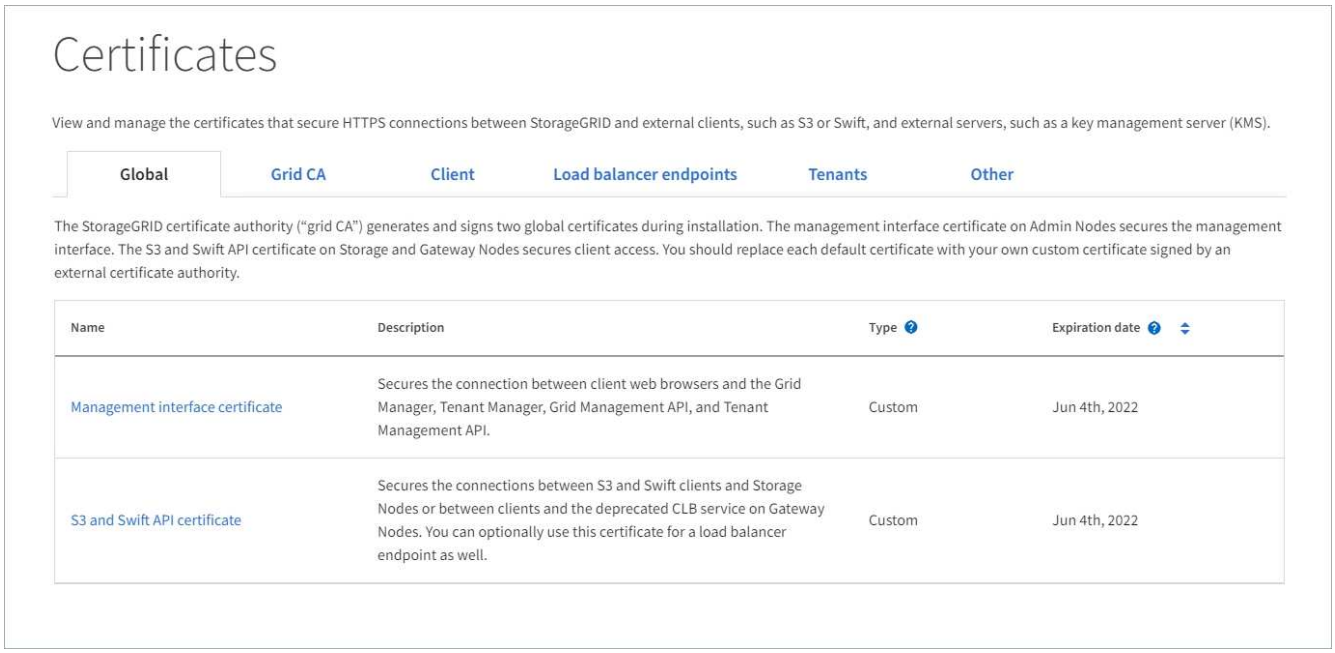
> StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

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.

1. En Grid Manager, seleccione **CONFIGURATON** > **Seguridad** > **certificados**.




2. Seleccione una ficha en la página certificados para obtener información sobre cada categoría de certificado y para acceder a la configuración de certificado. Sólo puede acceder a una ficha si tiene el permiso adecuado.

   - **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 del equilibrador de carga**: Protege las conexiones entre los clientes S3 y Swift 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 de API de S3 y Swift 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 explorador Web cliente a las interfaces de administración de StorageGRID.
- Certificado API S3 y Swift: Protege las conexiones API de cliente a los nodos de almacenamiento, los nodos de administración y los nodos de puerta de enlace, que las aplicaciones de cliente S3 y Swift 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 del administrador de grid y del administrador de inquilinos.
  - Reemplace el certificado API de S3 y Swift Se utiliza para conexiones de nodo de almacenamiento, servicio CLB (obsoleto) y extremo de equilibrador de carga (opcional).
- Restaure el certificado de interfaz de gestión predeterminado.
- Restaure el certificado API S3 y Swift 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 y Swift.

**CA de grid**

La Certificado de CA de grid, Generado por la autoridad de certificación 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.

Puede hacerlo Copie o descargue el certificado de Grid CA, pero no puede cambiarlo.

**Cliente**

Certificados de cliente, Generada por una autoridad de certificados externa, asegura las conexiones entre herramientas de supervisión externas y la base de datos Prometheus de StorageGRID.

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 hacerlo 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, Que cargue o genere, proteja las conexiones entre los clientes S3 y Swift y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración.

La tabla de extremo de equilibrador de carga tiene una fila para cada extremo de equilibrador de carga configurado e indica si se está utilizando el certificado API global S3 y Swift o un certificado de extremo de equilibrador de carga personalizado para el extremo. 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:

- Seleccione un nombre de extremo para abrir una ficha de explorador con información sobre el extremo de equilibrio de carga, incluidos los detalles de su certificado.
- Especifique un certificado de extremo de equilibrio de carga para FabricPool.
- Use el certificado global de la API de S3 y Swift en lugar de generar un nuevo certificado de extremo de equilibrio de carga.

**Clientes**

Los inquilinos pueden usar certificados de servidor de federación de identidades o. certificados de extremo de servicio de plataforma Para asegurar 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 federación de identidades
- Certificados de Cloud Storage Pool
- Certificados de servidor de gestión de claves (KMS)
- Certificados de inicio de sesión único
- Certificados de notificación de alertas por correo electrónico
- Certificados de servidor de syslog externos

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 dispone del permiso correspondiente.

Podrá:

- Ver y editar un certificado de federación de identidades
- Cargar certificados de servidor de gestión de claves (KMS) y de cliente
- Especifique un certificado de Cloud Storage Pool para S3, C2S S3 o Azure
- Especifique manualmente un certificado SSO para la confianza de la parte que confía
- Especifique un certificado para notificaciones de alertas por correo electrónico
- Especifique un certificado de servidor de syslog externo

#### Detalles del certificado de seguridad

A continuación se describe cada tipo de certificado de seguridad, con vínculos a artículos que contienen instrucciones de implementación.

### Certificado de interfaz de gestión

| Tipo de certificado | Descripción | Ubicación de navegación | Detalles |
|---|---|---|---|
| Servidor | 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.<br><br>Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos.<br><br>Puede usar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado. | **CONFIGURACIÓN** > **Seguridad** > **certificados**, seleccione la ficha **Global** y, a continuación, seleccione **Certificado de interfaz de administración** | Configure los certificados de interfaz de gestión |

**Certificado API S3 y Swift**

| Tipo de certificado | Descripción | Ubicación de navegación | Detalles |
|---|---|---|---|
| Servidor | Autentica conexiones de cliente S3 o Swift seguras con un nodo de almacenamiento, en el servicio Connection Load Balancer (CLB) obsoleto en un nodo de puerta de enlace y extremos de equilibrador de carga (opcional). | **CONFIGURATION** > **Security** > **Certificates**, seleccione la ficha **Global** y, a continuación, seleccione **S3 y Swift API Certificate** | Configure los certificados API S3 y Swift |

**Certificado de CA de grid**

Consulte Descripción de certificado de CA de cuadrícula predeterminada.

**Certificado de cliente de administrador**

| Tipo de certificado | Descripción | Ubicación de navegación | Detalles |
| --- | --- | --- | --- |
| Cliente | Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos.<br>• Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID.<br>• Permite una supervisión segura de StorageGRID mediante herramientas externas. | **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente** | Configurar certificados de cliente |

**Certificado de punto final de equilibrador de carga**

| Tipo de certificado | Descripción | Ubicación de navegación | Detalles |
| --- | --- | --- | --- |
| Servidor | Autentica la conexión entre clientes S3 o Swift y el servicio StorageGRID Load Balancer en nodos de puerta de enlace y nodos de administrador. 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.<br><br>También puede utilizar una versión personalizada del global Certificado API S3 y Swift Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar conexiones de equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada extremo de equilibrador de carga.<br><br>**Nota:** el certificado utilizado para la autenticación del equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID. | **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga** | • Configurar puntos finales del equilibrador de carga<br>• Cree un extremo de equilibrador de carga para FabricPool |

**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 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<br><br>Editar extremo de servicios de plataforma |

**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 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 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** > **Single Sign-On** | Configurar el inicio de sesión único |

**Certificado de notificación de alertas por correo electrónico**

| Tipo de certificado | Descripción | Ubicación de navegación | Detalles |
| --- | --- | --- | --- |
| Servidor y cliente | Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta.<br>• Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico.<br>• 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 | Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID.<br>**Nota:** no se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo. | **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog** y, a continuación, seleccione **Configurar servidor de syslog externo** | Configure un servidor de syslog externo |

#### 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 o Swift al extremo de equilibrio de carga y cargar el mismo certificado en el 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 verifica este certificado comparando 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.

## 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).

Para obtener más información sobre cómo protege StorageGRID las conexiones de cliente para la API DE REST, consulte Use S3 o. Use 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 asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor para la interfaz de administración** se activa cuando este certificado de servidor está a punto de caducar. 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 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:

- **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
- **IP**: Una o varias direcciones IP que se incluirán en el certificado.
- **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.

- **Días válidos**: Número de días después de la creación que expira el certificado.

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.

### 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 de 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.

**Lo que necesitará**

- Tiene 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 usa para conexiones de clientes S3 o Swift a nodos de almacenamiento, el servicio Connection Load Balancer

(CLB) obsoleto en los nodos de puerta de enlace o para cargar extremos de equilibrador. 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 asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor global para API de S3 y Swift** se activa cuando el certificado de servidor raíz está a punto de caducar. 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:
   - **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o varias direcciones IP que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
   - **Días válidos**: Número de días después de la creación que expira el certificado.

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

Es posible revertir a usar el certificado API S3 y Swift predeterminado para conexiones de clientes S3 y Swift a nodos de almacenamiento, así como el servicio CLB obsoleto en los nodos de puerta de enlace. Sin embargo, no puede utilizar el certificado API S3 y Swift predeterminado para un extremo de equilibrio 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 API global S3 y Swift, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar desde el sistema. El certificado API S3 y Swift predeterminado se utilizará para las conexiones de clientes S3 y Swift posteriores a los nodos de almacenamiento, así como para el servicio CLB obsoleto en los nodos de puerta de enlace.

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 S3
- Use Swift
- Configure los nombres de dominio de extremo API de 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.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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

## 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**

- Tiene 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.

> El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y 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 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 la información acerca de uso general de certificados de seguridad y.. configuración de certificados de servidor personalizados.

> Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad de certificados de cliente configurados en la página certificados** 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 cliente en la ficha Cliente.

Si usa un servidor de gestión de claves (KMS) para proteger los datos en los nodos de dispositivos especialmente configurados, consulte la información específica acerca de Cargando un certificado de cliente KMS.

**Lo que necesitará**

- Tiene permiso de acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un 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

Siga el procedimiento para agregar un certificado de cliente a su escenario:

- 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 Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.
4. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.
5. En la sección **Tipo de certificado**, cargue el certificado de interfaz de administración `.pem` archivo.
   a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
   b. Cargue el archivo de certificado de 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.

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

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

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

b. **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.

f. 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 más información sobre las métricas, consulte Instrucciones para supervisar StorageGRID.

### 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. Siga los pasos a. configure un certificado de interfaz de gestión.
2. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.
5. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.

6. En la sección **Tipo de certificado**, cargue el certificado de cliente, la clave privada y el paquete de CA `.pem` archivos:
   a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
   b. Cargue un certificado de cliente, una clave privada y archivos de 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.
7. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.
   a. **Nombre**: Escriba un nombre para la conexión.

      StorageGRID no requiere esta información, pero se debe proporcionar un nombre para probar la conexión.
   b. **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.
   f. 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 más información sobre las métricas, consulte Instrucciones para supervisar StorageGRID.

### 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 Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación,

seleccione la ficha **Cliente**.

2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.
4. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.
5. En la sección **Tipo de certificado**, seleccione **generar certificado**.
6. Especifique la información del certificado:
   - **Nombre de dominio**: Uno o más nombres de dominio completos del nodo de administración que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o más direcciones IP del nodo de administración que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
7. Seleccione **generar**.
8. 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.

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

   El nuevo certificado aparece en la ficha Cliente.

10. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Global**.
11. Seleccione **Certificado de interfaz de administración**.
12. Seleccione **utilizar certificado personalizado**.
13. 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.
    a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
    b. Cargue cada archivo de certificado (`.pem`).
    c. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

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

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

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

    b. **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 cliente de interfaz de gestión para **CA Cert** y **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.

    f. 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 más información sobre las métricas, consulte 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, a continuación, seleccione la ficha **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 que contenga al menos 1 y no más de 32 caracteres.
5. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, 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, a continuación, seleccione la ficha **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. Cargue el nombre de 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:

   - **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o varias direcciones IP que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
   - **Días válidos**: Número de días después de la creación que expira el certificado.

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, a continuación, seleccione la ficha **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. 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`

**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, a continuación, seleccione la ficha **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.

## Configuración de servidores de gestión de claves

### Configurar servidores de gestión de claves: Descripción general

Puede configurar uno o más servidores de gestión de claves externos (KMS) para proteger los datos en nodos de dispositivo especialmente configurados.

#### ¿Qué es un servidor de gestión de claves (KMS)?

Un servidor de gestión de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID en el sitio de StorageGRID asociado mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

Puede utilizar uno o varios servidores de gestión de claves para administrar las claves de cifrado de nodos para los nodos de dispositivo StorageGRID que tengan activada la configuración * cifrado de nodos* durante la instalación. El uso de servidores de gestión de claves con estos nodos de dispositivos le permite proteger los datos aunque se haya eliminado un dispositivo del centro de datos. Una vez que los volúmenes del dispositivo se han cifrado, no podrá acceder a ningún dato en el dispositivo a menos que el nodo se pueda comunicar con el KMS.

> StorageGRID no crea ni gestiona las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea usar un servidor de gestión de claves externo para proteger los datos StorageGRID, debe comprender cómo configurar ese servidor y debe comprender cómo gestionar las claves de cifrado. La realización de tareas de gestión de claves supera el alcance de estas instrucciones. Si necesita ayuda, consulte la documentación del servidor de gestión de claves o póngase en contacto con el soporte técnico.

### Consulte los métodos de cifrado de StorageGRID

StorageGRID proporciona una serie de opciones para cifrar datos. Debe revisar los métodos disponibles para determinar qué métodos cumplen sus requisitos de protección de datos.

La tabla proporciona un resumen de alto nivel de los métodos de cifrado disponibles en StorageGRID.

| Opción de cifrado | Cómo funciona | Se aplica a. |
| --- | --- | --- |
| Servidor de gestión de claves (KMS) en Grid Manager | Configure un servidor de administración de claves para el sitio StorageGRID (**CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**) y active el cifrado de nodos para el dispositivo. A continuación, un nodo de dispositivo se conecta al KMS para solicitar una clave de cifrado (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen. | Nodos de dispositivo con **cifrado de nodos** activado durante la instalación. Todos los datos del dispositivo están protegidos frente a la pérdida física o la eliminación del centro de datos.<br><br>La gestión de claves de cifrado con un KMS solo es compatible con los nodos de almacenamiento y los dispositivos de servicio. |
| Drive Security en SANtricity System Manager | Si la función Drive Security está habilitada para un dispositivo de almacenamiento, es posible usar SANtricity System Manager para crear y gestionar la clave de seguridad. Se requiere la clave para acceder a los datos en las unidades seguras. | Dispositivos de almacenamiento con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. No se puede utilizar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio.<br><br>• Dispositivos de almacenamiento SG6000<br>• Dispositivos de almacenamiento SG5700<br>• Dispositivos de almacenamiento SG5600 |
| Opción de cuadrícula de cifrado de objetos almacenados | La opción **cifrado de objetos almacenados** se puede activar en Grid Manager (**CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**). Cuando se habilita esta opción, todos los objetos nuevos que no se cifran a nivel de bloque o de objeto se cifran durante el procesamiento. | Datos de objetos S3 y Swift recientemente procesados.<br><br>Los objetos almacenados existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran.<br><br>• Configurar el cifrado de objetos almacenados |

| Opción de cifrado | Cómo funciona | Se aplica a. |
| --- | --- | --- |
| Cifrado de bloques de S3 | Se emite una solicitud DE cifrado PUT Bucket para habilitar el cifrado en el bloque. Los objetos nuevos que no se cifren en el nivel de objeto se cifran durante el procesamiento. | Solo datos de objetos S3 procesados recientemente.<br><br>Debe especificarse el cifrado para el bloque. Los objetos de bloque existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran.<br><br>• Use S3 |
| Cifrado del lado del servidor de objetos S3 (SSE) | Se emite una solicitud de S3 para almacenar un objeto e incluir el `x-amz-server-side-encryption` solicite el encabezado. | Solo datos de objetos S3 procesados recientemente.<br><br>Se debe especificar el cifrado para el objeto. Los metadatos de objetos y otros datos confidenciales no se cifran.<br><br>StorageGRID gestiona las claves.<br><br>• Use S3 |
| Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C) | Se emite una solicitud S3 para almacenar un objeto e incluir tres encabezados de solicitud.<br><br>• `x-amz-server-side-encryption-customer-algorithm`<br>• `x-amz-server-side-encryption-customer-key`<br>• `x-amz-server-side-encryption-customer-key-MD5` | Solo datos de objetos S3 procesados recientemente.<br><br>Se debe especificar el cifrado para el objeto. Los metadatos de objetos y otros datos confidenciales no se cifran.<br><br>Las claves se gestionan fuera de StorageGRID.<br><br>• Use S3 |
| Cifrado de volúmenes o almacenes de datos externos | Si la plataforma de implementación lo admite, puede utilizar un método de cifrado fuera de StorageGRID para cifrar un volumen o almacén de datos completo. | Todos los datos de objetos, metadatos y datos de configuración del sistema, suponiendo que se cifre cada volumen o almacén de datos.<br><br>Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados. |

| Opción de cifrado | Cómo funciona | Se aplica a. |
| --- | --- | --- |
| Cifrado de objetos fuera de StorageGRID | Se utiliza un método de cifrado fuera de StorageGRID para cifrar los metadatos y los datos de objetos antes de que se ingieran en StorageGRID. | Solo datos de objetos y metadatos (los datos de configuración del sistema no están cifrados).<br><br>Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados.<br><br>• "Amazon simple Storage Service - Guía para desarrolladores: Protección de datos mediante cifrado en el cliente" |

#### Utilice varios métodos de cifrado

En función de los requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

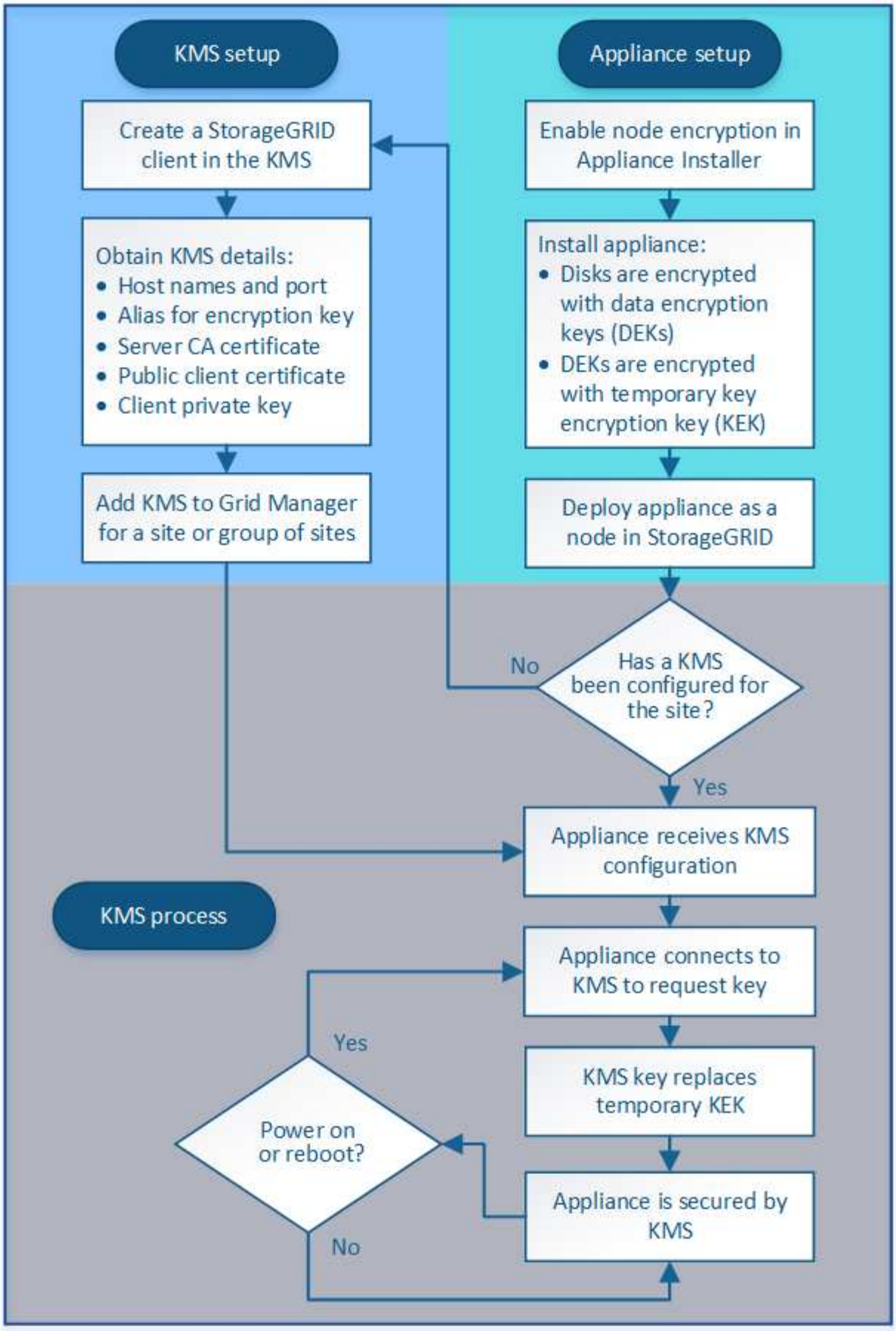
- Puede utilizar un KMS para proteger los nodos de dispositivos y también para usar la función de seguridad de unidades de System Manager de SANtricity a fin de «doble cifrado» de datos de las unidades de autocifrado de los mismos dispositivos.
- Puede usar un KMS para proteger los datos en los nodos del dispositivo y también puede usar la opción de cuadrícula de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de los objetos requiere cifrado, considere la posibilidad de controlar el cifrado en el nivel de bloque o de objeto individual. Habilitar varios niveles de cifrado tiene un coste de rendimiento adicional.

### Información general de la configuración de KMS y dispositivos

Antes de poder usar un servidor de gestión de claves (KMS) para proteger los datos de StorageGRID en los nodos de los dispositivos, debe completar dos tareas de configuración: Configurar uno o más servidores KMS y habilitar el cifrado de nodos de los nodos de los dispositivos. Cuando estas dos tareas de configuración se completan, el proceso de gestión de claves se realiza de forma automática.

El diagrama de flujo muestra los pasos de alto nivel para usar un KMS para proteger los datos de StorageGRID en los nodos de los dispositivos.




El diagrama de flujo muestra la configuración de KMS y la configuración de dispositivos que se producen en

paralelo; sin embargo, puede configurar los servidores de gestión de claves antes o después de habilitar el cifrado de nodos para los nodos de la aplicación nuevos, en función de sus requisitos.

#### Configurar el servidor de gestión de claves (KMS)

La configuración de un servidor de gestión de claves incluye los siguientes pasos de alto nivel.

| Paso | Consulte |
|---|---|
| Acceda al software KMS y añada un cliente para StorageGRID a cada clúster KMS o KMS. | Configure StorageGRID como cliente en KMS |
| Obtenga la información necesaria para el cliente StorageGRID en el KMS. | Configure StorageGRID como cliente en KMS |
| Agregue el KMS al Gestor de cuadrícula, asígnelo a un único sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración de KMS. | Añadir un servidor de gestión de claves (KMS) |

#### Configure el aparato

La configuración de un nodo de dispositivo para el uso de KMS incluye los siguientes pasos de alto nivel.

1. Durante la fase de configuración de hardware de la instalación del dispositivo, utilice el instalador del dispositivo StorageGRID para activar el ajuste **cifrado de nodos** del dispositivo.

   > No puede activar el ajuste **cifrado de nodos** después de agregar un dispositivo a la cuadrícula y no puede utilizar la administración de claves externa para dispositivos que no tienen el cifrado de nodos activado.

2. Ejecute el instalador del dispositivo StorageGRID. Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen de la cabina, como se indica a continuación:
   - Los depósitos se utilizan para cifrar los datos en cada volumen. Estas claves se generan utilizando el cifrado de disco de Linux Unified Key Setup (LUKS) en el sistema operativo del dispositivo y no se pueden cambiar.
   - Cada DEK individual se cifra mediante una clave de cifrado de clave maestra (KEK). El KEK inicial es una clave temporal que cifra los depósitos hasta que el dispositivo pueda conectarse al KMS.
3. Añada el nodo del dispositivo a StorageGRID.

Si quiere más información, consulte lo siguiente:

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

#### Proceso de cifrado de gestión de claves (se produce automáticamente)

El cifrado de gestión de claves incluye los siguientes pasos de alto nivel que se realizan automáticamente.

1. Al instalar un dispositivo con el cifrado de nodos activado en la cuadrícula, StorageGRID determina si existe una configuración KMS para el sitio que contiene el nodo nuevo.
   - Si ya se ha configurado un KMS para el sitio, el dispositivo recibe la configuración de KMS.
   - Si aún no se ha configurado un KMS para el sitio, el KEK temporal continúa encriptado los datos del dispositivo hasta que configura un KMS para el sitio y el dispositivo recibe la configuración de KMS.
2. El dispositivo usa la configuración KMS para conectarse al KMS y solicitar una clave de cifrado.
3. El KMS envía una clave de cifrado al dispositivo. La nueva clave del KMS sustituye al KEK temporal y ahora se utiliza para cifrar y descifrar los depósitos de los volúmenes del dispositivo.

> Los datos que existan antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifran con una clave temporal. Sin embargo, los volúmenes de los dispositivos no se deben considerar protegidos de la eliminación del centro de datos hasta que la clave temporal se sustituya por la clave de cifrado KMS.

4. Si el dispositivo está encendido o reiniciado, se vuelve a conectar con el KMS para solicitar la clave. La tecla, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o un reinicio.

**Consideraciones y requisitos para usar un servidor de gestión de claves**

## Antes de configurar un servidor de gestión de claves (KMS) externo, debe comprender las consideraciones y los requisitos.

#### ¿Cuáles son los requisitos de KMIP?

StorageGRID admite la versión KMIP 1.4.

"Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID admite los siguientes cifrados TLS v1.2 para KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Debe asegurarse de que cada nodo de dispositivo que utilice cifrado de nodo tenga acceso de red al clúster KMS o KMS configurado para el sitio.

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comunique a través del puerto que se utiliza para las comunicaciones del protocolo de interoperabilidad de gestión de claves (KMIP). El puerto KMIP predeterminado es 5696.

#### ¿Qué dispositivos son compatibles?

Puede usar un servidor de administración de claves (KMS) para administrar las claves de cifrado de cualquier dispositivo StorageGRID de la cuadrícula que tenga activada la configuración **cifrado de nodos**. Este ajuste solo se puede habilitar durante la fase de configuración de hardware de la instalación del dispositivo mediante el instalador de StorageGRID Appliance.

> No se puede habilitar el cifrado de nodos después de que se añade un dispositivo a la cuadrícula y no se puede usar la gestión de claves externa en los dispositivos que no tienen el cifrado de nodos habilitado.

Puede usar el KMS configurado para los siguientes dispositivos StorageGRID y nodos de dispositivos:

| Dispositivo | Tipo de nodo |
|---|---|
| Aplicación de servicios SG1000 | El nodo de administrador o el nodo de puerta de enlace |
| Servicio de atención al cliente SG100 | El nodo de administrador o el nodo de puerta de enlace |
| Dispositivo de almacenamiento SG6000 | Nodo de almacenamiento |
| Dispositivo de almacenamiento SG5700 | Nodo de almacenamiento |
| Dispositivo de almacenamiento SG5600 | Nodo de almacenamiento |

No puede usar el KMS configurado para nodos basados en software (sin dispositivo), incluidos los siguientes:

- Nodos puestos en marcha como máquinas virtuales (VM)
- Nodos implementados en motores de contenedor en hosts Linux

Los nodos puestos en marcha en estas otras plataformas pueden utilizar el cifrado fuera de StorageGRID a nivel de almacén de datos o disco.

#### ¿Cuándo se deben configurar los servidores de gestión de claves?

Para una instalación nueva, normalmente debe configurar uno o más servidores de gestión de claves en Grid Manager antes de crear inquilinos. Este orden garantiza que los nodos estén protegidos antes de que se almacenen datos de objeto en ellos.

Puede configurar los servidores de gestión de claves en Grid Manager antes o después de instalar los nodos de dispositivo.

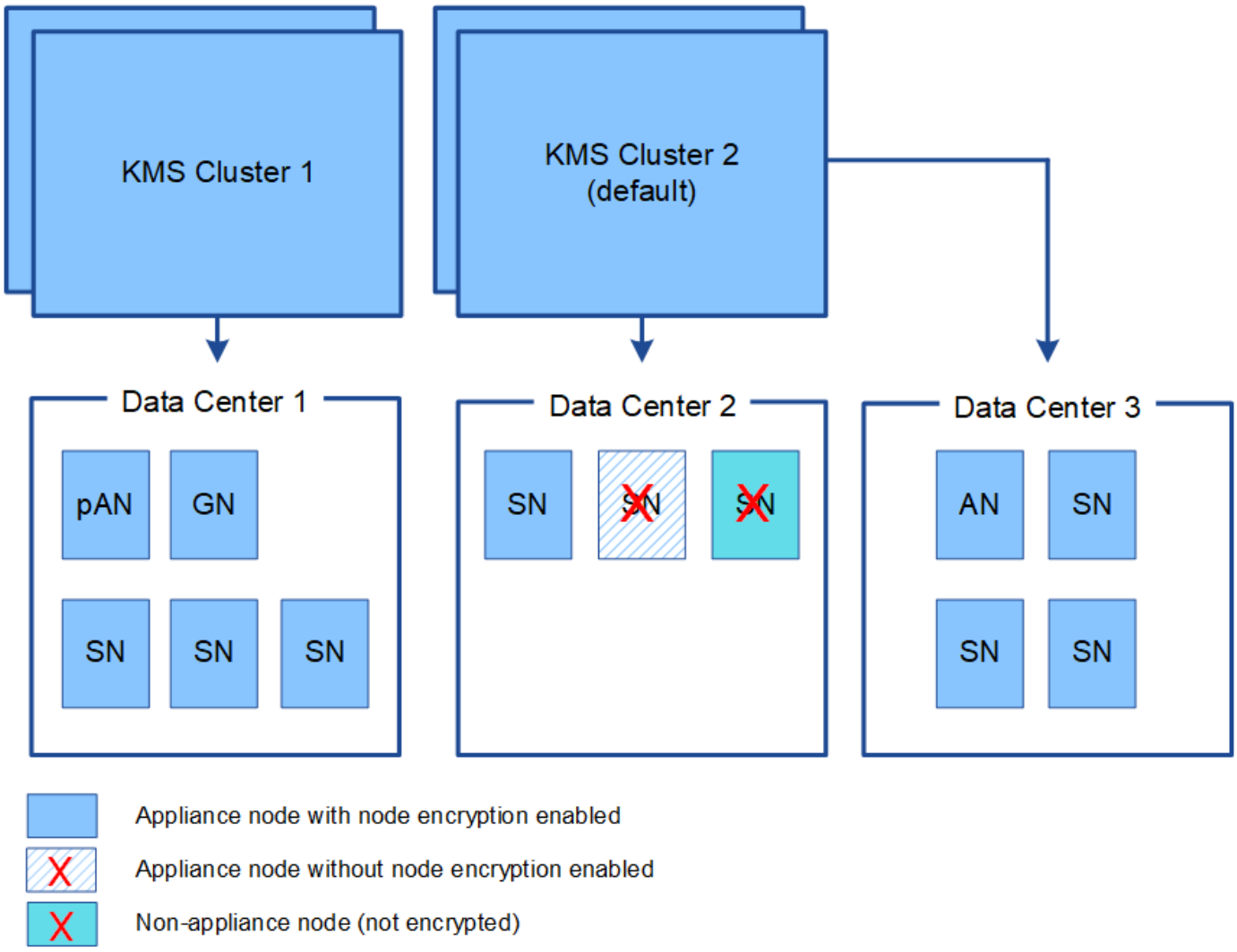
#### ¿Cuántos servidores de gestión de claves necesito?

Puede configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de dispositivos en el sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de dispositivos StorageGRID en un único sitio o a un grupo de sitios.

StorageGRID admite el uso de clústeres KMS. Cada clúster de KMS contiene varios servidores de gestión de claves replicados que comparten configuraciones de configuración y claves de cifrado. Se recomienda usar clústeres KMS para la gestión de claves porque mejora las funcionalidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supongamos que el sistema StorageGRID tiene tres sitios de centro de datos. Podría configurar un clúster KMS para proporcionar una clave a todos los nodos de dispositivos en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos de dispositivos de los demás sitios. Al agregar el segundo clúster KMS, puede configurar un KMS predeterminado para el Centro de datos 2 y el Centro de datos 3.

Tenga en cuenta que no puede utilizar KMS para nodos que no son de dispositivo ni para los que no tenían activada la configuración de **cifrado de nodos** durante la instalación.




**¿Qué ocurre cuando se gira una clave?**

Como práctica recomendada para la seguridad, debe girar periódicamente la clave de cifrado utilizada por cada KMS configurado.

Al girar la clave de cifrado, utilice el software KMS para pasar de la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.

> Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS en el Gestor de cuadrícula. En su lugar, gire la clave actualizando la versión de la clave en el software KMS. Utilice el mismo alias de clave para las claves nuevas que se usaron para las claves anteriores. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.

Cuando la nueva versión de clave esté disponible:

- Se distribuye automáticamente a los nodos de dispositivos cifrados del sitio o de los sitios asociados con el KMS. La distribución debe producirse dentro de una hora a partir de la cual se gira la clave.
- Si el nodo de dispositivo cifrado está sin conexión cuando se distribuye la nueva versión de clave, el nodo recibirá la nueva clave en cuanto se reinicie.

- Si la nueva versión de clave no se puede utilizar para cifrar los volúmenes del dispositivo por cualquier motivo, se activa la alerta **error de rotación de clave de cifrado KMS** para el nodo del dispositivo. Es posible que deba ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

#### ¿Puedo reutilizar un nodo de dispositivo después de cifrar?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID, primero debe retirar el nodo grid para mover los datos del objeto a otro nodo. A continuación, puede usar el instalador del dispositivo StorageGRID para borrar la configuración de KMS. Al borrar la configuración KMS se deshabilita la configuración **cifrado de nodos** y se elimina la asociación entre el nodo del dispositivo y la configuración KMS del sitio StorageGRID.

> Sin acceso a la clave de cifrado KMS, no se puede acceder a los datos que queden en el dispositivo y queden bloqueados de forma permanente.

**Información relacionada**

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

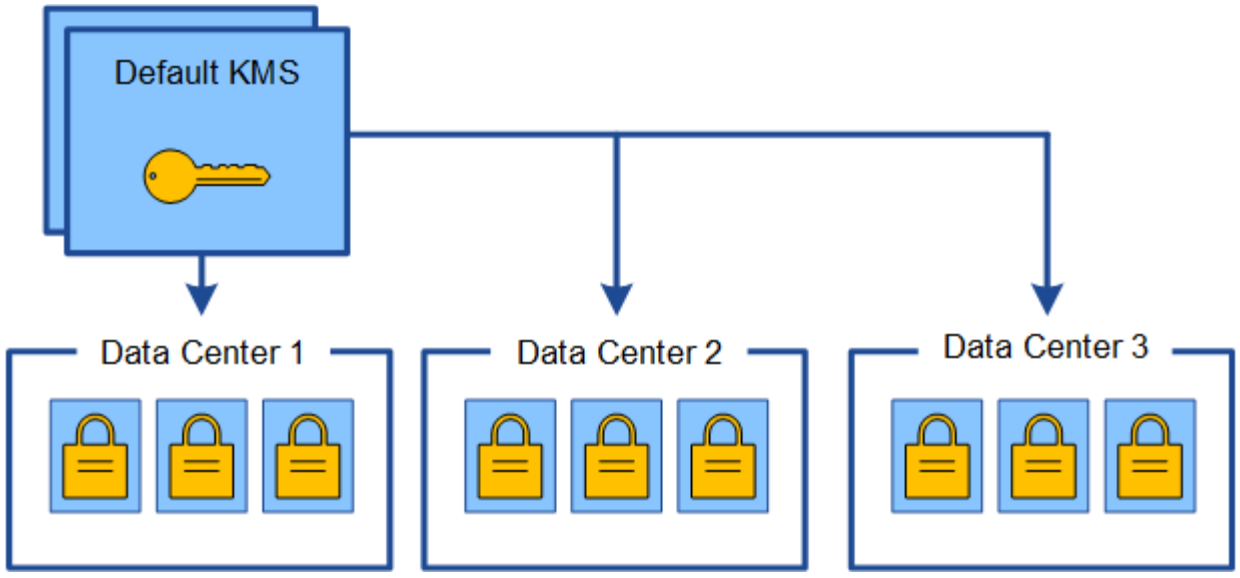
### Consideraciones para cambiar el KMS de un sitio

Cada servidor de gestión de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos de dispositivos en un único sitio o en un grupo de sitios. Si necesita cambiar qué KMS se utiliza para un sitio, es posible que necesite copiar la clave de cifrado de un KMS a otro.

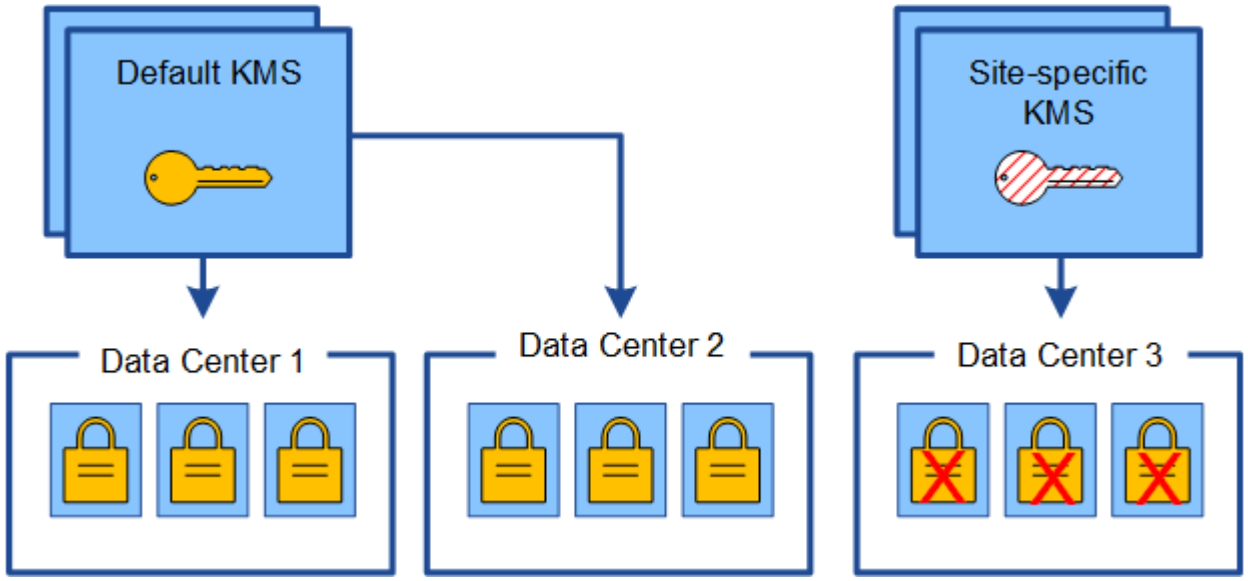
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original al KMS nuevo. Debe asegurarse de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

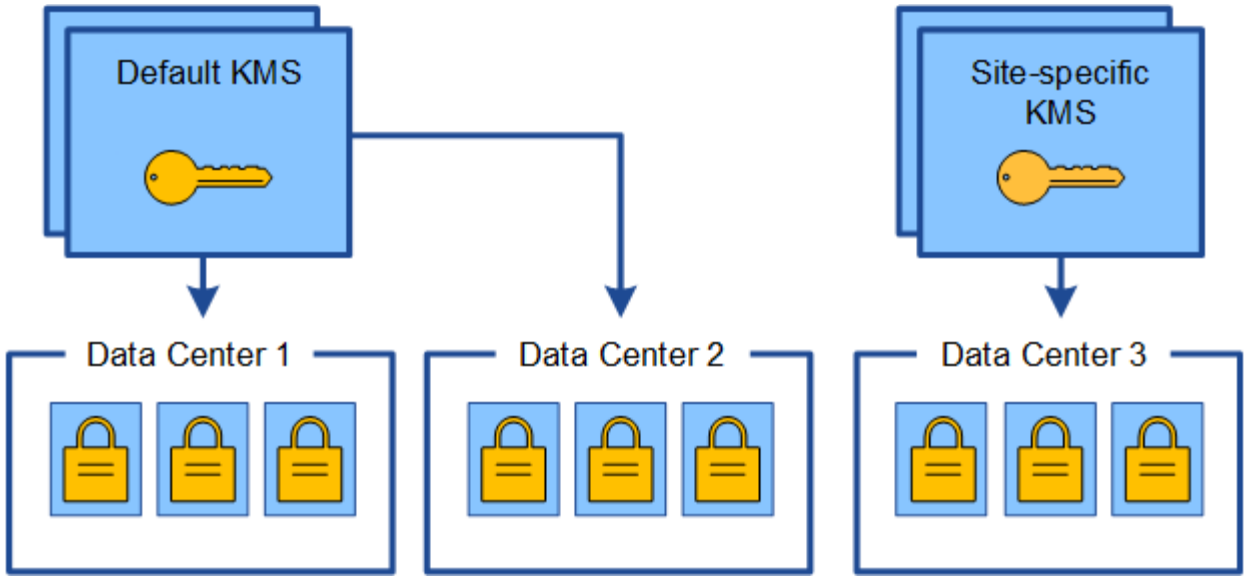
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar esos dispositivos.




3. Decide agregar un KMS específico de un sitio para un sitio (Data Center 3 en la figura). Sin embargo, como los nodos del dispositivo ya están cifrados, se produce un error de validación cuando se intenta guardar la configuración para el KMS específico del sitio. El error se produce porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos en ese sitio.




4. Para solucionar el problema, copia la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, copia la clave original en una nueva clave con el mismo alias. La clave original se convierte en una versión anterior de la clave nueva). El KMS específico del sitio tiene ahora la clave correcta para descifrar los nodos del dispositivo en el centro de datos 3, para que se puedan guardar en StorageGRID.




**Utilice casos para cambiar qué KMS se utiliza para un sitio**

La tabla resume los pasos necesarios para los casos más comunes para cambiar el KMS de un sitio.

| Caso de uso para cambiar el KMS de un sitio | Pasos requeridos |
|---|---|
| Tiene una o más entradas KMS específicas del sitio y desea usar una de ellas como KMS predeterminado. | Edite el KMS específico del sitio. En el campo **administra claves para**, seleccione **Sitios no administrados por otro KMS (KMS predeterminado)**. El KMS específico del sitio se utilizará ahora como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado.<br><br>Editar un servidor de gestión de claves (KMS) |
| Tiene un KMS predeterminado y agrega un sitio nuevo en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio. | 1. Si los nodos del dispositivo en el sitio nuevo ya han sido cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un KMS nuevo.<br>2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio.<br><br>Añadir un servidor de gestión de claves (KMS) |

| Caso de uso para cambiar el KMS de un sitio | Pasos requeridos |
| --- | --- |
| Desea que el KMS para un sitio utilice un servidor diferente. | 1. Si los nodos del dispositivo del sitio ya han sido cifrados por el KMS existente, use el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al KMS nuevo.<br>2. Con el Administrador de cuadrícula, edite la configuración de KMS existente e introduzca el nuevo nombre de host o la dirección IP.<br><br>Añadir un servidor de gestión de claves (KMS) |

### Configure StorageGRID como cliente en KMS

Debe configurar StorageGRID como cliente para cada servidor de gestión de claves externo o clúster de KMS antes de poder añadir el KMS a StorageGRID.

#### Acerca de esta tarea

Estas instrucciones se aplican a Thales CipherTrust Manager k170v, versiones 2.0, 2.1 y 2.2. Si tiene preguntas sobre el uso de un servidor de gestión de claves diferente con StorageGRID, póngase en contacto con el soporte técnico.

"Thales CipherTrust Manager"

#### Pasos

1. Desde el software KMS, cree un cliente StorageGRID para cada clúster KMS o KMS que vaya a utilizar.

   Cada KMS gestiona una única clave de cifrado para los nodos de dispositivos StorageGRID en un único sitio o en un grupo de sitios.

2. Desde el software KMS, cree una clave de cifrado AES para cada clúster KMS o KMS.

   La clave de cifrado debe ser exportable.

3. Registre la siguiente información de cada clúster KMS o KMS.

   Necesitará esta información cuando agregue el KMS a StorageGRID.

   - Nombre de host o dirección IP para cada servidor.
   - Puerto KMIP utilizado por el KMS.
   - Alias de clave para la clave de cifrado del KMS.

   > La clave de cifrado ya debe existir en el KMS. StorageGRID no crea ni gestiona claves KMS.

4. Para cada clúster de KMS o KMS, obtenga un certificado de servidor firmado por una entidad de certificación (CA) o un paquete de certificado que contiene cada uno de los archivos de certificado de CA codificados con PEM, concatenado en el orden de la cadena de certificados.

   El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

- El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.
- El campo Nombre alternativo del asunto (SAN) de cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que se conectará StorageGRID.

  > Al configurar el KMS en StorageGRID, debe introducir las mismas FQDN o direcciones IP en el campo **Nombre de host**.

- El certificado de servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que suele utilizar el puerto 5696.

5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada del certificado de cliente.

   El certificado de cliente permite que StorageGRID se autentique en el KMS.

### Añadir un servidor de gestión de claves (KMS)

## Utilice el asistente del servidor de gestión de claves de StorageGRID para agregar cada clúster KMS o KMS.

**Lo que necesitará**

- Ha revisado el consideraciones y requisitos para usar un servidor de gestión de claves.
- Ya tienes Se ha configurado StorageGRID como cliente en el KMSY tiene la información necesaria para cada clúster KMS o KMS.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

**Acerca de esta tarea**

Si es posible, configure cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS. Si crea el KMS predeterminado primero, todos los dispositivos cifrados por nodo de la cuadrícula se cifrarán con el KMS predeterminado. Si desea crear más tarde un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulte Consideraciones para cambiar el KMS de un sitio para obtener más detalles.

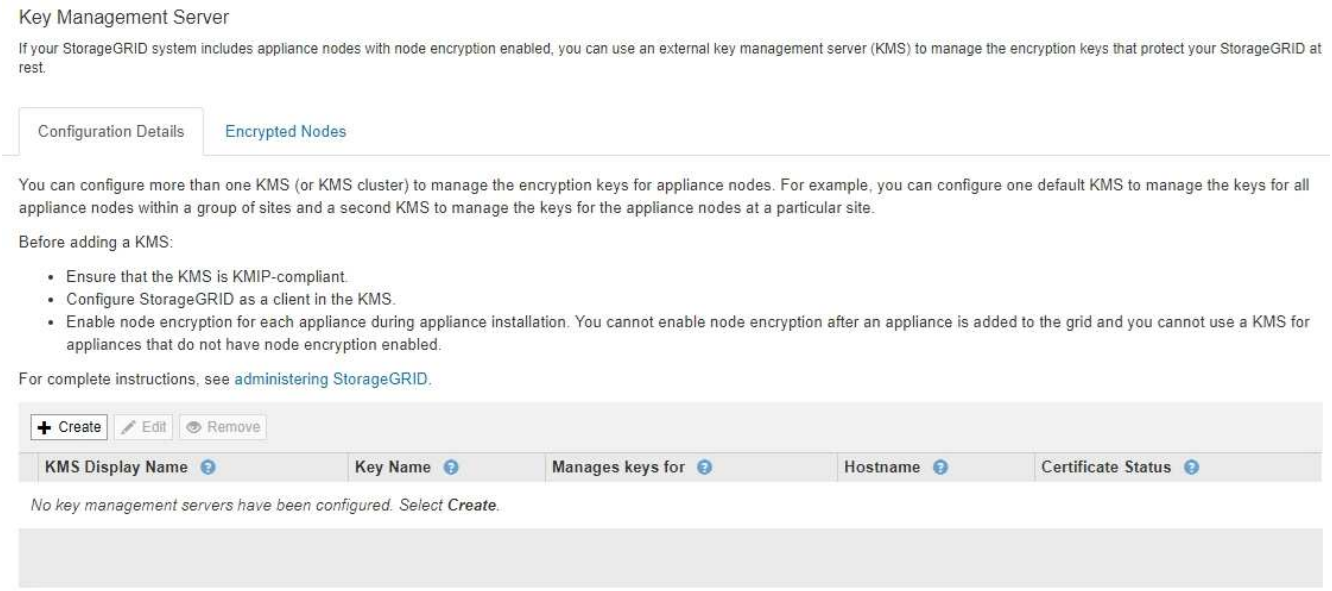
#### Paso 1: Introduzca los detalles de KMS

En el paso 1 (introducir detalles de KMS) del asistente para agregar un servidor de administración de claves, se proporcionan detalles sobre el clúster KMS o KMS.

**Pasos**

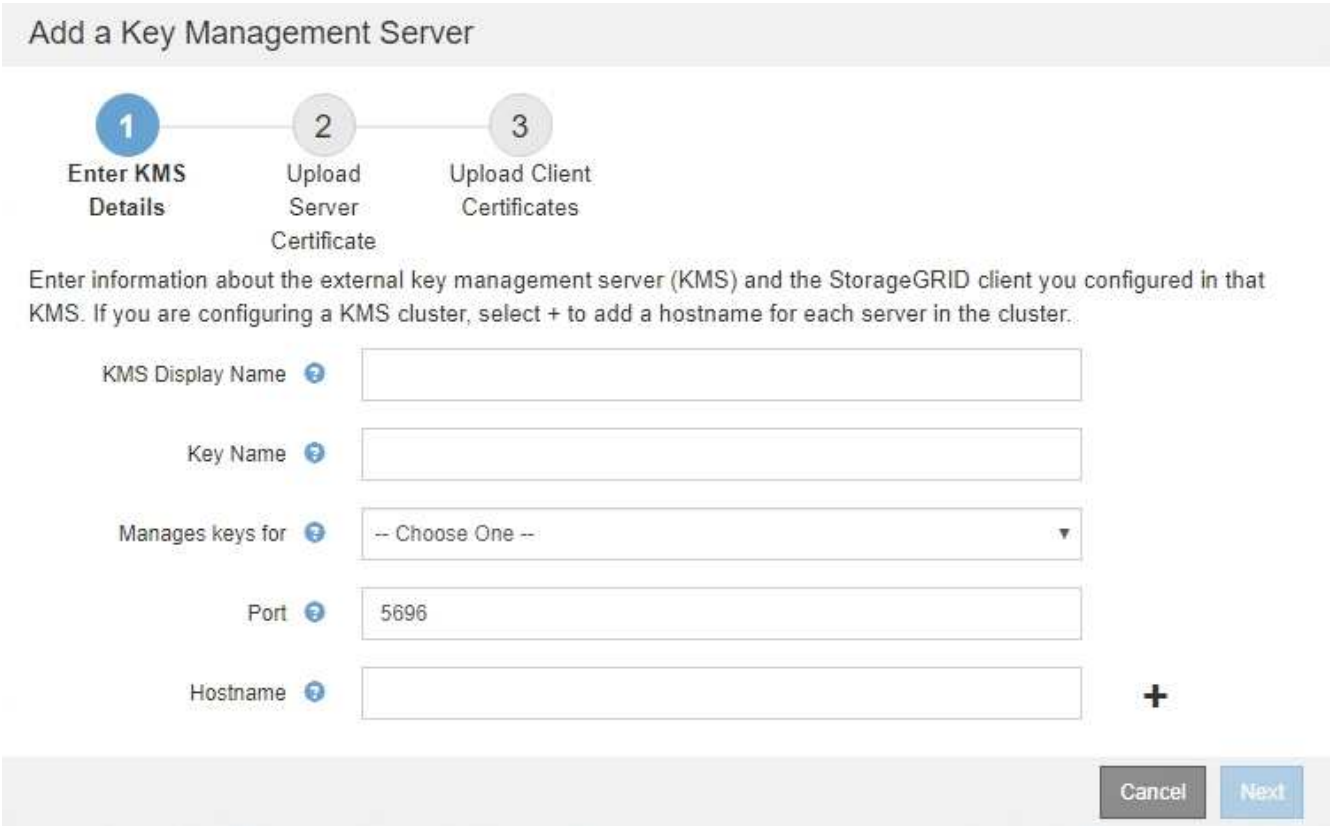
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.




2. Seleccione **Crear**.

   Paso 1 (introducir detalles de KMS) del asistente Añadir un servidor de gestión de claves aparece.




3. Introduzca la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

| Campo | Descripción |
|---|---|
| Nombre de visualización DE KMS | Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres. |

| Campo | Descripción |
| --- | --- |
| Nombre de la clave | El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. |
| Administra claves para | El sitio StorageGRID que se asociará a este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS.<br>• Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos en un sitio específico.<br>• Seleccione **Sitios no administrados por otro KMS (KMS predeterminado)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que agregue en expansiones posteriores.<br>**Nota:** se producirá Un error de validación al guardar la configuración de KMS si selecciona un sitio que anteriormente estaba cifrado por el KMS predeterminado pero no proporciona la versión actual de la clave de cifrado original al nuevo KMS. |
| Puerto | El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP. |
| Nombre del hostl | El nombre de dominio completo o la dirección IP del KMS.<br>**Nota:** el campo SAN del certificado de servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS. |

4. Si va a utilizar un clúster de KMS, seleccione el signo más ➕ para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **Siguiente**.

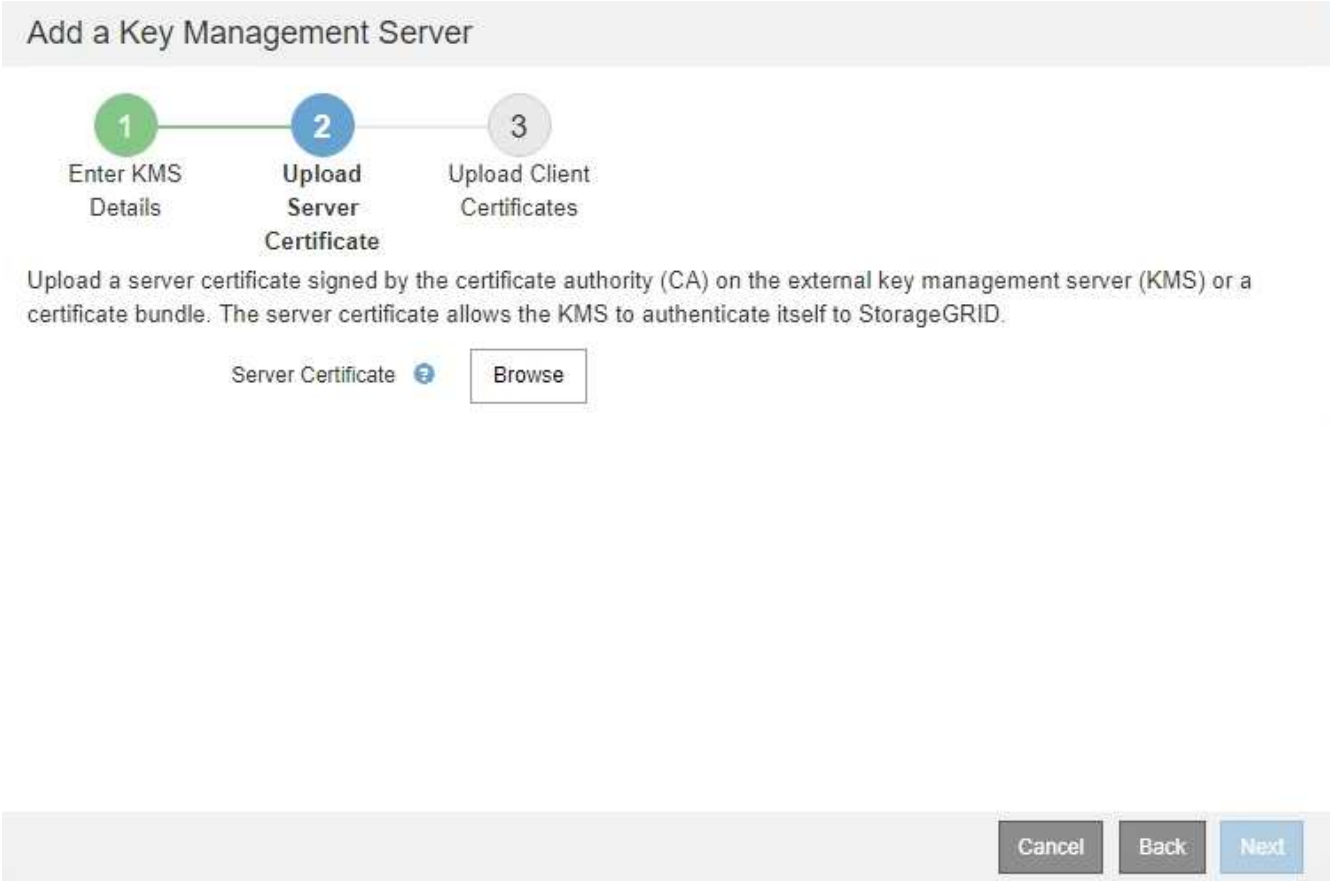
#### Paso 2: Cargar certificado de servidor

En el paso 2 (cargar certificado de servidor) del asistente Agregar un servidor de gestión de claves, carga el certificado de servidor (o el paquete de certificados) para el KMS. El certificado de servidor permite que el

KMS externo se autentique en StorageGRID.

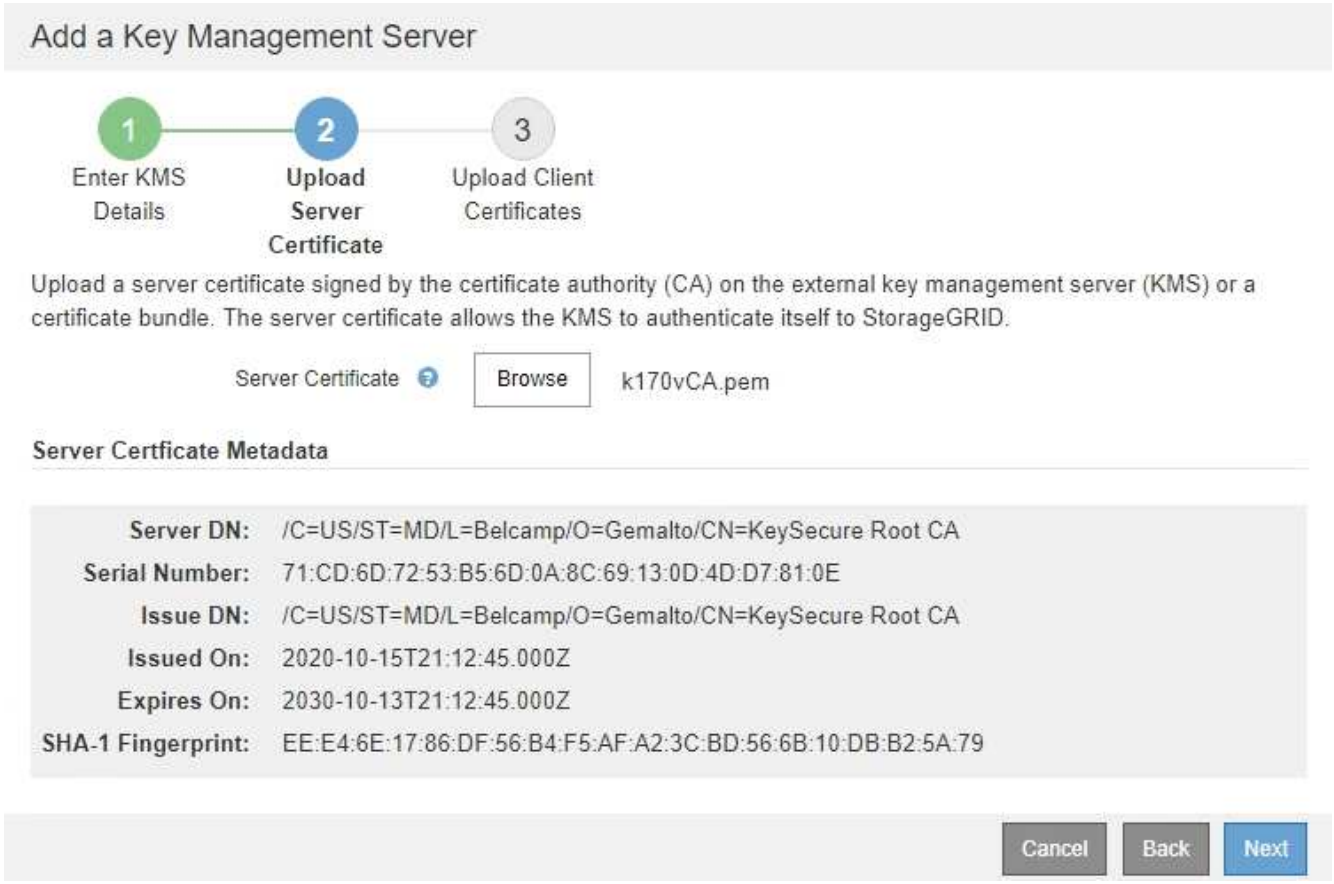
**Pasos**

1. Desde **Paso 2 (cargar certificado de servidor)**, vaya a la ubicación del certificado de servidor o del paquete de certificados guardados.




2. Cargue el archivo de certificado.

   Se muestran los metadatos del certificado del servidor.




Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en la pestaña correspondiente.

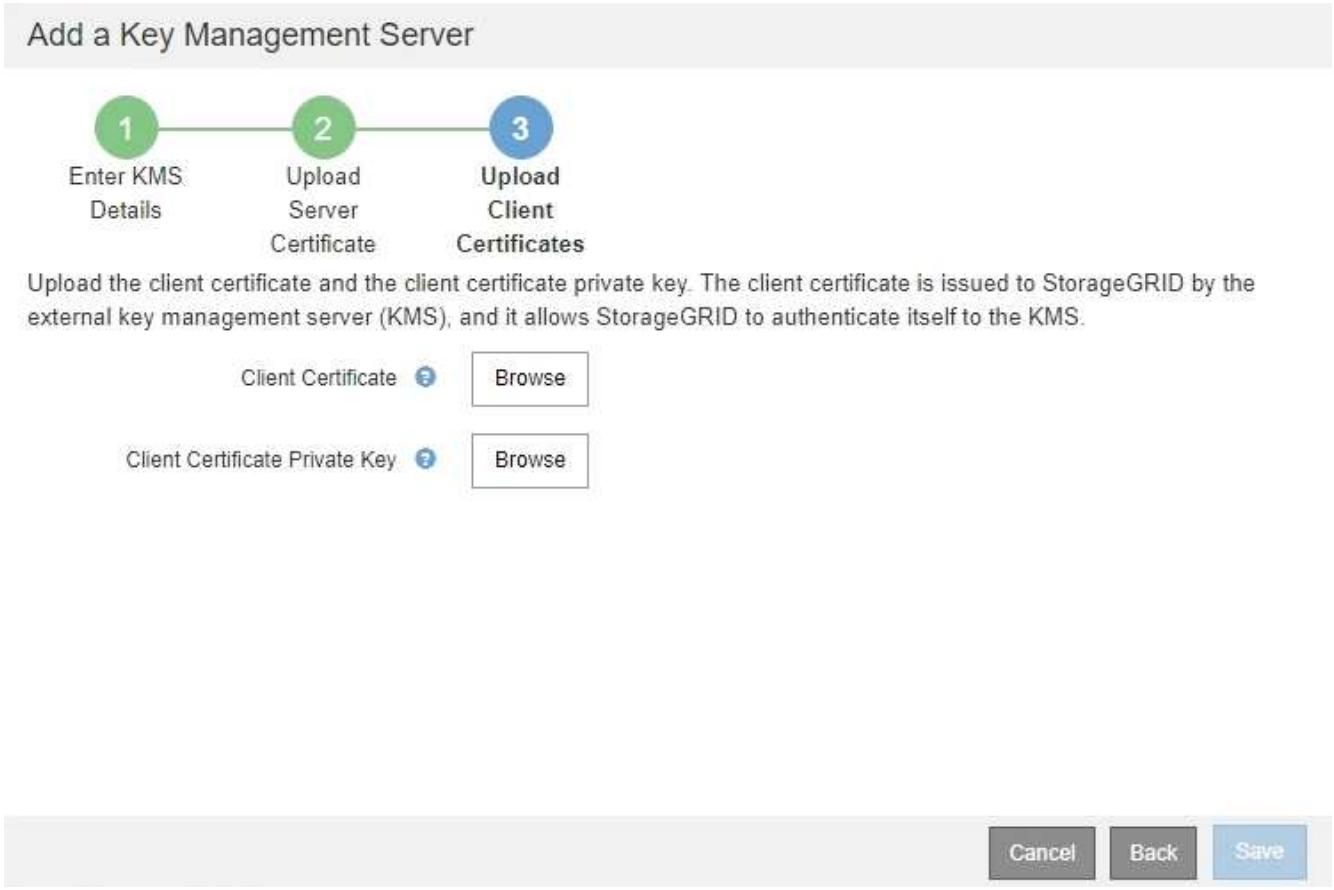
3. Seleccione **Siguiente**.

#### Paso 3: Cargar certificados de cliente

En el paso 3 (cargar certificados de cliente) del asistente Agregar un servidor de gestión de claves, carga el certificado de cliente y la clave privada del certificado de cliente. El certificado de cliente permite que StorageGRID se autentique en el KMS.

**Pasos**

1. Desde **Paso 3 (cargar certificados de cliente)**, vaya a la ubicación del certificado de cliente.

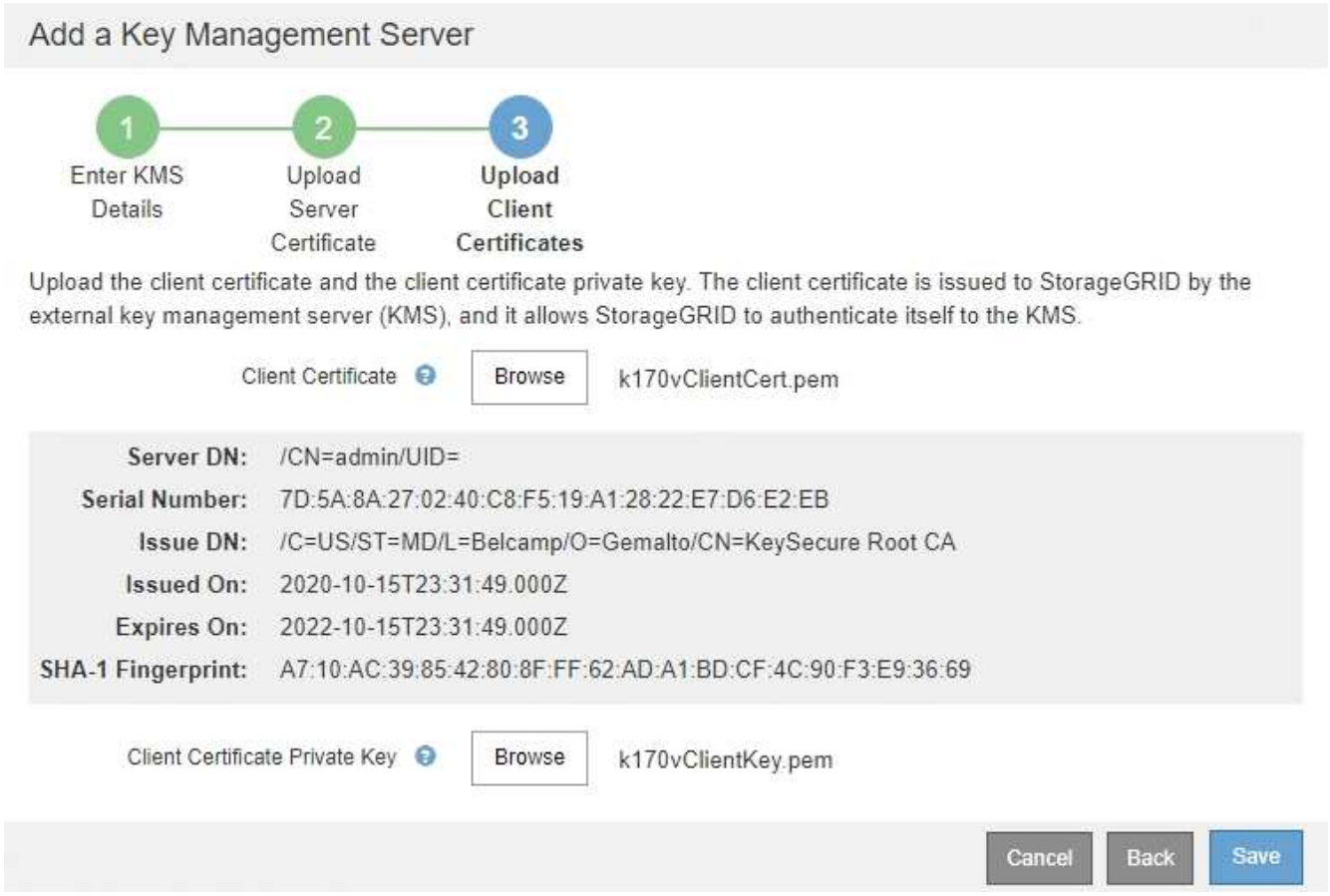



2. Cargue el archivo de certificado de cliente.

   Aparecen los metadatos del certificado de cliente.

3. Busque la ubicación de la clave privada del certificado de cliente.
4. Cargue el archivo de clave privada.

   Aparecen los metadatos del certificado de cliente y la clave privada del certificado de cliente.




5. Seleccione **Guardar**.

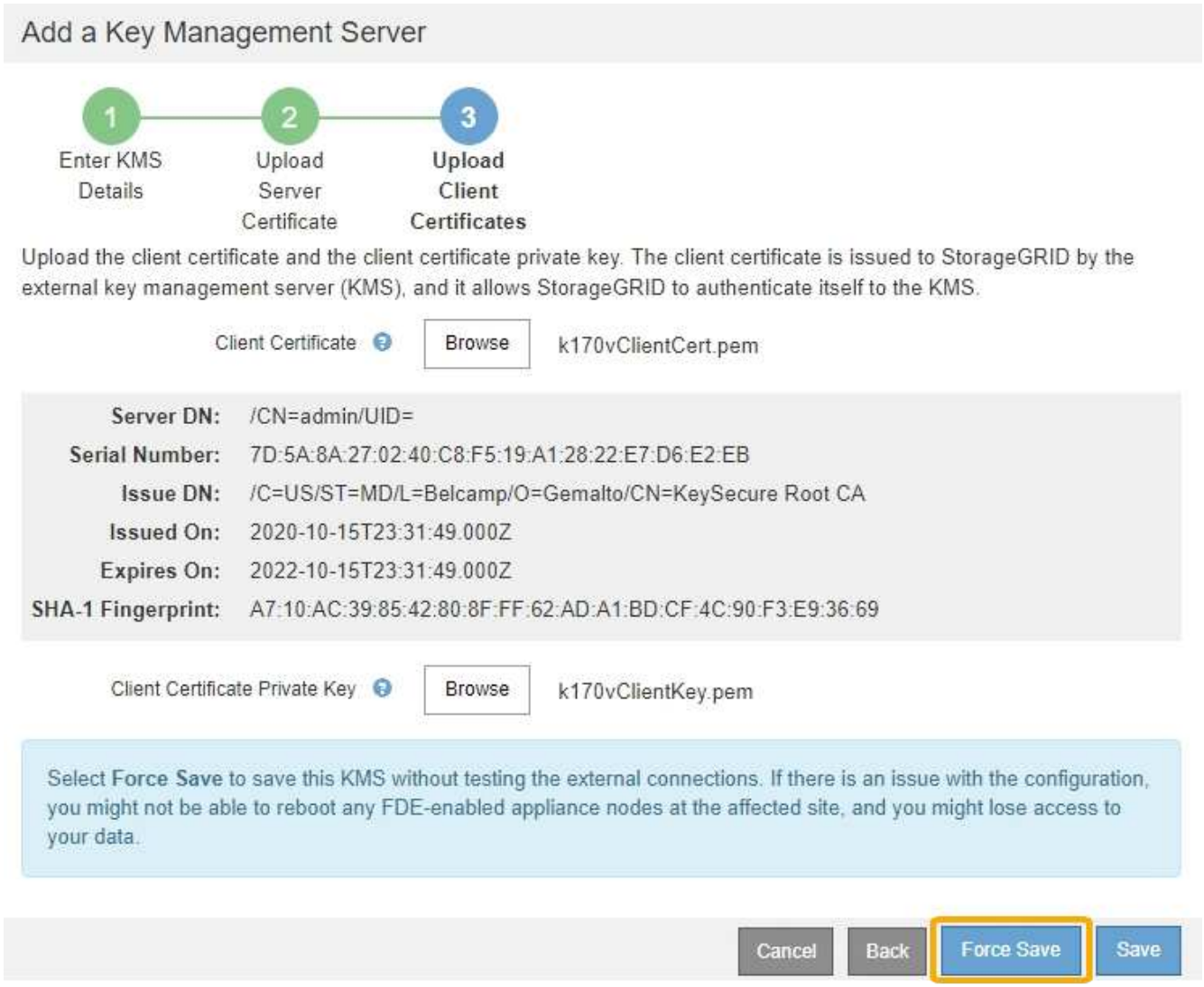
   Se prueban las conexiones entre el servidor de gestión de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves nuevo se añade a la tabla de la página del servidor de gestión de claves.

   > Inmediatamente después de añadir un KMS, el estado del certificado en la página servidor de gestión de claves aparece como Desconocido. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar el navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Guardar**, revise los detalles del mensaje y seleccione **Aceptar**.

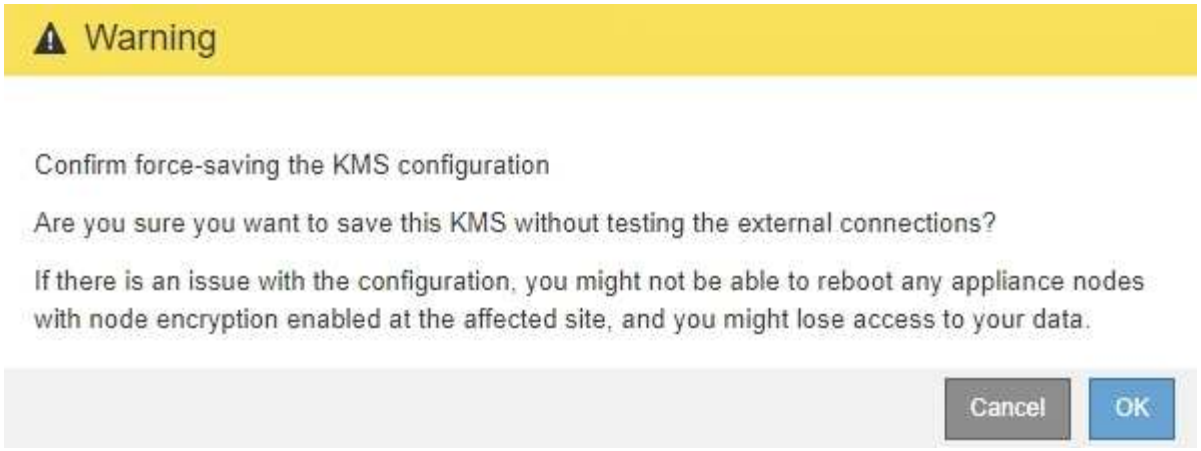
   Por ejemplo, puede recibir un error 422: Entidad no procesable si se produjo un error en una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Force Save**.




Al seleccionar **Force Save**, se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

8. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.




La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

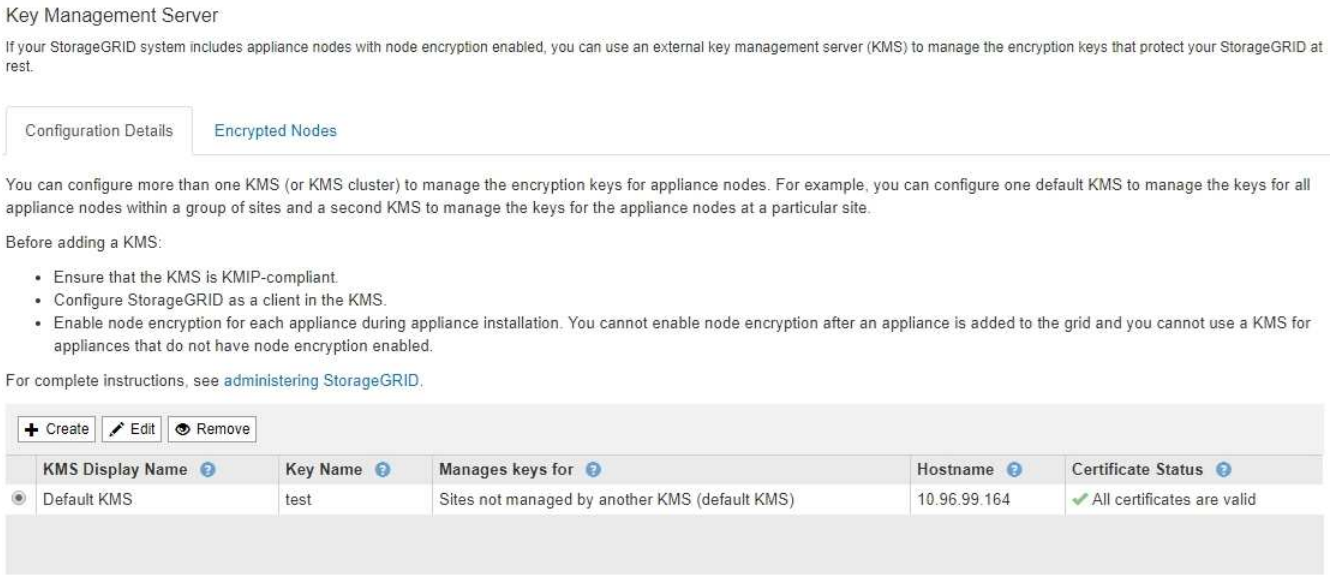
### Ver detalles de KMS

Puede ver información sobre cada servidor de gestión de claves (KMS) del sistema StorageGRID, incluidos el estado actual de los certificados de servidor y de cliente.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra cualquier servidor de gestión de claves configurado.




2. Revise la información de la tabla de cada KMS.

| Campo | Descripción |
|---|---|
| Nombre de visualización DE KMS | Nombre descriptivo del KMS. |
| Nombre de la clave | El alias clave del cliente StorageGRID en el KMS. |

| Campo | Descripción |
| --- | --- |
| Administra claves para | El sitio StorageGRID asociado con el KMS.<br><br>Este campo muestra el nombre de un sitio StorageGRID específico o **Sitios no administrados por otro KMS (KMS predeterminado).** |
| Nombre del hostl | El nombre de dominio completo o la dirección IP del KMS.<br><br>Si existe un clúster de dos servidores de gestión de claves, se muestran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de gestión de claves en un clúster, el nombre de dominio completo o la dirección IP del primer KMS se enumeran junto con la cantidad de servidores de gestión de claves adicionales en el clúster.<br><br>Por ejemplo: `10.10.10.10 and 10.10.10.11` o. `10.10.10.10 and 2 others`.<br><br>Para ver todos los nombres de host de un clúster, seleccione un KMS y, a continuación, seleccione **Editar**. |
| Estado del certificado | Estado actual del certificado de servidor, del certificado de CA opcional y del certificado de cliente: Válido, caducado, casi espirado o desconocido.<br><br>**Nota:** puede que StorageGRID tarde hasta 30 minutos en obtener actualizaciones del estado del certificado. Debe actualizar el navegador web para ver los valores actuales. |

3. Si el estado de certificado es desconocido, espere hasta 30 minutos y, a continuación, actualice el explorador web.

> Inmediatamente después de añadir un KMS, el estado del certificado en la página servidor de gestión de claves aparece como Desconocido. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar el explorador web para ver el estado real.

4. Si la columna Estado del certificado indica que un certificado ha caducado o está a punto de expirar, envíe el Lo antes posible. del problema.

   Consulte las acciones recomendadas para las alertas **KMS CA de vencimiento**, **KMS de vencimiento** del certificado de cliente* y **KMS de vencimiento** del certificado de servidor* en las instrucciones para Supervisión y solución de problemas de StorageGRID.

Debe solucionar cualquier problema con los certificados Lo antes posible. para mantener el acceso a los datos.

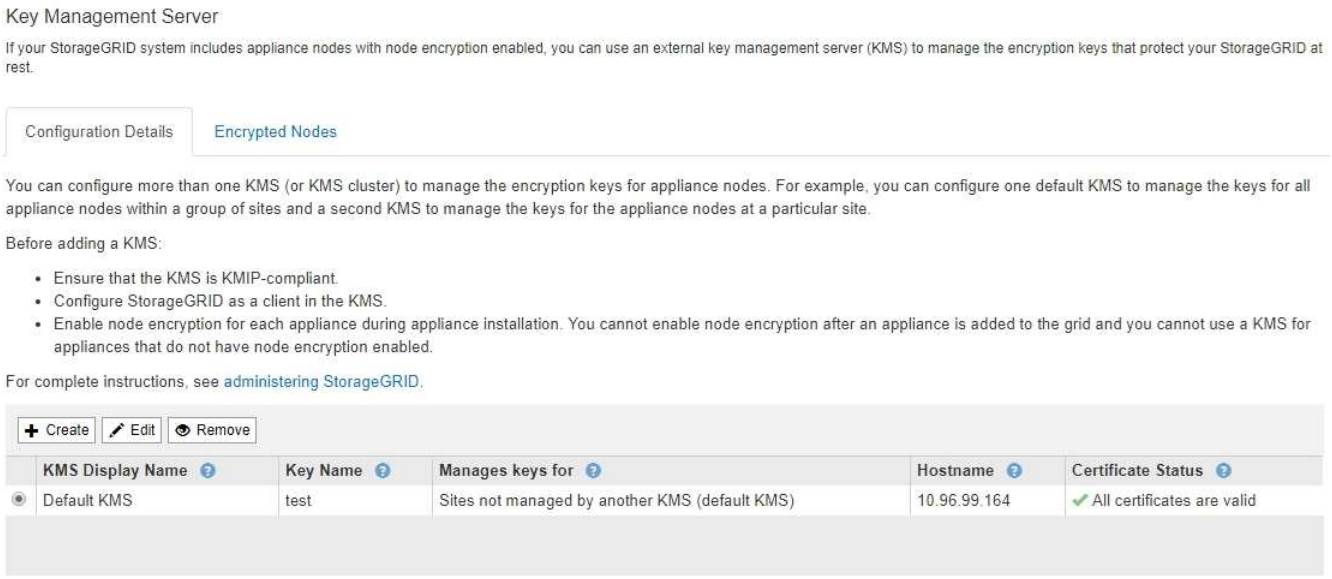
### Vea los nodos cifrados

Puede ver información acerca de los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

**Pasos**

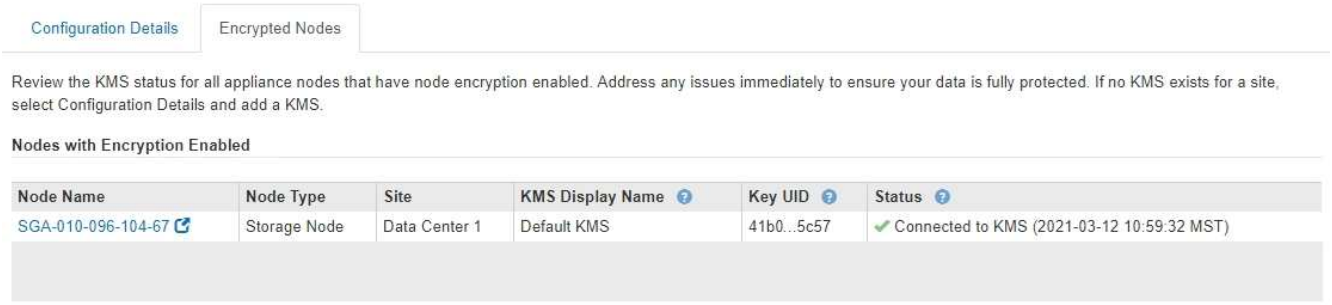
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra todos los servidores de gestión de claves que se configuraron.




2. En la parte superior de la página, seleccione la ficha **nodos cifrados**.

   La ficha nodos cifrados muestra los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.




3. Revise la información de la tabla de cada nodo del dispositivo.

| Columna | Descripción |
|---|---|
| Nombre del nodo | El nombre del nodo del dispositivo. |
| Tipo de nodo | El tipo de nodo: Almacenamiento, administrador o puerta de enlace. |
| Sitio | El nombre del sitio StorageGRID donde se instala el nodo. |
| Nombre de visualización DE KMS | Nombre descriptivo del KMS utilizado para el nodo.<br><br>Si no aparece ningún KMS, seleccione la ficha Detalles de configuración para agregar un KMS.<br><br>Añadir un servidor de gestión de claves (KMS) |
| UID de clave | El ID único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, pase el cursor por la celda.<br><br>Un guión (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo y el KMS. |
| Estado | El estado de la conexión entre el KMS y el nodo del dispositivo. Si el nodo está conectado, la Marca de tiempo se actualiza cada 30 minutos. El estado de la conexión puede tardar varios minutos en actualizarse después de que cambie la configuración de KMS.<br><br>**Nota:** debe actualizar el explorador Web para ver los nuevos valores. |

4. Si la columna Estado indica un problema de KMS, resuelva el problema inmediatamente.

   Durante las operaciones normales de KMS, el estado será **conectado a KMS**. Si un nodo está desconectado de la cuadrícula, se muestra el estado de conexión del nodo (administrativamente abajo o Desconocido).

   Otros mensajes de estado corresponden a las alertas StorageGRID con los mismos nombres:

   - No se ha podido cargar la configuración DE KMS

- Error de conectividad DE KMS
- No se ha encontrado el nombre de la clave de cifrado DE KMS
- Error en la rotación de la clave de cifrado DE KMS
- LA clave KMS no pudo descifrar el volumen de un dispositivo
- KMS no está configurado

Consulte las acciones recomendadas para estas alertas en las instrucciones de Supervisión y solución de problemas de StorageGRID.

Debe solucionar cualquier problema inmediatamente para garantizar que los datos están totalmente protegidos.

### Editar un servidor de gestión de claves (KMS)

Es posible que deba editar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de expirar.

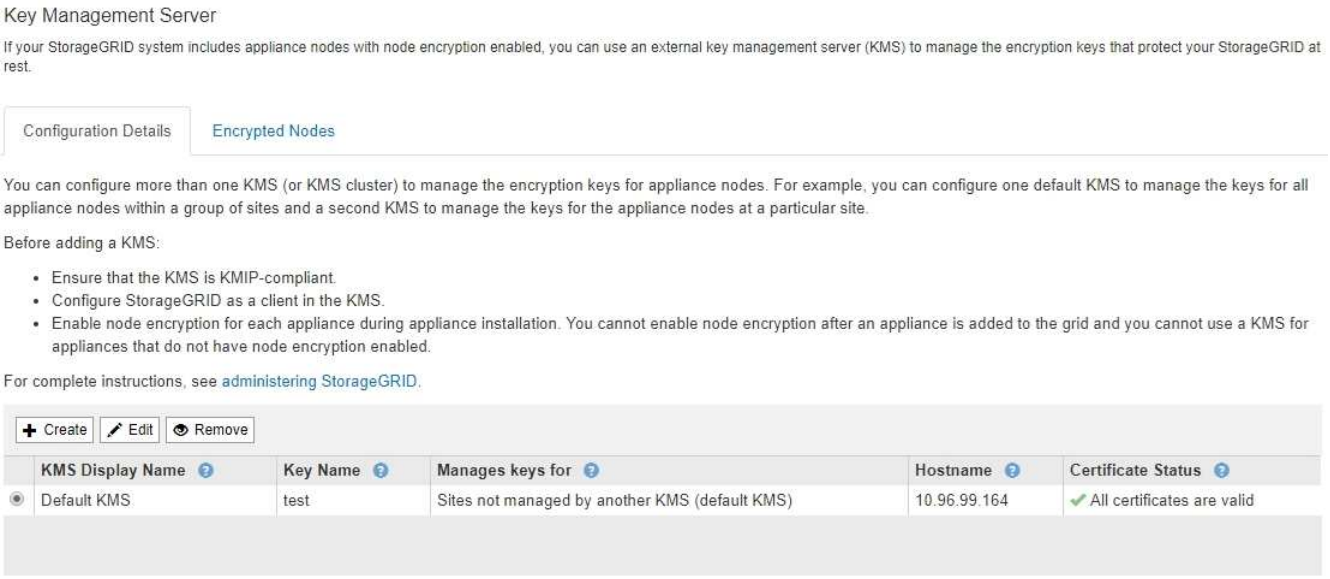
**Lo que necesitará**

- Ha revisado el consideraciones y requisitos para usar un servidor de gestión de claves.
- Si planea actualizar el sitio seleccionado para un KMS, ha revisado el Consideraciones para cambiar el KMS de un sitio.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página servidor de gestión de claves para mostrar todos los servidores de gestión de claves configurados.




2. Seleccione el KMS que desea editar y seleccione **Editar**.

3. Opcionalmente, actualice los detalles en **Paso 1 (introducir detalles de KMS)** del asistente Editar un servidor de administración de claves.

| Campo | Descripción |
|---|---|
| Nombre de visualización DE KMS | Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres. |
| Nombre de la clave | El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres.<br><br>Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.<br><br>Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS. En su lugar, gire la clave actualizando la versión de la clave en el software KMS. StorageGRID requiere que se pueda acceder a todas las versiones de claves usadas anteriormente (así como a las futuras) desde el KMS con el mismo alias de clave. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.<br><br>Consideraciones y requisitos para usar un servidor de gestión de claves |
| Administra claves para | Si va a editar un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione **Sitios no administrados por otro KMS (KMS predeterminado)**. Esta selección convierte un KMS específico del sitio al KMS predeterminado, que se aplicará a todos los sitios que no tienen un KMS dedicado y a cualquier sitio agregado en una expansión.<br><br>**Nota:** Si está editando un KMS específico del sitio, no puede seleccionar otro sitio. Si va a editar el KMS predeterminado, no puede seleccionar un sitio específico. |
| Puerto | El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP. |
| Nombre del hostl | El nombre de dominio completo o la dirección IP del KMS.<br><br>**Nota:** el campo SAN del certificado de servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS. |

4. Si va a configurar un clúster KMS, seleccione el signo más ➕ para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **Siguiente**.

Aparece el paso 2 (cargar certificado de servidor) del asistente Editar un servidor de administración de claves.

6. Si necesita sustituir el certificado del servidor, seleccione **examinar** y cargue el nuevo archivo.
7. Seleccione **Siguiente**.

   Aparece el paso 3 (cargar certificados de cliente) del asistente Editar un servidor de gestión de claves.

8. Si necesita sustituir el certificado de cliente y la clave privada del certificado de cliente, seleccione **examinar** y cargue los nuevos archivos.
9. Seleccione **Guardar**.

   Se prueban las conexiones entre el servidor de gestión de claves y todos los nodos de dispositivos cifrados por nodo en los sitios afectados. Si todas las conexiones de nodos son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves se agrega a la tabla de la página servidor de gestión de claves.

10. Si aparece un mensaje de error, revise los detalles del mensaje y seleccione **Aceptar**.

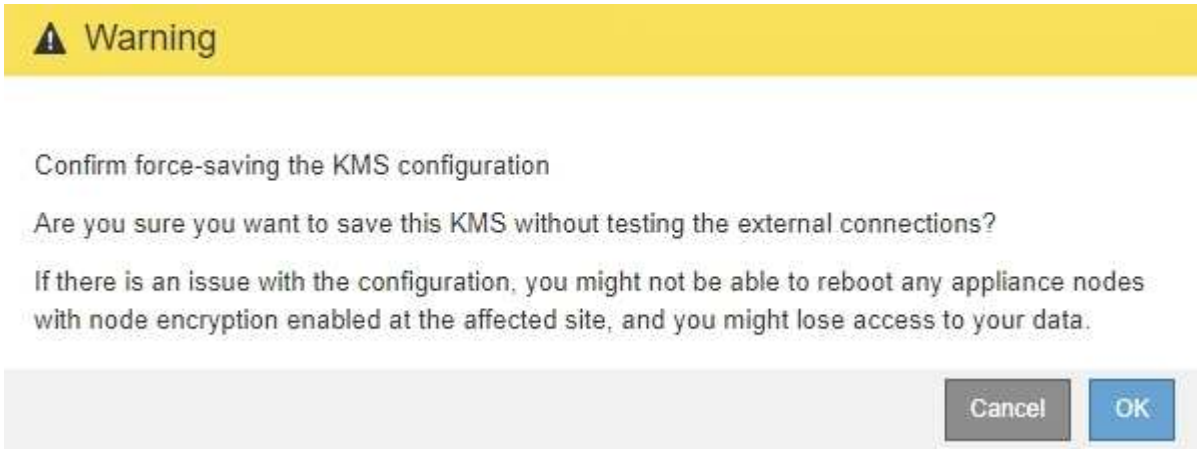
    Por ejemplo, puede recibir un error 422: Entidad no procesable si el sitio seleccionado para este KMS ya está administrado por otro KMS o si se produjo un error en una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar ahorro**.

    > Al seleccionar **Force Save**, se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

    Se guarda la configuración de KMS.

12. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.




La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

### Quitar un servidor de gestión de claves (KMS)

En algunos casos, es posible quitar un servidor de gestión de claves. Por ejemplo, puede que desee quitar un KMS específico de un sitio si ha retirado del servicio el sitio.

#### Lo que necesitará

- Ha revisado el consideraciones y requisitos para usar un servidor de gestión de claves.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

#### Acerca de esta tarea

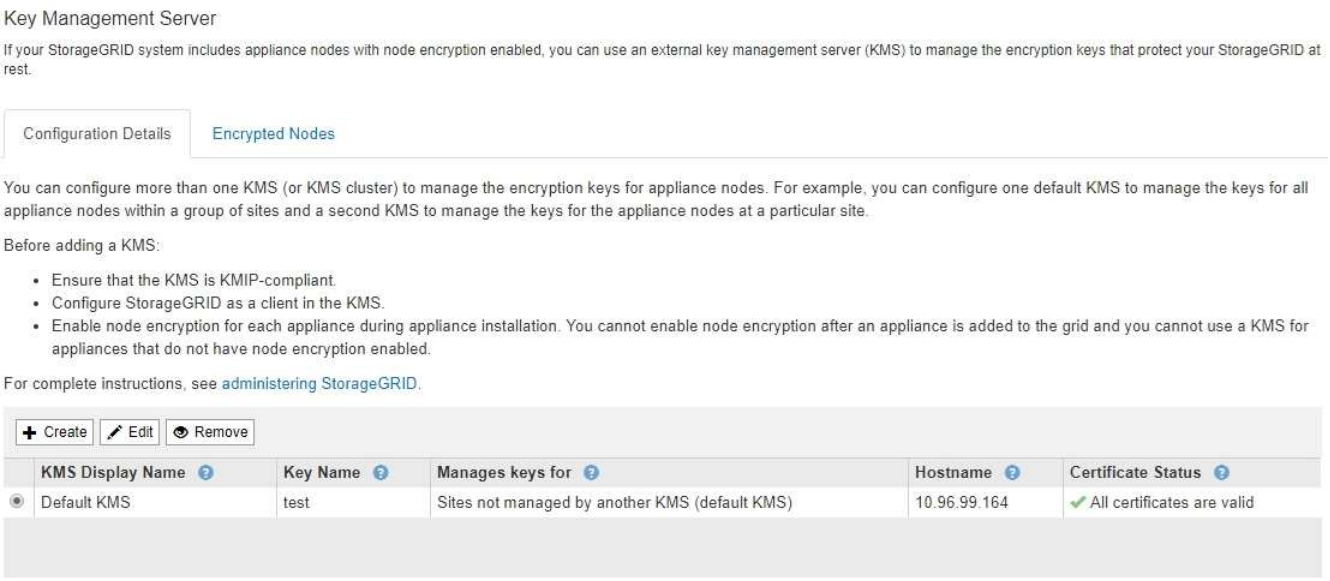
Puede eliminar un KMS en los siguientes casos:

- Puede eliminar un KMS específico de un sitio si se ha dado de baja o si el sitio incluye ningún nodo de dispositivo con cifrado de nodo activado.
- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tiene nodos de dispositivo con cifrado de nodo activado.

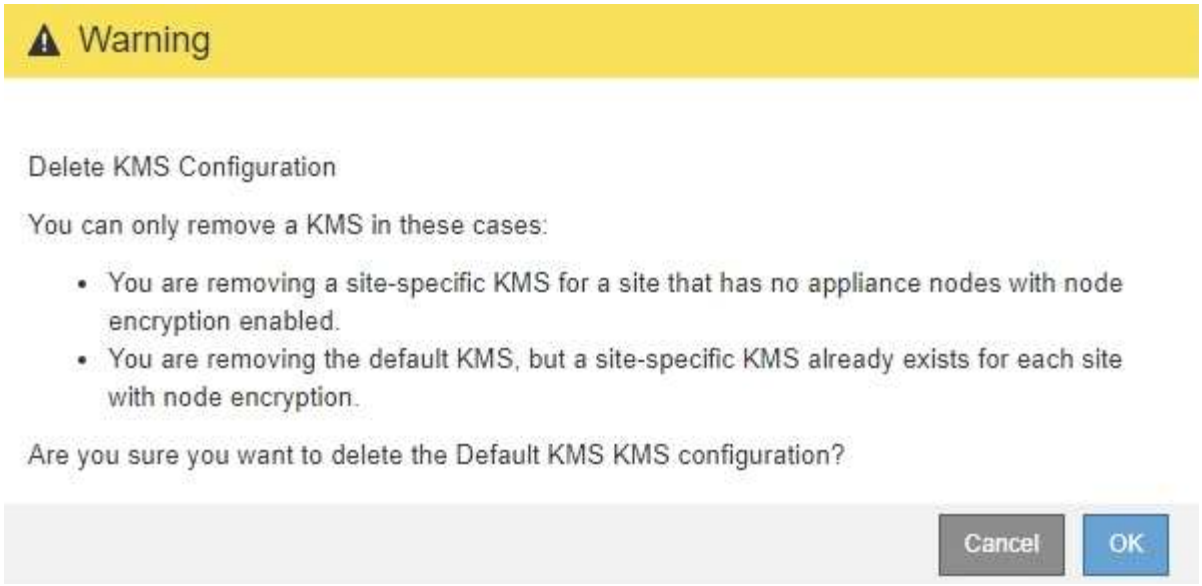
#### Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página servidor de gestión de claves para mostrar todos los servidores de gestión de claves configurados.




2. Seleccione el botón de opción del KMS que desea quitar y seleccione **Quitar**.
3. Revise las consideraciones en el cuadro de diálogo de advertencia.




4. Seleccione **OK**.

   La configuración de KMS se elimina.

## Administrar la configuración de proxy

### Configure las opciones de proxy de almacenamiento

Si utiliza servicios de plataforma o pools de almacenamiento en cloud, puede configurar un proxy no transparente entre los nodos de almacenamiento y los extremos de S3 externos. Por ejemplo, es posible que necesite un proxy no transparente para permitir que los mensajes de servicios de plataforma se envíen a extremos externos, como un punto final en Internet.

#### Lo que necesitará

- Tiene permisos de acceso específicos.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

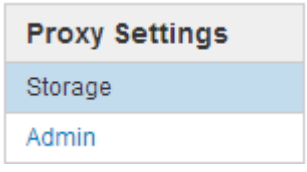
#### Acerca de esta tarea

Puede configurar los ajustes de un único proxy de almacenamiento.

#### Pasos

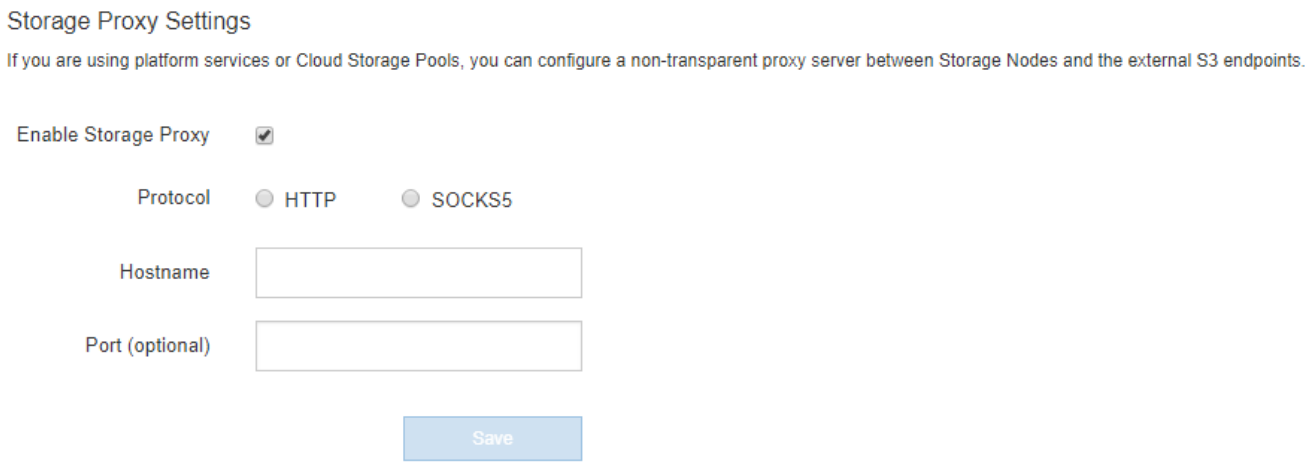
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Se muestra la página Storage Proxy Settings. De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.




2. Active la casilla de verificación **Activar proxy de almacenamiento**.

Aparecen los campos para configurar un proxy de almacenamiento.




3. Seleccione el protocolo del proxy de almacenamiento no transparente.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. De manera opcional, introduzca el puerto utilizado para conectarse al servidor proxy.

   Puede dejar este campo en blanco si utiliza el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

   Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos extremos para los servicios de plataforma o Cloud Storage Pools.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Compruebe la configuración del servidor proxy para asegurarse de que los mensajes de StorageGRID relacionados con el servicio de la plataforma no se bloqueen.

**Después de terminar**

Si necesita desactivar un proxy de almacenamiento, anule la selección de la casilla de verificación **Activar proxy de almacenamiento** y seleccione **Guardar**.

**Información relacionada**

- Red y puertos para servicios de plataforma
- Gestión de objetos con ILM

### Configure los ajustes del proxy de administración

Si envía mensajes de AutoSupport con HTTP o HTTPS (consulte Configure AutoSupport), puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

**Lo que necesitará**

- Tiene permisos de acceso específicos.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

**Acerca de esta tarea**

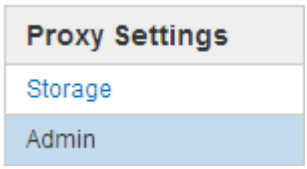
Puede configurar los ajustes de un único proxy de administración.

**Pasos**

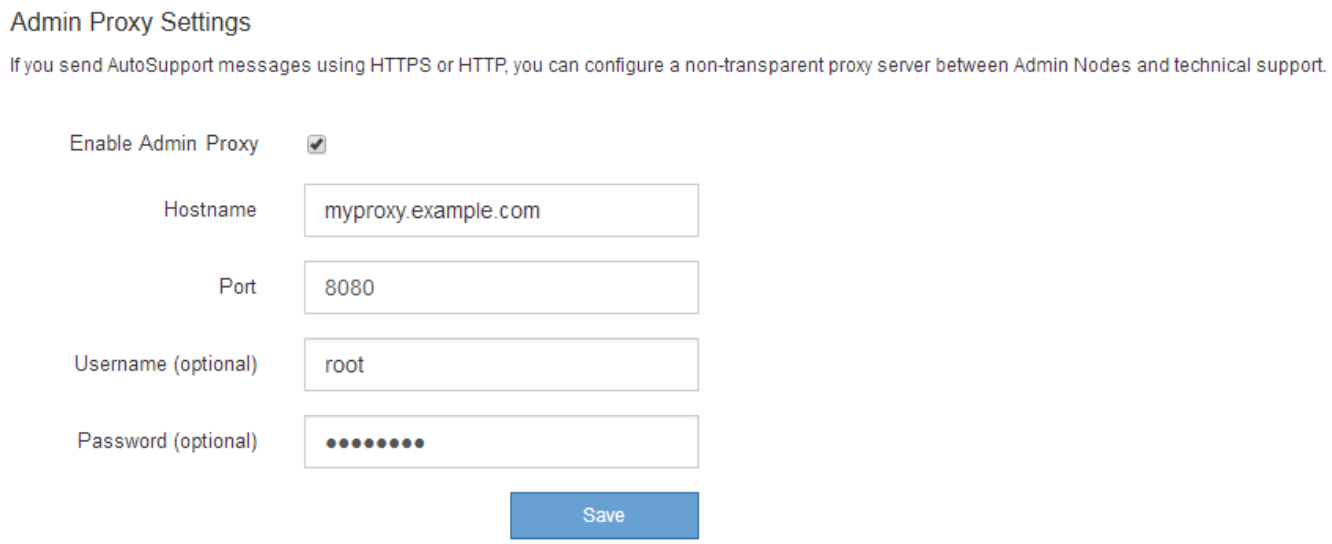
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Aparece la página Admin Proxy Settings (Configuración del proxy de administración). De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. En el menú de la barra lateral, seleccione **Admin**.




3. Active la casilla de verificación **Activar proxy de administración**.




4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Si lo desea, introduzca el nombre de usuario del proxy.

   Deje este campo en blanco si el servidor proxy no requiere un nombre de usuario.

7. De forma opcional, introduzca la contraseña del proxy.

   Deje este campo en blanco si el servidor proxy no requiere una contraseña.

8. Seleccione **Guardar**.

   Una vez guardado el proxy de administrador, se configura el servidor proxy entre los nodos de administrador y el soporte técnico.

   Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesita desactivar el proxy, anule la selección de la casilla de verificación **Activar proxy de administración** y seleccione **Guardar**.

## Administrar redes de clientes que no son de confianza

### Administrar redes de clientes que no son de confianza: Descripción general

Si está utilizando una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles aceptando tráfico de cliente entrante sólo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente de cada nodo de cuadrícula es *Trusted*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de cuadrícula en todos los puertos externos disponibles (consulte la información acerca de las comunicaciones externas en Directrices sobre redes).

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red cliente de cada nodo sea *no confiable*. Si la red de cliente de un nodo no es de confianza, el nodo sólo acepta conexiones entrantes en los puertos configurados explícitamente como puntos finales de equilibrador de carga. Consulte Configurar puntos finales del equilibrador de carga.

#### Ejemplo 1: Gateway Node solo acepta solicitudes HTTPS S3

Supongamos que desea que un nodo de puerta de enlace rechace todo el tráfico entrante en la red cliente excepto las solicitudes HTTPS S3. Debe realizar estos pasos generales:

1. En la página Load Balancer Endpoints, configure un extremo de equilibrador de carga para S3 a través de HTTPS en el puerto 443.
2. En la página redes de cliente no fiables, especifique que la red de cliente del nodo de puerta de enlace no sea de confianza.

Después de guardar la configuración, se descarta todo el tráfico entrante en la red cliente del nodo de puerta de enlace, excepto las solicitudes HTTPS S3 en el puerto 443 y las solicitudes ICMP echo (ping).

#### Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de plataforma S3

Supongamos que desea habilitar el tráfico saliente del servicio de la plataforma S3 desde un nodo de almacenamiento, pero desea impedir las conexiones entrantes a ese nodo de almacenamiento en la red cliente. Debe realizar este paso general:

- En la página redes de cliente no fiables, indique que la red de clientes del nodo de almacenamiento no es de confianza.

Después de guardar la configuración, el nodo de almacenamiento ya no acepta ningún tráfico entrante en la red cliente, pero continúa permitiendo solicitudes salientes a Amazon Web Services.

### Especifique que la red de cliente del nodo no es de confianza

Si utiliza una red de cliente, puede especificar si la red de cliente de cada nodo es de confianza o no es de confianza. También puede especificar la configuración predeterminada para los nuevos nodos agregados en una ampliación.

#### Lo que necesitará

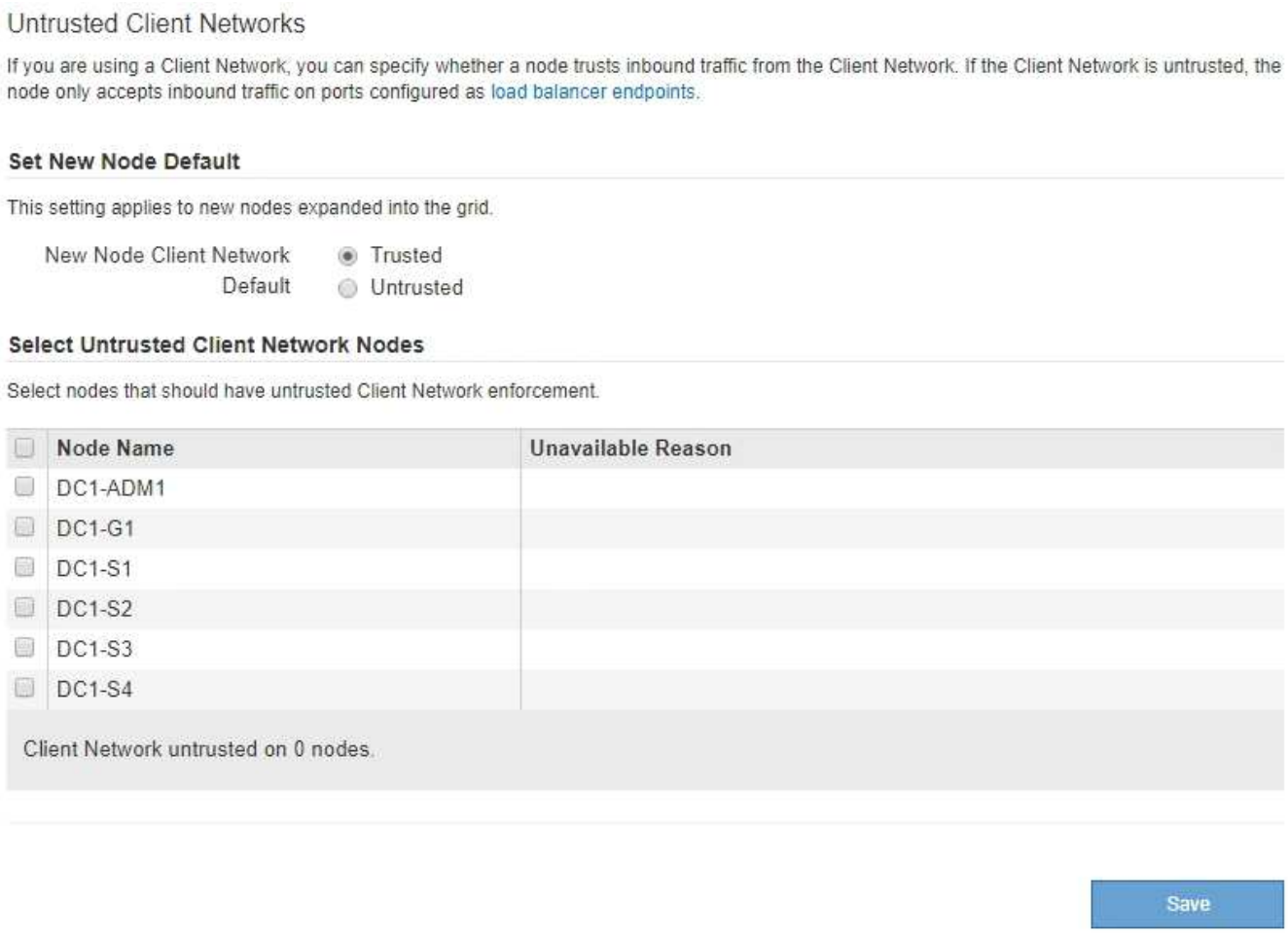
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante sólo en puntos finales configurados explícitamente, ha definido los puntos finales del equilibrador de carga.

> Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **redes de cliente no fiables**.

   En la página redes de cliente no fiables se enumeran todos los nodos del sistema StorageGRID. La columna motivo no disponible incluye una entrada si la red de cliente del nodo debe ser de confianza.




2. En la sección **establecer nuevo nodo predeterminado** , especifique cuál debe ser la configuración predeterminada cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.
   - **Trusted**: Cuando se agrega un nodo en una expansión, su red de cliente es de confianza.
   - **No fiable**: Cuando se agrega un nodo en una expansión, su red cliente no es de confianza. Según sea necesario, puede volver a esta página para cambiar la configuración de un nuevo nodo concreto.

   > Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

3. En la sección **Seleccionar nodos de red de cliente no confiable**, seleccione los nodos que deben permitir conexiones de cliente sólo en puntos finales de equilibrador de carga configurados explícitamente.

   Puede seleccionar o anular la selección de la casilla de comprobación en el título para seleccionar o anular la selección de todos los nodos.

4. Seleccione **Guardar**.

   Las nuevas reglas de firewall se agregan y aplican inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

# Gestione inquilinos

## Gestione inquilinos

Como administrador de grid, puede crear y gestionar las cuentas de inquilino que utilizan los clientes de S3 y Swift para almacenar y recuperar objetos, supervisar el uso del almacenamiento y gestionar las acciones que pueden realizar los clientes mediante el sistema StorageGRID.

### ¿Qué son las cuentas de inquilinos?

Las cuentas de inquilino permiten a las aplicaciones cliente que usan la API DE REST de simple Storage Service (S3) o la API DE REST de Swift para almacenar y recuperar objetos en StorageGRID.

Cada cuenta de inquilino admite el uso de un único protocolo, que se especifica al crear la cuenta. Para almacenar y recuperar objetos en un sistema StorageGRID con ambos protocolos, debe crear dos cuentas de inquilino: Una para los bloques y objetos de S3, y otra para los contenedores y objetos de Swift. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, bloques o contenedores, y objetos.

Opcionalmente, puede crear cuentas de arrendatario adicionales si desea segregar los objetos almacenados en su sistema por entidades diferentes. Por ejemplo, puede configurar varias cuentas de inquilino en cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si administra un sistema StorageGRID en una aplicación empresarial, es posible que desee segregar el almacenamiento de objetos de la red por los diferentes departamentos de la organización. En este caso, podría crear cuentas de inquilino para el departamento de marketing, el departamento de soporte al cliente, el departamento de recursos humanos, etc.

  > Si utiliza el protocolo cliente S3, puede utilizar bloques S3 y políticas de bucket para separar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones para implementar aplicaciones cliente S3 para obtener más información.

- **Caso de uso del proveedor de servicios:** Si administra un sistema StorageGRID como proveedor de servicios, puede segregar el almacenamiento de objetos de la red por las diferentes entidades que alquile el almacenamiento en la red. En este caso, creará cuentas de inquilino para la empresa A, la empresa B, la empresa C, etc.

### Cree y configure cuentas de inquilino

Al crear una cuenta de inquilino, especifique la siguiente información:

- Nombre para mostrar de la cuenta de inquilino.
- Qué protocolo de cliente utilizará la cuenta de inquilino (S3 o Swift).
- Para las cuentas de inquilino de S3: Si la cuenta de inquilino tiene permiso para usar servicios de plataforma con bloques de S3. Si permite que las cuentas de arrendatario utilicen servicios de plataforma, debe asegurarse de que la cuadrícula está configurada para respaldar su uso. Consulte «gestionar servicios de plataforma».
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. Si se supera la cuota, el arrendatario no puede crear nuevos objetos.

> La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).

- Si está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

Después de crear una cuenta de inquilino, puede realizar las siguientes tareas:

- **Administrar servicios de plataforma para la red**: Si habilita servicios de plataforma para cuentas de inquilino, asegúrese de comprender cómo se entregan los mensajes de servicios de plataforma y los requisitos de red que el uso de servicios de plataforma tiene lugar en la implementación de StorageGRID.
- **Supervisar el uso del almacenamiento de una cuenta de inquilino**: Después de que los inquilinos comiencen a usar sus cuentas, puede utilizar Grid Manager para supervisar cuánto almacenamiento consume cada inquilino.

> Los valores de uso de almacenamiento de un inquilino pueden dejar de estar obsoletos si se aíslan nodos de otros nodos del grid. Los totales se actualizarán cuando se restaure la conectividad de red.

  Si ha establecido cuotas para inquilinos, puede habilitar la alerta * uso de cuota de inquilino alto* para determinar si los inquilinos están consumiendo sus cuotas. Si está habilitada, esta alerta se activa cuando un inquilino ha utilizado el 90% de su cuota. Para obtener más información, consulte la referencia de alertas en las instrucciones para supervisar y solucionar problemas de StorageGRID.

- **Configurar operaciones de cliente**: Puede configurar si algunos tipos de operaciones de cliente están prohibidas.

### Configure los inquilinos S3

Una vez creada una cuenta de inquilino de S3, los usuarios de inquilinos pueden acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configuración de la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y creación de grupos y usuarios locales

- Gestión de claves de acceso de S3
- Crear y gestionar bloques de S3
- Supervisión del uso de almacenamiento
- Uso de servicios de plataforma (si está activado)

> Los usuarios de inquilinos S3 pueden crear y gestionar bloques de clave de acceso S3 con el administrador de inquilinos, pero deben usar una aplicación cliente S3 para procesar y gestionar objetos.

**Configure los inquilinos Swift**

Después de crear una cuenta de inquilino de Swift, el usuario raíz del inquilino puede acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de almacenamiento

> Los usuarios de Swift deben tener el permiso de acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso de acceso raíz no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

**Información relacionada**

Usar una cuenta de inquilino

## Cree una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema de StorageGRID.

Al crear una cuenta de inquilino, se especifica un nombre, un protocolo de cliente y, opcionalmente, una cuota de almacenamiento. Si se habilitó el inicio de sesión único (SSO) para StorageGRID, también se especifica qué grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino. Si StorageGRID no utiliza el inicio de sesión único, también debe especificar si la cuenta de inquilino utilizará su propio origen de identidad y configurar la contraseña inicial para el usuario raíz local del inquilino.

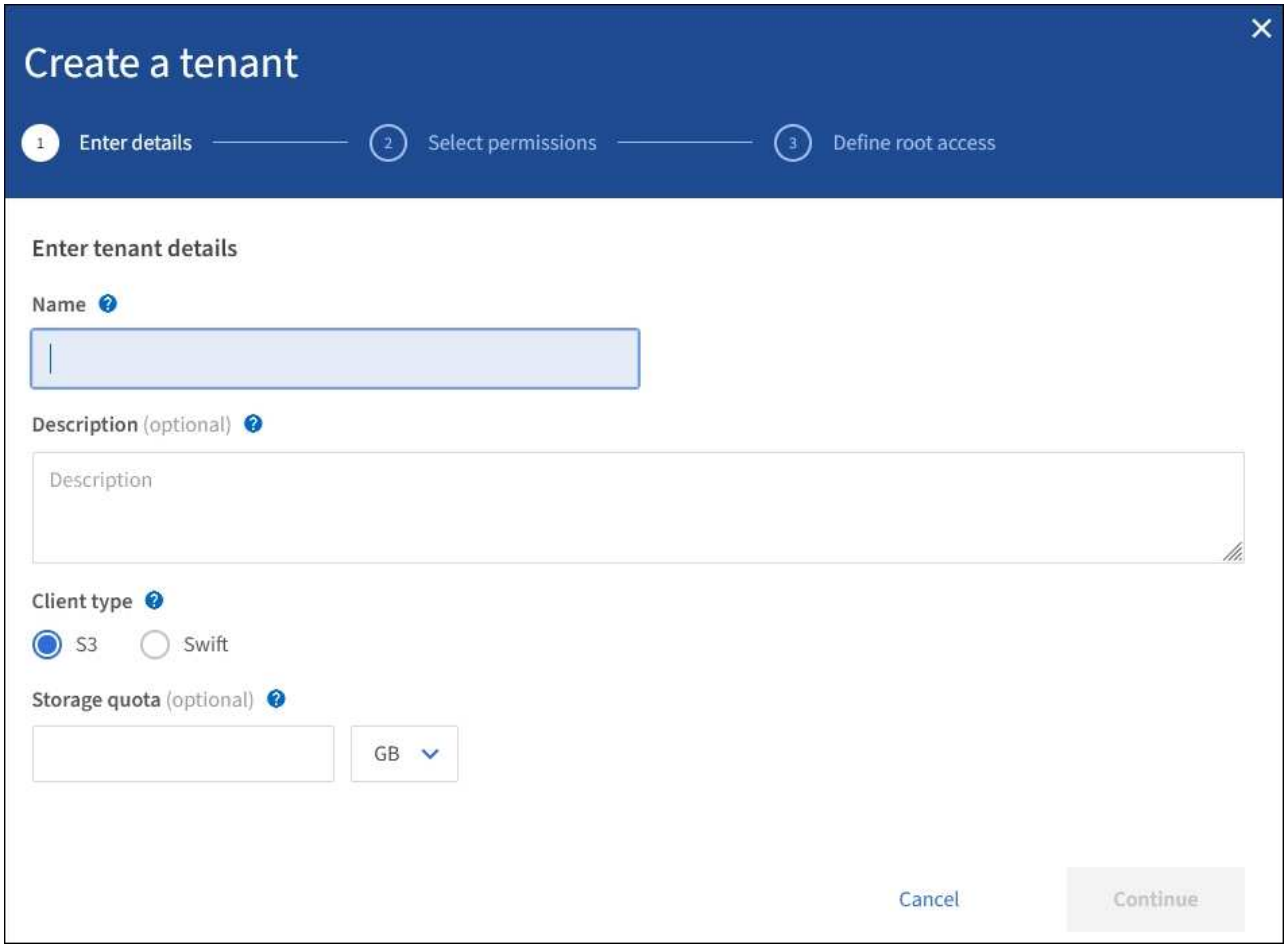
Grid Manager proporciona un asistente que le guía por los pasos para crear una cuenta de arrendatario. Los pasos varían en función de si federación de identidades y.. inicio de sesión único Están configurados y si la cuenta de Grid Manager que utiliza para crear la cuenta de arrendatario pertenece a un grupo de administración con el permiso acceso raíz.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Si la cuenta de arrendatario utilizará el origen de identidad configurado para el Administrador de grid y desea otorgar permiso de acceso raíz para la cuenta de arrendatario a un grupo federado, ha importado ese grupo federado en el Gestor de grid. No es necesario asignar ningún permiso de Grid Manager a este grupo de administración. Consulte instrucciones para administrar grupos de administración.

**Pasos**

1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear** e introduzca la siguiente información para el arrendatario:
   a. **Nombre**: Introduzca un nombre para la cuenta de arrendatario. Los nombres de inquilinos no tienen que ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.
   b. **Descripción** (opcional): Introduzca una descripción que le ayude a identificar al inquilino.
   c. **Tipo de cliente**: Seleccione el tipo de cliente de **S3** o **Swift**.
   d. **Cuota de almacenamiento** (opcional): Si desea que este arrendatario tenga una cuota de almacenamiento, introduzca un valor numérico para la cuota y seleccione las unidades correctas (GB, TB o PB).




3. Seleccione **continuar** y configure el inquilino S3 o Swift.

**Inquilino de S3**

Seleccione los permisos apropiados para el arrendatario. Algunos de estos permisos tienen requisitos adicionales. Para obtener más detalles, consulte la ayuda en línea de cada permiso.

- Permitir los servicios de plataforma
- Utilizar su propio origen de identidad (seleccionable solo si no se utiliza SSO)
- Permitir selección de S3 (consulte Gestione S3 Select para cuentas de inquilinos)

**Inquilino de Swift**

Si el inquilino utilizará su propia fuente de identidad, seleccione **usar su propia fuente de identidad** (seleccionable sólo si no se utiliza SSO).

1. Seleccione **continuar** y defina el acceso raíz para la cuenta de arrendatario.

**federación de identidades no configurada**

1. Introduzca una contraseña para el usuario raíz local.
2. Seleccione **Crear arrendatario**.

**SSO habilitado**

Cuando SSO está habilitado para StorageGRID, el inquilino debe utilizar el origen de identidad configurado para Grid Manager. Ningún usuario local puede iniciar sesión. Especifique qué grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.

1. Seleccione un grupo federado existente en Grid Manager para tener el permiso de acceso raíz inicial para el arrendatario.

   Si dispone de los permisos adecuados, se mostrarán los grupos federados existentes del Gestor de grid al seleccionar el campo. De lo contrario, introduzca el nombre exclusivo del grupo.

2. Seleccione **Crear arrendatario**.

**SSO no está habilitado**

1. Complete los pasos descritos en la tabla en función de si el inquilino gestionará sus propios grupos y usuarios o utilizará el origen de identidad configurado para Grid Manager.

| Si el inquilino… | Realice lo siguiente… |
|---|---|
| Administrar sus propios grupos y usuarios | a. Seleccione **usar la propia fuente de identidad**.<br><br>**Nota**: Si esta casilla de verificación está seleccionada y desea utilizar la federación de identidades para grupos de arrendatarios y usuarios, el arrendatario debe configurar su propio origen de identidad. Consulte instrucciones para el uso de cuentas de inquilino.<br><br>b. Especifique una contraseña para el usuario raíz local del arrendatario y, a continuación, seleccione **Crear arrendatario**.<br><br>c. Seleccione **Iniciar sesión como root** para configurar el arrendatario, o seleccione **Finalizar** para configurar el arrendatario más tarde. |
| Utilice los grupos y usuarios configurados para Grid Manager | a. Realice una o ambas de las siguientes acciones:<br><br>◦ Seleccione un grupo federado existente en el Gestor de grid que tenga el permiso de acceso raíz inicial para el arrendatario.<br><br>**Nota**: Si dispone de los permisos adecuados, los grupos federados existentes de Grid Manager aparecen cuando seleccione el campo. De lo contrario, introduzca el nombre exclusivo del grupo.<br><br>◦ Especifique una contraseña para el usuario raíz local del inquilino.<br><br>b. Seleccione **Crear arrendatario**. |

1. Para iniciar sesión en el inquilino ahora:

- Si tiene acceso a Grid Manager en un puerto restringido, seleccione **restringido** en la tabla arrendatario para obtener más información sobre cómo acceder a esta cuenta de arrendatario.

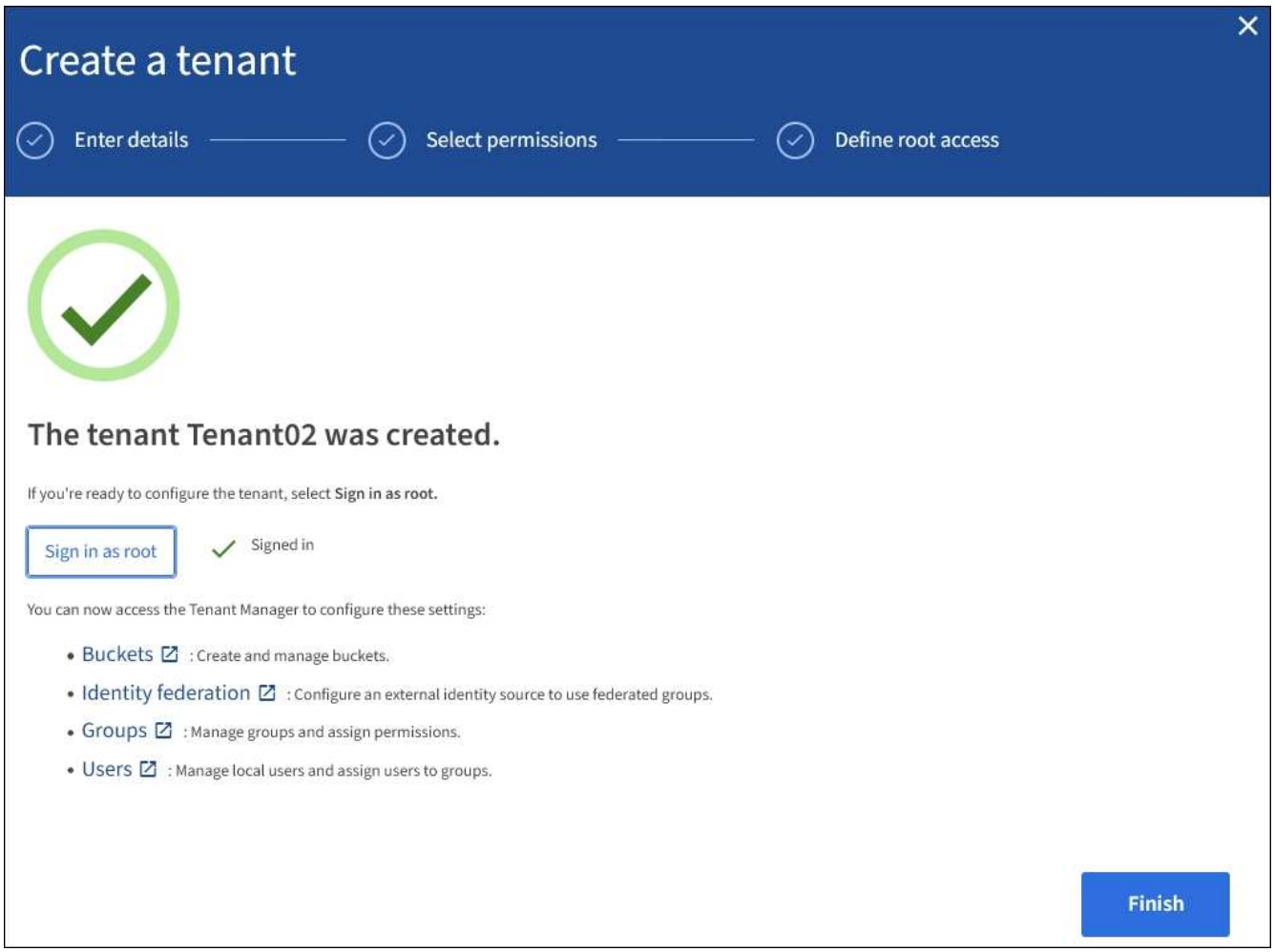
  La dirección URL del administrador de inquilinos tiene el siguiente formato:

  `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`

  - *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o la dirección IP de un nodo de administrador
  - *`port`* es el puerto de solo inquilino
  - *`20-digit-account-id`* Es el ID de cuenta único del inquilino

- Si está accediendo a Grid Manager en el puerto 443 pero no ha establecido una contraseña para el usuario raíz local, en la tabla Tenants del Grid Manager, seleccione **Iniciar sesión** e introduzca las credenciales de un usuario en el grupo federado de acceso raíz.
- Si va a acceder a Grid Manager en el puerto 443 y establece una contraseña para el usuario raíz local:
  i. Seleccione **Iniciar sesión como root** para configurar el arrendatario ahora.

     Al iniciar sesión, aparecen enlaces para configurar bloques o contenedores, federación de identidades, grupos y usuarios.




i. Seleccione los vínculos para configurar la cuenta de arrendatario.

Cada enlace abre la página correspondiente en el Administrador de arrendatarios. Para completar la página, consulte instrucciones para el uso de cuentas de inquilino.

ii. De lo contrario, seleccione **Finalizar** para acceder al arrendatario más adelante.

2. Para acceder al inquilino más adelante:

| Si está usando… | Realice una de estas… |
|---|---|
| Puerto 443 | • En Grid Manager, seleccione **ARRENDATARIOS** y seleccione **Iniciar sesión** a la derecha del nombre del arrendatario.<br>• Introduzca la URL del inquilino en un navegador web:<br>`https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/`<br>◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administrador<br>◦ *20-digit-account-id* Es el ID de cuenta único del inquilino |
| Un puerto restringido | • En Grid Manager, seleccione **ARRENDATARIOS** y seleccione **restringido**.<br>• Introduzca la URL del inquilino en un navegador web:<br>`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id`<br>◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administrador<br>◦ *port* es el puerto restringido solo para inquilinos<br>◦ *20-digit-account-id* Es el ID de cuenta único del inquilino |

**Información relacionada**

- Controlar el acceso mediante firewalls
- Gestione servicios de plataformas para cuentas de inquilinos de S3

## Cambiar la contraseña del usuario raíz local del inquilino

Puede que necesite cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz está bloqueado en la cuenta.

**Lo que necesitará**

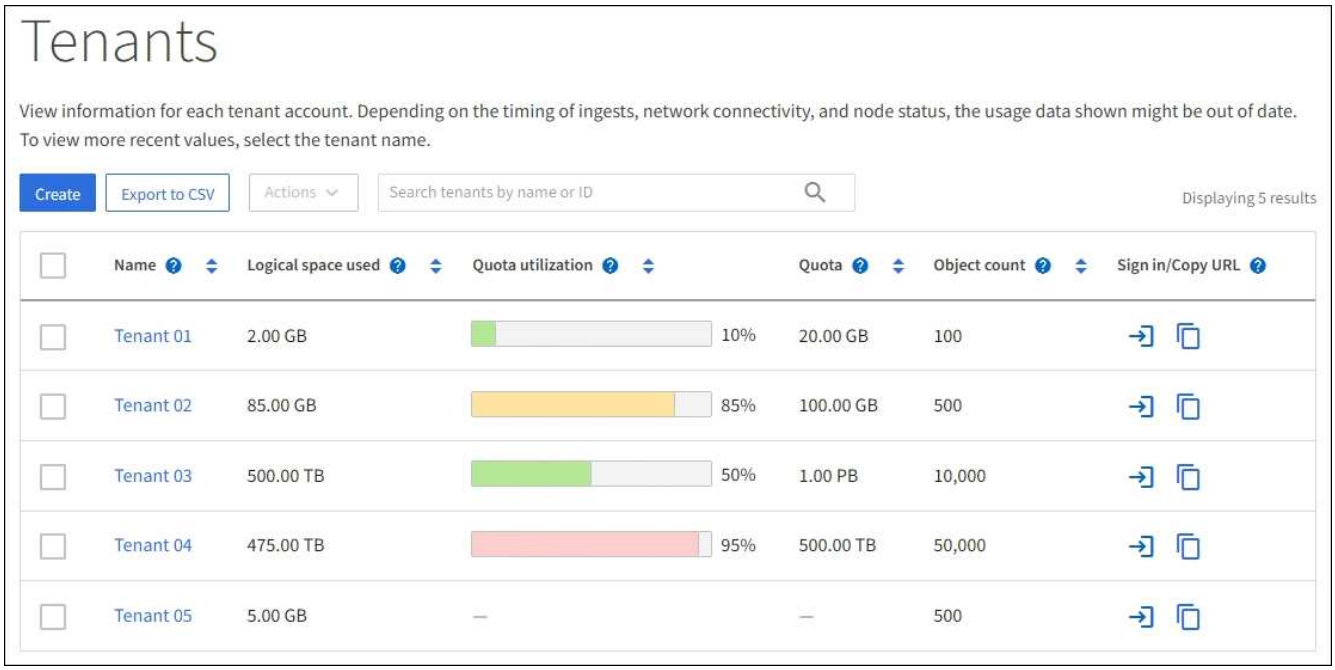
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta de inquilino. Para realizar tareas de usuario raíz, los usuarios deben pertenecer a un grupo federado que tenga el permiso acceso raíz para el arrendatario.

**Pasos**

1. Seleccione **ARRENDATARIOS**.




2. Seleccione la cuenta de arrendatario que desee editar.

   Se habilita el botón Actions.

3. En el menú desplegable **acciones**, seleccione **Cambiar contraseña raíz**.
4. Introduzca la nueva contraseña de la cuenta de inquilino.
5. Seleccione **Guardar**.

## Edite la cuenta de inquilino

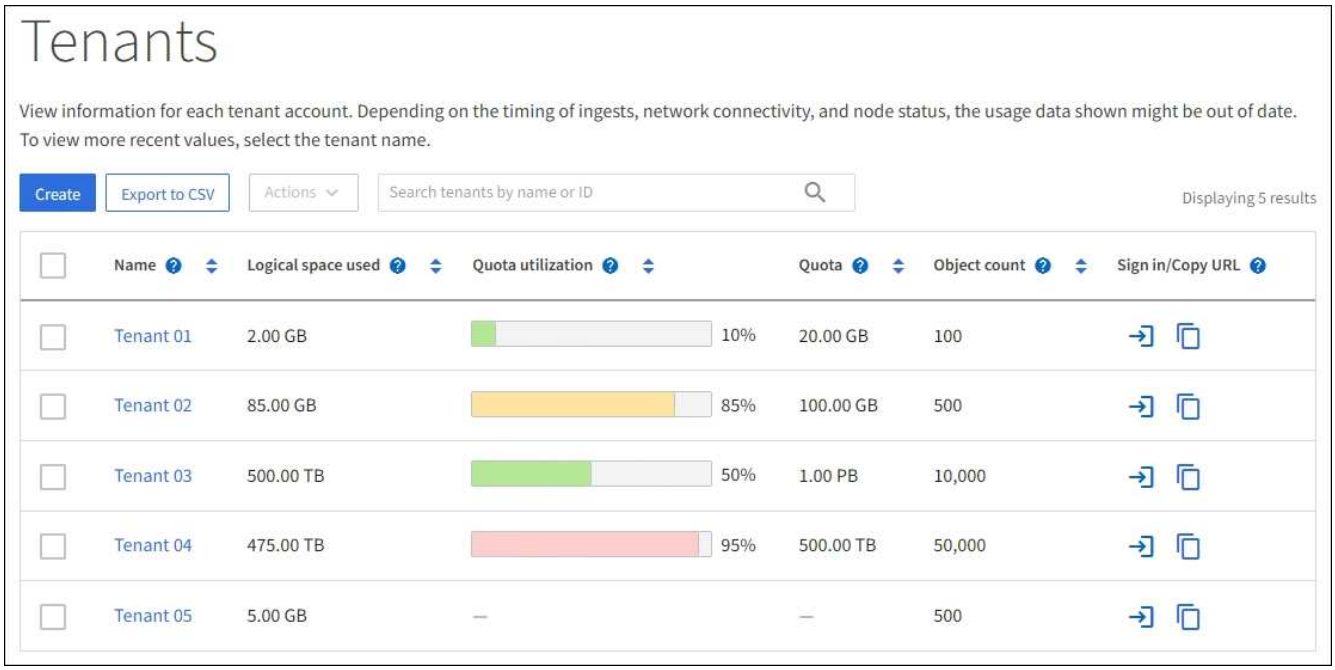
Puede editar una cuenta de arrendatario para cambiar el nombre para mostrar, cambiar la configuración del origen de identidad, permitir o desactivar servicios de plataforma o introducir una cuota de almacenamiento.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Pasos**

1. Seleccione **ARRENDATARIOS**.

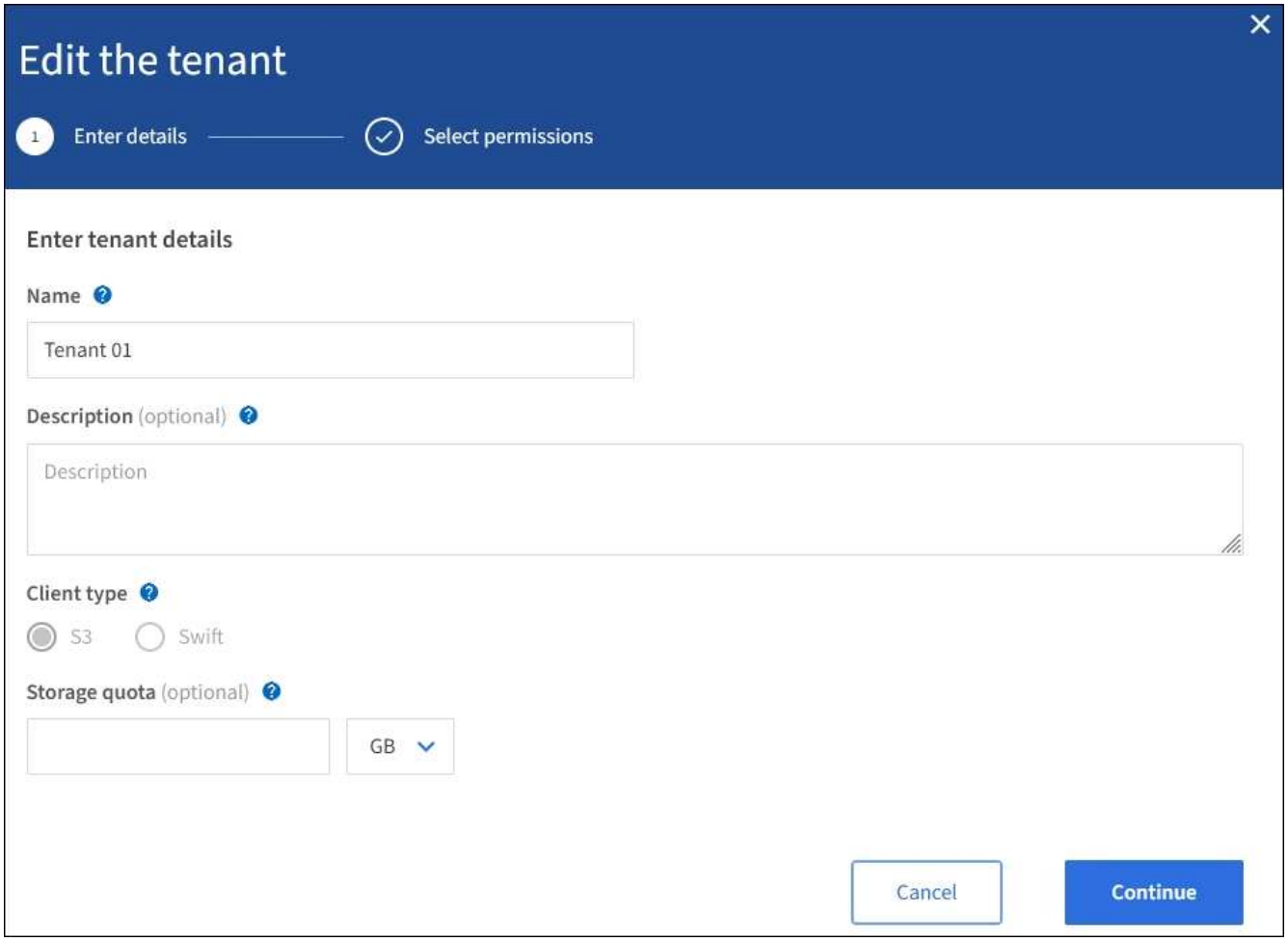



2. Seleccione la cuenta de arrendatario que desee editar.

   Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre o ID de inquilino.

3. En el menú desplegable acciones, seleccione **Editar**.

   Este ejemplo se utiliza para una cuadrícula que no utiliza el inicio de sesión único (SSO). Esta cuenta de inquilino no ha configurado su propio origen de identidad.




4. Cambie los valores de estos campos según sea necesario:
   - **Nombre**
   - **Descripción**
   - **Tipo de cliente**
   - **Cuota de almacenamiento**
5. Seleccione **continuar**.
6. Seleccione o anule la selección de los permisos para la cuenta de inquilino.
   - Si deshabilita **Servicios de plataforma** para un arrendatario que ya los está utilizando, los servicios que han configurado para sus cubos S3 dejarán de funcionar. No se envía ningún mensaje de error al inquilino. Por ejemplo, si el inquilino ha configurado la replicación de CloudMirror para un bloque de S3, podrán seguir almacenando objetos en el bloque, pero las copias de esos objetos ya no se realizarán en el bloque S3 externo que se hayan configurado como extremo.
   - Cambie la configuración de la casilla de verificación **usa el origen de identidad propio** para determinar si la cuenta de arrendatario utilizará su propio origen de identidad o el origen de identidad configurado para el administrador de cuadrícula.

     Si la casilla de verificación **usa el origen de identidad propio** es:

     - Desactivado y seleccionado, el arrendatario ya ha activado su propio origen de identidad. Un arrendatario debe desactivar su origen de identidad antes de poder utilizar el origen de identidad configurado para el Gestor de cuadrícula.

        - Deshabilitado e ilimitado, SSO se encuentra habilitado para el sistema StorageGRID. El inquilino debe utilizar el origen de identidad configurado para el administrador de grid.
    - Activa o desactiva **S3 Select** según sea necesario. Consulte Gestione S3 Select para cuentas de inquilinos.
7. Seleccione **Guardar**.

**Información relacionada**

- Gestione servicios de plataformas para cuentas de inquilinos de S3
- Usar una cuenta de inquilino

## Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar de forma permanente el acceso del inquilino al sistema.

**Lo que necesitará**

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- Debe haber quitado todos los bloques (S3), los contenedores (Swift) y los objetos asociados con la cuenta de inquilino.

**Pasos**

1. Seleccione **ARRENDATARIOS**.
2. Seleccione la cuenta de arrendatario que desea eliminar.

   Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre o ID de inquilino.
3. En el menú desplegable **acciones**, seleccione **Eliminar**.
4. Seleccione **OK**.

## Gestione los servicios de la plataforma

### Gestione servicios de plataformas para cuentas de inquilinos de S3

Si habilita los servicios de plataforma para cuentas de inquilino de S3, debe configurar su grid para que los inquilinos puedan acceder a los recursos externos necesarios para usar estos servicios.

#### ¿Qué son los servicios de plataforma?

Los servicios de plataforma incluyen la replicación de CloudMirror, las notificaciones de eventos y el servicio de integración de búsqueda.

Estos servicios permiten a los inquilinos utilizar la siguiente funcionalidad con sus bloques S3:

- **Duplicación de CloudMirror**: El servicio de replicación de CloudMirror de StorageGRID se utiliza para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

  Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en

Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

> La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.

- **Notificaciones**: Las notificaciones de eventos por bloque se usan para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon simple Notification Service™ (SNS) externo especificado.

  Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

  > Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

- **Servicio de integración de búsqueda**: El servicio de integración de búsqueda se usa para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos utilizando el servicio externo.

  Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

  > Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma ofrecen a los inquilinos la capacidad de usar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis con sus datos. Puesto que la ubicación objetivo para los servicios de plataforma suele ser externa a la implementación de StorageGRID, debe decidir si desea permitir a los inquilinos utilizar estos servicios. Si lo hace, debe habilitar el uso de servicios de plataforma al crear o editar cuentas de inquilino. También debe configurar la red de modo que los mensajes de servicios de plataforma que generan los inquilinos puedan llegar a sus destinos.

#### Recomendaciones para el uso de servicios de plataformas

Antes de utilizar los servicios de plataforma, tenga en cuenta las siguientes recomendaciones:

- Si un bloque de S3 del sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, también debe habilitar el control de versiones de bloques de S3 para el extremo de destino. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el extremo.
- No debe usar más de 100 inquilinos activos con solicitudes S3 que requieran la replicación, las notificaciones y la integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede dar como resultado un rendimiento del cliente S3 más lento.
- Las solicitudes a un extremo que no se puedan completar se pondrán en cola para un máximo de 500,000 solicitudes. Este límite se comparte por igual entre los inquilinos activos. Los nuevos inquilinos pueden superar temporalmente este límite de 500,000 para que los nuevos inquilinos no se vean penalizados de forma injusta.

**Información relacionada**

- Usar una cuenta de inquilino
- Configure las opciones de proxy de almacenamiento
- Supervisión y solución de problemas

**Red y puertos para servicios de plataforma**

Si permite que un inquilino de S3 utilice los servicios de plataforma, debe configurar las redes para el grid para garantizar que los mensajes de servicios de plataforma se puedan entregar a sus destinos.

Puede habilitar los servicios de plataforma para una cuenta de inquilino de S3 al crear o actualizar la cuenta de inquilino. Si se habilitan los servicios de plataforma, el inquilino puede crear extremos que sirvan como destino para la replicación de CloudMirror, notificaciones de eventos o mensajes de integración de búsqueda desde sus bloques de S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los extremos de destino.

Por ejemplo, los inquilinos pueden configurar los siguientes tipos de extremos de destino:

- Un clúster de Elasticsearch alojado localmente
- Aplicación local que admite la recepción de mensajes del servicio de notificación simple (SNS)
- Un bloque de S3 alojado localmente en la misma instancia de StorageGRID u otra
- Un extremo externo, como un extremo en Amazon Web Services.

Para garantizar que los mensajes de servicios de plataforma se puedan entregar, debe configurar la red o las redes que contienen los nodos de almacenamiento ADC. Debe asegurarse de que se pueden utilizar los siguientes puertos para enviar mensajes de servicios de plataforma a los extremos de destino.

De forma predeterminada, los mensajes de servicios de plataforma se envían a los siguientes puertos:

- **80**: Para los URI de punto final que comienzan con http
- **443**: Para los URI de punto final que comienzan con https

Los inquilinos pueden especificar un puerto diferente cuando crean o editan un extremo.

> Si se usa una puesta en marcha de StorageGRID como destino de la replicación de CloudMirror, podrían recibirse mensajes de replicación en un puerto distinto de 80 o 443. Compruebe que el puerto que se utiliza para S3 en la implementación de StorageGRID de destino se especifique en el extremo.

Si utiliza un servidor proxy no transparente, también debe hacerlo Configure las opciones de proxy de almacenamiento para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

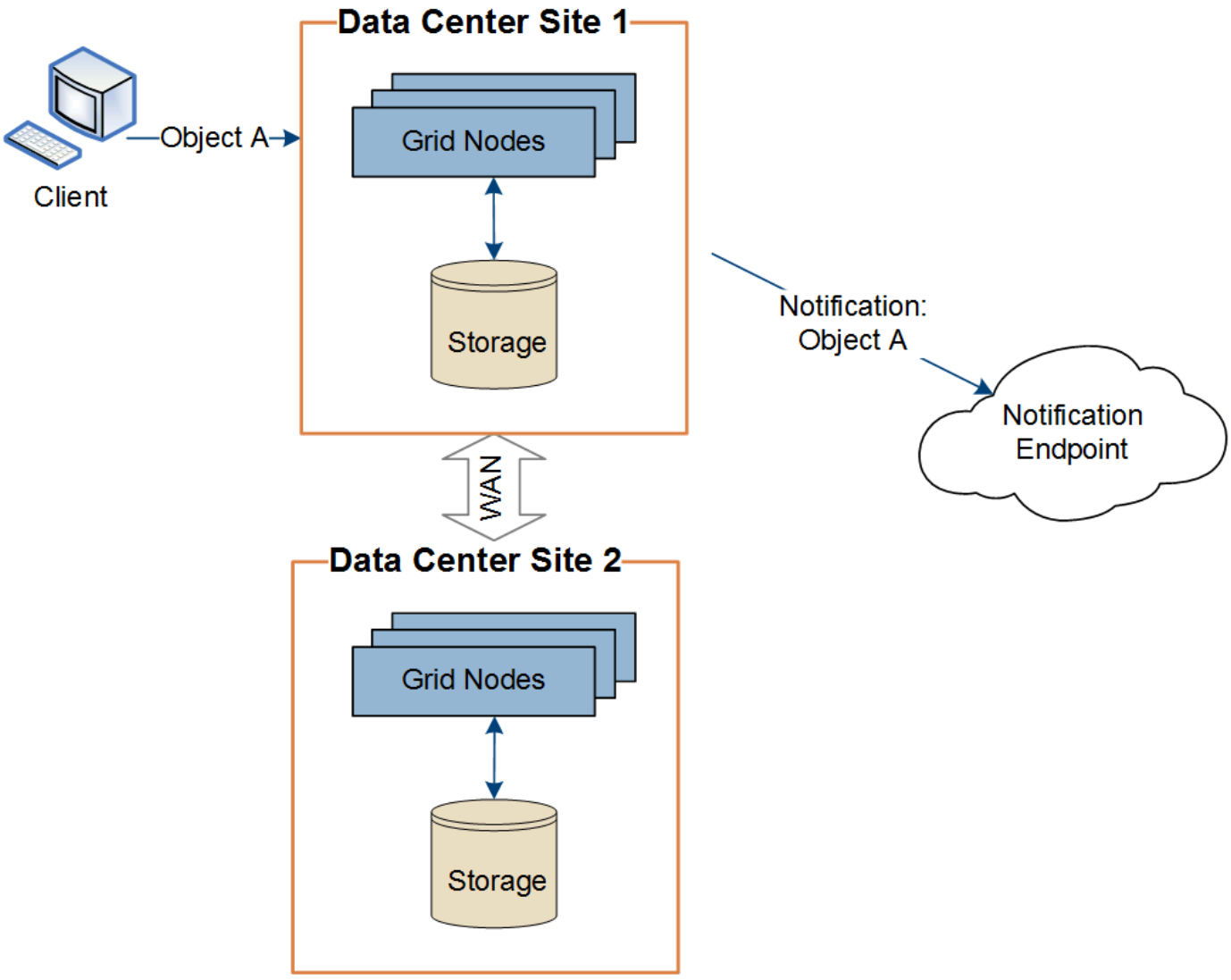
**Información relacionada**

- Usar una cuenta de inquilino

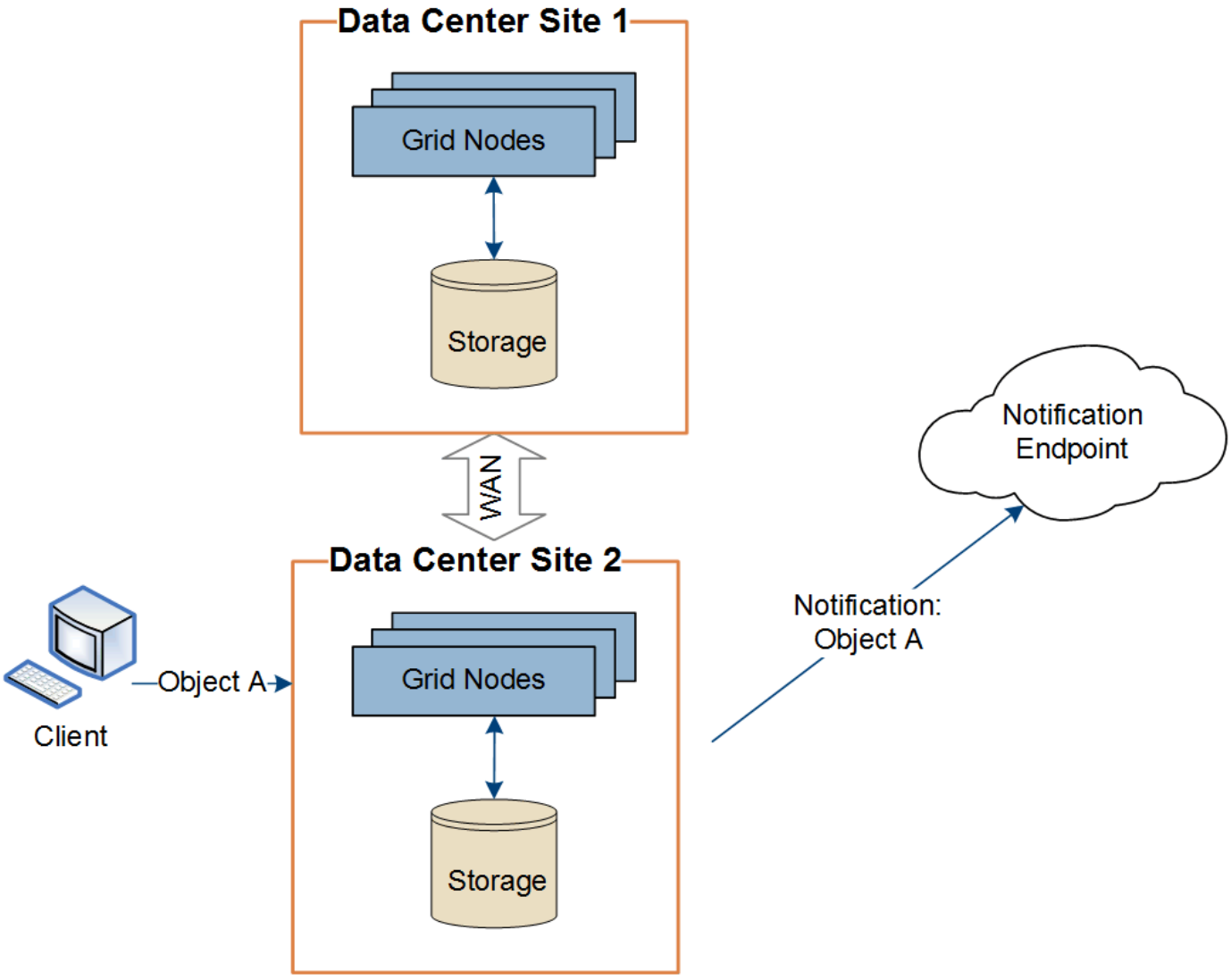
**Entrega de mensajes de servicios de plataforma por sitio**

Todas las operaciones de servicios de plataforma se realizan in situ.

Es decir, si un inquilino utiliza un cliente para realizar una operación S3 API Create en un objeto conectando a un nodo de puerta de enlace en el sitio 1 del centro de datos, se activa y envía la notificación acerca de esa acción desde el sitio 1 del centro de datos.




Si el cliente realiza posteriormente una operación de eliminación de API de S3 en ese mismo objeto desde el centro de datos Sitio 2, se activa y envía la notificación sobre la acción de eliminación desde el centro de datos Sitio 2.




Asegúrese de que la red de cada sitio esté configurada de modo que los mensajes de servicios de la plataforma se puedan entregar a sus destinos.

#### Solucione problemas de servicios de plataforma

Los extremos utilizados en los servicios de plataforma los crean y mantienen los usuarios de arrendatarios en el Administrador de arrendatarios; sin embargo, si un arrendatario tiene problemas al configurar o utilizar servicios de plataforma, puede utilizar el Administrador de grid para ayudar a resolver el problema.

##### Problemas con nuevos extremos

Para que un inquilino pueda utilizar los servicios de plataforma, deben crear uno o varios extremos mediante el administrador de inquilinos. Cada extremo representa un destino externo para un servicio de plataforma, como un bloque de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple o un clúster de Elasticsearch alojado localmente o en AWS. Cada extremo incluye la ubicación del recurso externo y las credenciales que se necesitan para acceder a ese recurso.

Cuando un inquilino crea un extremo, el sistema StorageGRID valida que existe el extremo y que se puede acceder a él utilizando las credenciales que se han especificado. La conexión con el extremo se valida desde un nodo en cada sitio.

Si falla la validación del punto final, un mensaje de error explica por qué falló la validación del punto final. El usuario inquilino debe resolver el problema y, a continuación, intentar crear el extremo de nuevo.

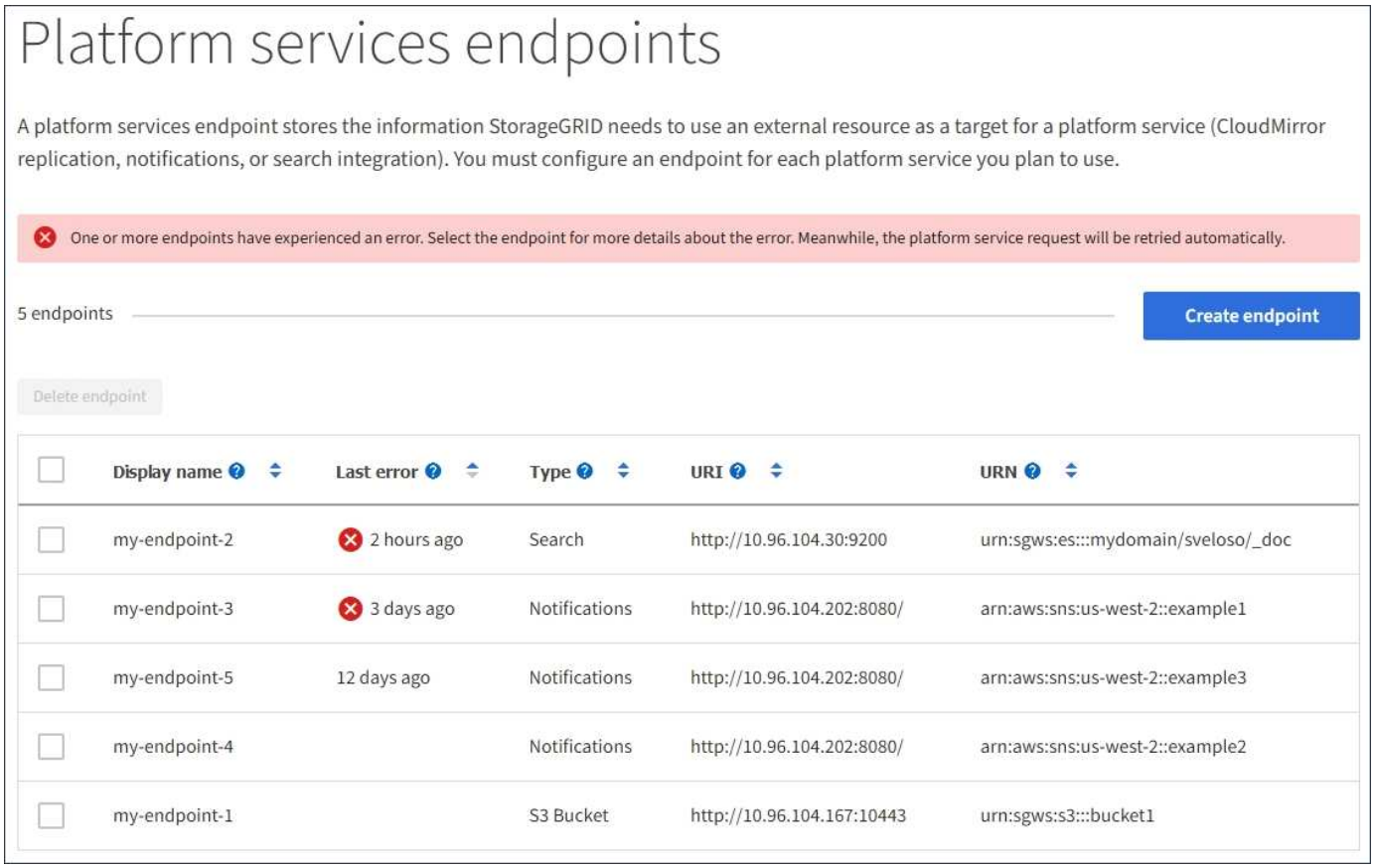
Se producirá un error al crear el extremo si los servicios de plataforma no están habilitados para la cuenta de inquilino.

**Problemas con los extremos existentes**

Si se produce un error cuando StorageGRID intenta acceder a un extremo existente, se muestra un mensaje en la consola del administrador de inquilinos.

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Los usuarios de arrendatarios pueden ir a la página endpoints para revisar el mensaje de error más reciente de cada extremo y determinar cuánto tiempo ha ocurrido el error. La columna **último error** muestra el mensaje de error más reciente para cada extremo e indica cuánto tiempo se produjo el error. Errores que incluyen el icono se ha producido en los últimos 7 días.




Algunos mensajes de error en la columna **último error** pueden incluir un identificador de registro entre paréntesis. Un administrador de grid o soporte técnico puede usar este ID para encontrar información más detallada sobre el error en bycast.log.

#### Problemas relacionados con los servidores proxy

Si configuró un proxy de almacenamiento entre nodos de almacenamiento y extremos de servicio de plataforma, se pueden producir errores si el servicio del proxy no permite los mensajes de StorageGRID. Para resolver estos problemas, compruebe la configuración del servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no están bloqueados.

#### Determine si se ha producido un error

Si se han producido errores de extremo en los últimos 7 días, la consola del administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página endpoints para ver más detalles sobre el error.

#### Error en las operaciones del cliente

Algunos problemas de los servicios de plataforma pueden provocar errores en las operaciones del cliente en el bloque de S3. Por ejemplo, las operaciones del cliente S3 fallarán si se detiene el servicio interno Replicated State Machine (RSM) o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node*** > **SSM** > **Servicios**.

#### Errores de punto final recuperables e irrecuperables

Una vez creados los extremos, los errores de solicitud de servicio de la plataforma pueden producirse por varios motivos. Algunos errores se pueden recuperar con la intervención del usuario. Por ejemplo, pueden producirse errores recuperables por los siguientes motivos:

- Las credenciales del usuario se han eliminado o han caducado.
- El bloque de destino no existe.
- La notificación no se puede entregar.

Si StorageGRID encuentra un error recuperable, la solicitud de servicio de la plataforma se reintentará hasta que se complete correctamente.

Otros errores son irrecuperables. Por ejemplo, se produce un error irrecuperable si se elimina el extremo.

Si StorageGRID encuentra un error de punto final irrecuperable, la alarma heredada total de eventos (SMTT) se activa en el Administrador de grid. Para ver la alarma de legado total de eventos:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***node*** > **SSM** > **Eventos**.
3. Ver último evento en la parte superior de la tabla.

   Los mensajes de eventos también se muestran en la `/var/local/log/bycast-err.log`.

4. Siga las instrucciones proporcionadas en el contenido de la alarma SMTT para corregir el problema.
5. Seleccione la ficha **Configuración** para restablecer los recuentos de eventos.
6. Notifique al inquilino los objetos cuyos mensajes de servicios de plataforma no se han entregado.
7. Indique al inquilino que vuelva a activar la replicación o notificación fallida actualizando los metadatos o las

etiquetas del objeto.

El arrendatario puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

#### Los mensajes de servicios de la plataforma no se pueden entregar

Si el destino encuentra un problema que le impide aceptar mensajes de servicios de plataforma, la operación de cliente en el bloque se realiza correctamente, pero el mensaje de servicios de plataforma no se entrega. Por ejemplo, este error puede ocurrir si se actualizan las credenciales en el destino de modo que StorageGRID ya no pueda autenticarse en el servicio de destino.

Si no se pueden entregar mensajes de servicios de plataforma debido a un error irrecuperable, la alarma heredada total de eventos (SMTT) se activa en Grid Manager.

#### Rendimiento más lento para las solicitudes de servicio de la plataforma

El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino.

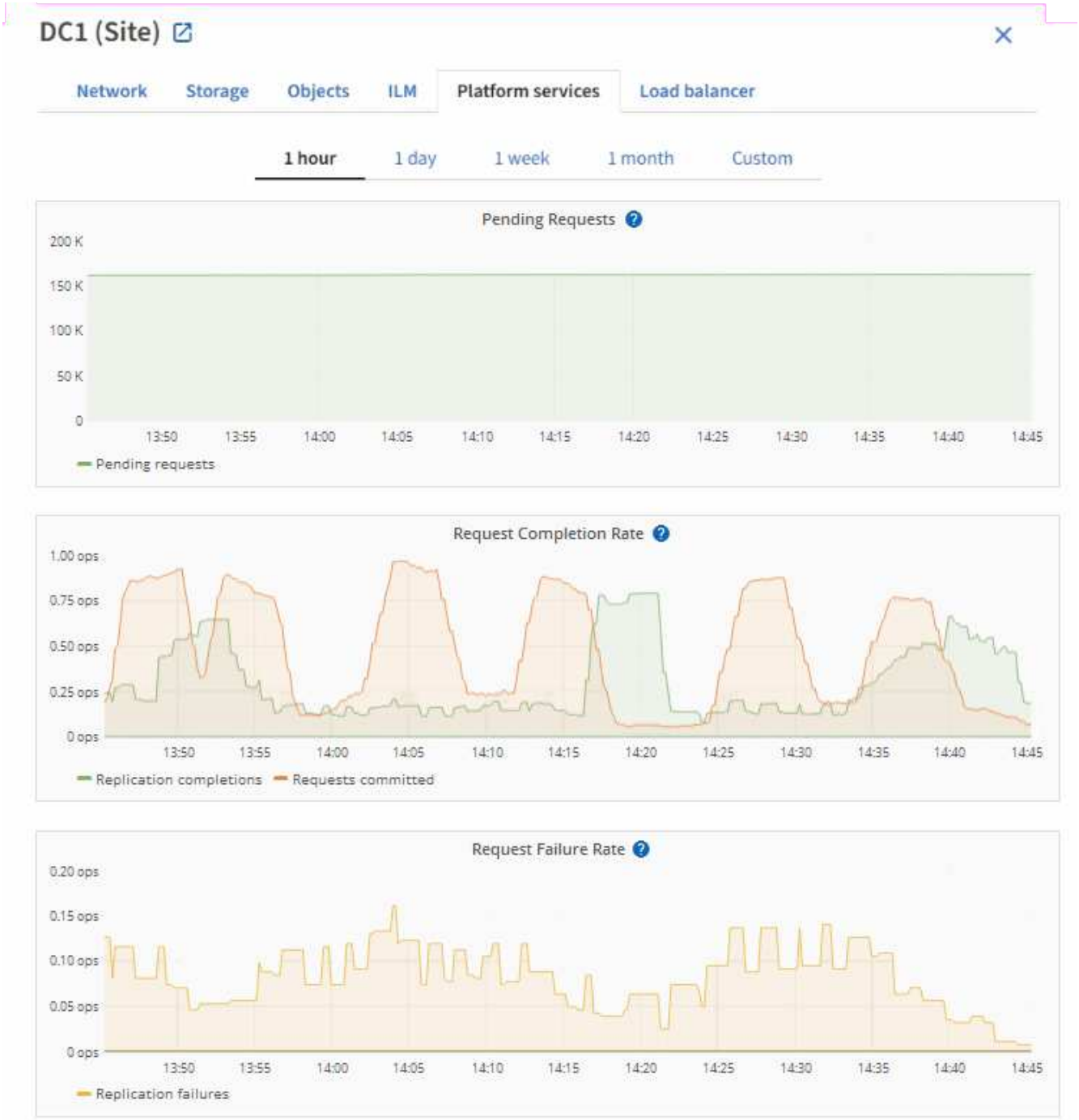
El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro.

Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

#### Las solicitudes de servicio de la plataforma fallan

Para ver la tasa de fallos de solicitud para servicios de plataforma:

1. Seleccione **NODES**.
2. Seleccione ***site*** > **Servicios de plataforma**.
3. Vea el gráfico de tasa de errores de solicitud.




**Alerta de servicios de plataforma no disponibles**

La alerta **Servicios de plataforma no disponibles** indica que no se pueden realizar operaciones de servicio de plataforma en un sitio porque hay demasiados nodos de almacenamiento con el servicio RSM en ejecución o disponibles.

El servicio RSM garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos extremos.

Para resolver esta alerta, determine qué nodos de almacenamiento del sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC). A continuación, asegúrese de que la mayoría simple de estos nodos de almacenamiento esté en funcionamiento y disponible.

Si se produce un error en más de un nodo de almacenamiento que contiene el servicio RSM de un sitio, perderá las solicitudes de servicio de plataforma pendientes para ese sitio.

#### Orientación adicional para la solución de problemas para extremos de servicios de la plataforma

Para obtener información adicional sobre la solución de problemas de los extremos de servicios de la plataforma, consulte las instrucciones para usar una cuenta de inquilino.

#### Información relacionada

- Supervisión y solución de problemas
- Configure las opciones de proxy de almacenamiento

## Gestione S3 Select para cuentas de inquilinos

Puede permitir que determinados inquilinos S3 usen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select proporciona una forma eficiente de buscar en grandes cantidades de datos sin tener que implementar una base de datos y recursos asociados para permitir las búsquedas. También reduce el coste y la latencia de la recuperación de datos.

### ¿Qué es S3 Select?

S3 Select permite que los clientes S3 utilicen solicitudes SelectObjectContent para filtrar y recuperar solo los datos necesarios de un objeto. La implementación de StorageGRID de S3 Select incluye un subconjunto de comandos y funciones de S3 Select.

### Consideraciones y requisitos para usar S3 Select

StorageGRID requiere lo siguiente para consultas S3 Select:

- El objeto que desea consultar tiene el formato CSV o es un archivo comprimido GZIP o BZIP2 que contiene un archivo con formato CSV.
- El administrador de grid debe otorgar a los inquilinos la capacidad de S3 Select. Seleccione **permitir selección de S3** cuando crear un inquilino o. edición de un arrendatario.
- La solicitud SelectObjectContent debe enviarse a un Extremo del equilibrador de carga de StorageGRID. Los nodos de administración y puerta de enlace que utiliza el extremo deben ser nodos de dispositivo SG100 o SG1000 o nodos de software basados en VMware.

Tenga en cuenta las siguientes limitaciones:

- No se admiten los nodos de equilibrador de carga de configuración básica.
- Las consultas no se pueden enviar directamente a los nodos de almacenamiento.
- Las consultas enviadas a través del servicio CLB obsoleto no son compatibles.

Las solicitudes SelectObjectContent pueden reducir el rendimiento de equilibrio de carga de todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Consulte Instrucciones para usar S3 Select.

Para ver Gráficos Grafana Para las operaciones de S3 Select a lo largo del tiempo, seleccione **SUPPORT** > **Tools** > **Metrics** en Grid Manager.

# Configure las conexiones de clientes S3 y Swift

## Acerca de las conexiones de los clientes S3 y Swift

Como administrador de grid, gestiona las opciones de configuración que controlan cómo los inquilinos S3 y Swift pueden conectar las aplicaciones cliente con el sistema StorageGRID para almacenar y recuperar datos. Hay una serie de opciones diferentes para responder a los distintos requisitos de cliente y cliente.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad

> El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Opcionalmente, puede configurar las siguientes funciones en el sistema StorageGRID:

- * Interfaces VLAN*: Puede crear interfaces LAN virtuales (VLAN) en nodos de administración y nodos de puerta de enlace para aislar y dividir el tráfico de cliente y cliente para seguridad, flexibilidad y rendimiento. Después de crear una interfaz VLAN, lo debe agregar a un grupo de alta disponibilidad.
- **Grupos de alta disponibilidad**: Puede crear un grupo ha de las interfaces para nodos de puerta de enlace o nodos de administración para crear una configuración de copia de seguridad activa, o puede utilizar DNS round-robin o un equilibrador de carga de terceros y varios grupos ha para lograr una configuración activo-activo. Las conexiones de clientes se realizan mediante las direcciones IP virtuales de los grupos de alta disponibilidad.
- **Servicio de equilibrador de carga**: Puede permitir a los clientes utilizar el servicio de equilibrador de carga mediante la creación de puntos finales de equilibrador de carga para las conexiones de cliente. Al crear un extremo de equilibrio de carga, especifica un número de puerto, si el extremo acepta conexiones HTTP o HTTPS, el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).
- **Red cliente no confiable**: Puede hacer que la Red cliente sea más segura configurándola como no confiable. Cuando la red de cliente no es de confianza, los clientes sólo pueden conectarse utilizando puntos finales de equilibrador de carga.

También es posible habilitar el uso de HTTP para los clientes que se conectan a StorageGRID directamente a los nodos de almacenamiento o mediante el servicio CLB (obsoleto), y es posible configurar los nombres de dominio de extremo de la API de S3 para los clientes S3.

## Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

**Acerca de esta tarea**

Esta tabla resume las distintas formas en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. En las instrucciones se describe cómo encontrar esta información en Grid Manager si ya se han configurado puntos finales de equilibrador de carga y grupos de alta disponibilidad (ha).

| Dónde se realiza la conexión | Servicio al que se conecta el cliente | Dirección IP | Puerto |
|---|---|---|---|
| Grupo de ALTA DISPONIBILIDAD | Equilibrador de carga | La dirección IP virtual de un grupo de alta disponibilidad | • Puerto de punto final del equilibrador de carga |
| Grupo de ALTA DISPONIBILIDAD | CLB<br><br>**Nota:** el servicio CLB está en desuso. | La dirección IP virtual de un grupo de alta disponibilidad | Puertos S3 predeterminados:<br>• HTTPS: 8082<br>• HTTP: 8084<br><br>Puertos Swift predeterminados:<br>• HTTPS:8083<br>• HTTP: 8085 |
| Nodo de administración | Equilibrador de carga | La dirección IP del nodo de administrador | • Puerto de punto final del equilibrador de carga |
| Nodo de puerta de enlace | Equilibrador de carga | La dirección IP del nodo de puerta de enlace | • Puerto de punto final del equilibrador de carga |

| Dónde se realiza la conexión | Servicio al que se conecta el cliente | Dirección IP | Puerto |
|---|---|---|---|
| Nodo de puerta de enlace | CLB<br><br>**Nota:** el servicio CLB está en desuso. | La dirección IP del nodo de puerta de enlace<br><br>**Nota:** de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados. | Puertos S3 predeterminados:<br>• HTTPS: 8082<br>• HTTP: 8084<br>Puertos Swift predeterminados:<br>• HTTPS:8083<br>• HTTP: 8085 |
| Nodo de almacenamiento | LDR | La dirección IP del nodo de almacenamiento | Puertos S3 predeterminados:<br>• HTTPS: 18082<br>• HTTP: 18084<br>Puertos Swift predeterminados:<br>• HTTPS: 18083<br>• HTTP: 18085 |

**Ejemplos**

Para conectar un cliente S3 al extremo de equilibrio de carga de un grupo ha de nodos de puerta de enlace, utilice una URL estructurada como se muestra a continuación:

- `https://VIP-of-HA-group:LB-endpoint-port`

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.5 y el número de puerto de un extremo de equilibrio de carga de S3 es 10443, un cliente de S3 puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.5:10443`

Para conectar un cliente Swift al extremo Load Balancer de un grupo de ha de nodos de Gateway, utilice una URL estructurada como se muestra a continuación:

- `https://VIP-of-HA-group:LB-endpoint-port`

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.6 y el número de puerto de un extremo de equilibrio de carga de Swift es 10444, un cliente de Swift puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.6:10444`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a

StorageGRID. Póngase en contacto con el administrador de red local.

**Pasos**

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. Para encontrar la dirección IP de un nodo de grid:
   a. Seleccione **NODES**.
   b. Seleccione el nodo de administrador, Gateway Node o Storage Node al que desea conectarse.
   c. Seleccione la ficha **Descripción general**.
   d. En la sección Node Information, tenga en cuenta las direcciones IP del nodo.
   e. Seleccione **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaz.

      Puede establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

      - **Eth0:** Red Grid
      - **Eth1:** Red de administración (opcional)
      - **Eth2:** Red cliente (opcional)

      > Si va a ver un nodo de administrador o un nodo de puerta de enlace y es el nodo activo de un grupo de alta disponibilidad, en eth2 se muestra la dirección IP virtual del grupo de alta disponibilidad.

3. Para buscar la dirección IP virtual de un grupo de alta disponibilidad:
   a. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
   b. En la tabla, tenga en cuenta la dirección IP virtual del grupo ha.
4. Para buscar el número de puerto de un extremo Load Balancer:
   a. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.

      Aparece la página Load Balancer Endpoints, donde se muestra la lista de puntos finales que ya se han configurado.

   b. Seleccione un punto final y seleccione **Editar punto final**.

      Se abre la ventana Edit Endpoint y se muestran detalles adicionales sobre el extremo.

   c. Confirme que el extremo que ha seleccionado está configurado para su uso con el protocolo correcto (S3 o Swift) y, a continuación, seleccione **Cancelar**.
   d. Tenga en cuenta el número de puerto del extremo que desea utilizar para una conexión de cliente.

      > Si el número de puerto es 80 o 443, el extremo se configura únicamente en los nodos de puerta de enlace, ya que esos puertos están reservados en los nodos de administración. Todos los demás puertos están configurados tanto en los nodos de puerta de enlace como en los de administración.

## Configure las interfaces VLAN

Puede crear interfaces de LAN virtual (VLAN) en nodos de administrador y de puerta de enlace, y usarlas en grupos de alta disponibilidad y extremos de equilibrador de carga

para aislar y dividir el tráfico para garantizar la seguridad, la flexibilidad y el rendimiento.

### Consideraciones sobre las interfaces VLAN

- Para crear una interfaz de VLAN, introduzca un ID de VLAN y elija una interfaz principal en uno o varios nodos.
- Se debe configurar una interfaz padre como interfaz troncal en el conmutador.
- Una interfaz principal puede ser Grid Network (eth0), Client Network (eth2) o una interfaz troncal adicional para la máquina virtual o el host con configuración básica (por ejemplo, ens256).
- Para cada interfaz de VLAN, solo puede seleccionar una interfaz principal para un nodo determinado. Por ejemplo, no puede utilizar tanto la interfaz de red de cuadrícula como la interfaz de red de cliente en el mismo nodo de puerta de enlace que la interfaz principal para la misma VLAN.
- Si la interfaz de VLAN es para el tráfico del nodo de administración, que incluye tráfico relacionado con el administrador de grid y el administrador de inquilinos, seleccione interfaces sólo en nodos de administración.
- Si la interfaz de VLAN es para el tráfico de clientes S3 o Swift, seleccione interfaces en nodos de administrador o nodos de puerta de enlace.
- Si necesita agregar interfaces de línea externa, consulte lo siguiente para obtener más información:
  - **VMware (después de instalar el nodo)**: VMware: Añada tronco o interfaces de acceso a un nodo
  - **RHEL o CentOS (antes de instalar el nodo)**: Crear archivos de configuración del nodo
  - **Ubuntu o Debian (antes de instalar el nodo)**: Crear archivos de configuración del nodo
  - **RHEL, CentOS, Ubuntu o Debian (después de instalar el nodo)**: Linux: Añada tronco o interfaces de acceso a un nodo

### Cree una interfaz VLAN

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Se ha configurado una interfaz de línea externa en la red y está conectada al nodo de máquina virtual o Linux. Conoce el nombre de la interfaz troncal.
- Conoce el ID de la VLAN que desea configurar.

#### Acerca de esta tarea

El administrador de red podría haber configurado una o más interfaces troncales y una o varias VLAN para separar el tráfico de administración o cliente que pertenezca a diferentes aplicaciones o inquilinos. Cada VLAN se identifica por un ID o etiqueta numéricos. Por ejemplo, la red puede utilizar VLAN 100 para el tráfico FabricPool y VLAN 200 para una aplicación de archivado.

Puede utilizar Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando se crean interfaces VLAN, se especifica el identificador de VLAN y se seleccionan las interfaces principales (troncales) en uno o varios nodos.

##### Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione **Crear**.

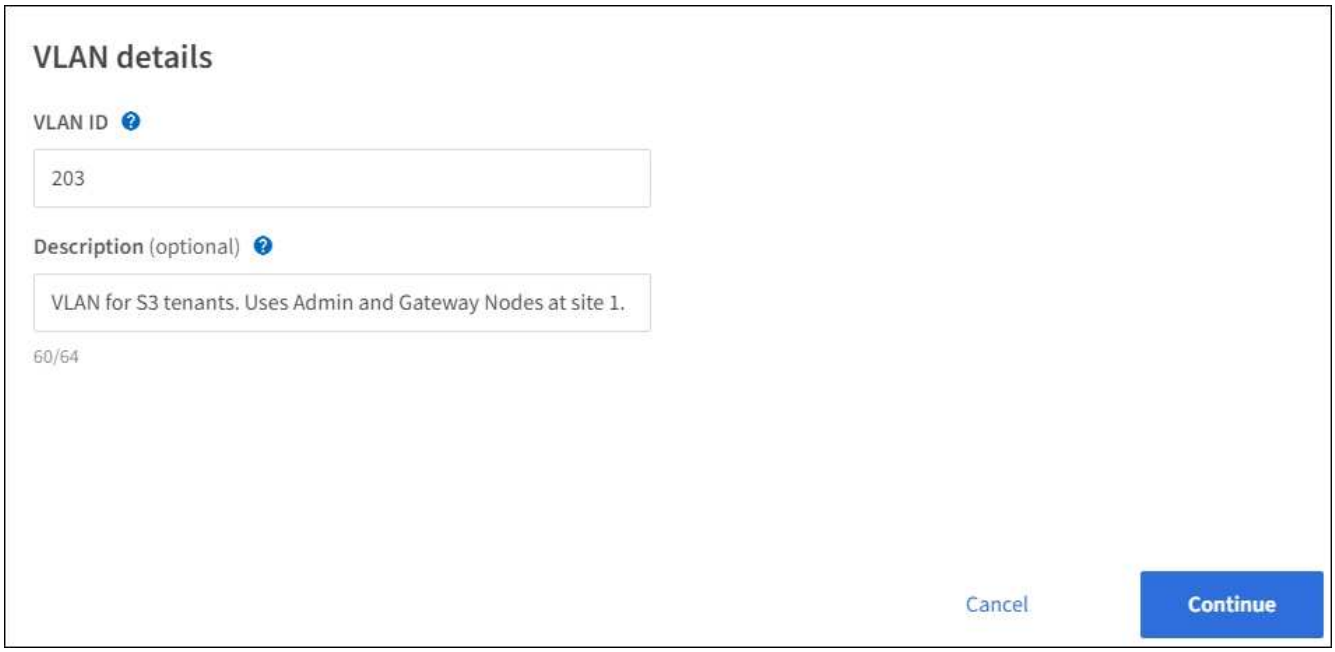
#### Introduzca los detalles de las interfaces de VLAN

1. Especifique el ID de la VLAN en la red. Puede introducir cualquier valor entre 1 y 4094.

   No es necesario que los ID de VLAN sean únicos. Por ejemplo, puede utilizar el identificador de VLAN 200 para el tráfico de administración en un sitio y el mismo identificador de VLAN para el tráfico de cliente en otro sitio. Puede crear interfaces VLAN independientes con diferentes conjuntos de interfaces principales en cada sitio. Sin embargo, dos interfaces VLAN con un mismo ID no pueden compartir la misma interfaz en un nodo.

   Si especifica un ID que ya se ha utilizado, aparecerá un mensaje. Puede continuar creando otra interfaz VLAN para la misma identificación de VLAN o puede seleccionar **Cancelar** y, a continuación, editar el ID existente.

2. De manera opcional, introduzca una breve descripción para la interfaz de VLAN.



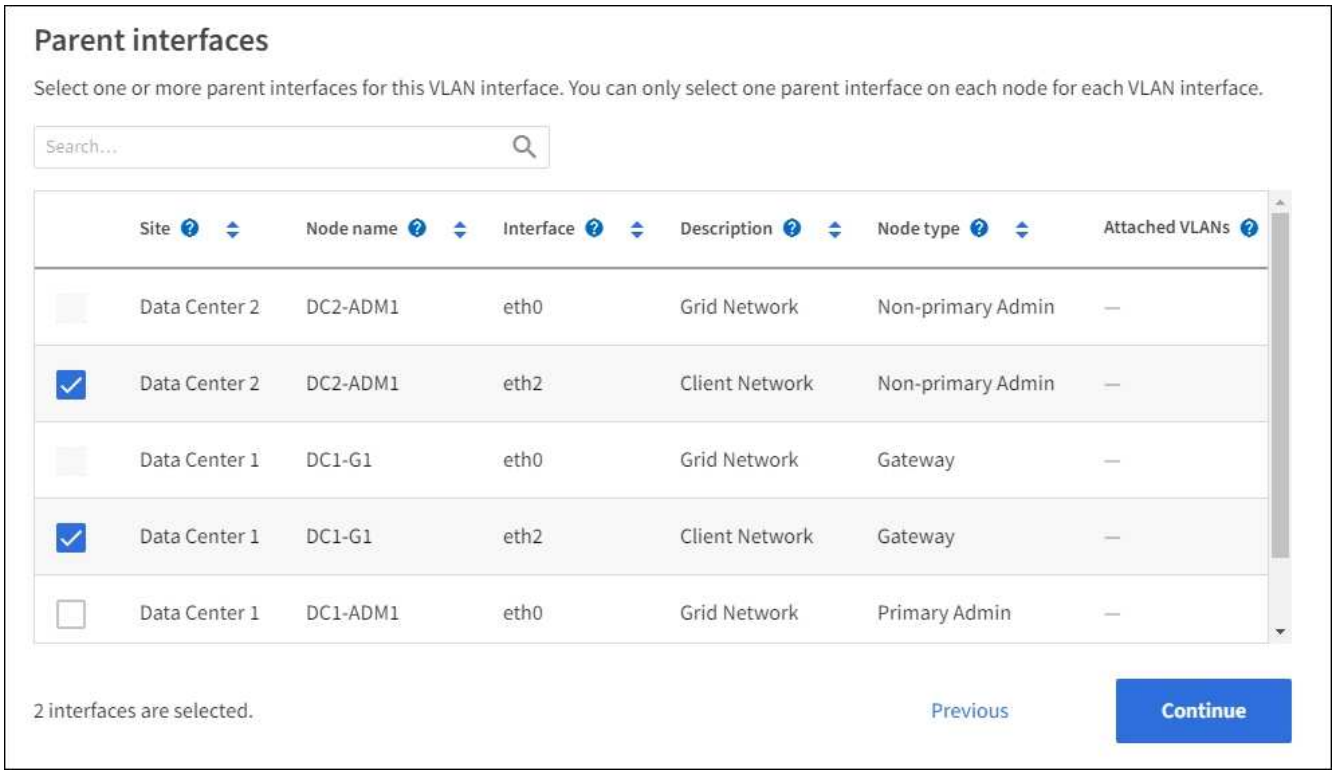

3. Seleccione **continuar**.

#### Elija interfaces padre

En la tabla, se enumeran las interfaces disponibles para todos los nodos de administrador y los nodos de puerta de enlace en cada sitio del grid. Las interfaces de red de administración (eth1) no se pueden utilizar como interfaces principales y no se muestran.

1. Seleccione una o varias interfaces primarias para asociar esta VLAN.

   Por ejemplo, es posible que desee conectar una VLAN a la interfaz de red de cliente (eth2) para un nodo de puerta de enlace y un nodo de administrador.




2. Seleccione **continuar**.

#### Confirme la configuración

1. Revise la configuración y realice cualquier cambio.
   - Si necesita cambiar el ID de VLAN o la descripción, seleccione **introducir detalles de VLAN** en la parte superior de la página.
   - Si necesita cambiar una interfaz padre, seleccione **elegir interfaces padre** en la parte superior de la página o seleccione **anterior**.
   - Si necesita quitar una interfaz principal, seleccione la papelera .
2. Seleccione **Guardar**.
3. Espere hasta 5 minutos para que la nueva interfaz aparezca como una selección en la página grupos de alta disponibilidad y aparezca en la tabla * interfaces de red* para el nodo (**NODES** > ***nodo de interfaz principal*** > **Red**).

### Edite una interfaz VLAN

Cuando edite una interfaz de VLAN, puede realizar los siguientes tipos de cambios:

- Cambie el ID o la descripción de la VLAN.
- Agregar o quitar interfaces principales.

Por ejemplo, es posible que desee quitar una interfaz principal de una interfaz VLAN si va a retirar el nodo asociado.

Tenga en cuenta lo siguiente:

- No puede cambiar un ID de VLAN si la interfaz VLAN se utiliza en un grupo de alta disponibilidad.

- No puede quitar una interfaz principal si se utiliza esa interfaz principal en un grupo de alta disponibilidad.

  Por ejemplo, supongamos que la VLAN 200 está conectada a las interfaces principales de los nodos A y B. Si un grupo de alta disponibilidad utiliza la interfaz VLAN 200 para el nodo A y la interfaz eth2 para el nodo B, puede quitar la interfaz principal sin usar para el nodo B, pero no puede quitar la interfaz principal utilizada para el nodo A.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione la casilla de comprobación de la interfaz de VLAN que desea editar. A continuación, seleccione **acciones** > **Editar**.
3. Si lo desea, actualice el ID de VLAN o la descripción. A continuación, seleccione **continuar**.

   No se puede actualizar un identificador de VLAN si la VLAN se utiliza en un grupo de alta disponibilidad.

4. Opcionalmente, active o anule la selección de las casillas de verificación para agregar interfaces padre o para eliminar interfaces no utilizadas. A continuación, seleccione **continuar**.
5. Revise la configuración y realice cualquier cambio.
6. Seleccione **Guardar**.

#### Quite una interfaz VLAN

Puede eliminar una o varias interfaces VLAN.

No puede quitar una interfaz VLAN si actualmente se utiliza en un grupo de alta disponibilidad. Para poder eliminarlo, debe quitar la interfaz VLAN del grupo ha.

Para evitar cualquier interrupción en el tráfico de cliente, considere realizar una de las siguientes acciones:

- Añada una nueva interfaz VLAN al grupo de alta disponibilidad antes de eliminar esta interfaz de VLAN.
- Cree un nuevo grupo de alta disponibilidad que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que desea quitar tiene actualmente la interfaz activa, edite el grupo de alta disponibilidad. Mueva la interfaz de VLAN que desea quitar a la parte inferior de la lista de prioridades. Espere hasta que se establezca la comunicación en la nueva interfaz principal y, a continuación, quite la interfaz antigua del grupo de alta disponibilidad. Por último, elimine la interfaz de VLAN en ese nodo.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione la casilla de comprobación de cada interfaz de VLAN que desea quitar. A continuación, seleccione **acciones** > **Eliminar**.
3. Seleccione **Sí** para confirmar su selección.

   Se eliminan todas las interfaces VLAN seleccionadas. Se muestra un banner verde de éxito en la página de interfaces de VLAN.

## Gestión de grupos de alta disponibilidad

## Gestionar grupos de alta disponibilidad: Descripción general

Puede agrupar las interfaces de red de varios nodos de administrador y puerta de enlace en un grupo de alta disponibilidad (ha). Si la interfaz activa del grupo de alta disponibilidad falla, una interfaz de backup puede administrar la carga de trabajo.

### ¿Qué es un grupo de alta disponibilidad?

Puede usar grupos de alta disponibilidad para proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift o proporcionar conexiones de alta disponibilidad a Grid Manager y Tenant Manager.

Cada grupo de alta disponibilidad proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de ALTA DISPONIBILIDAD que incluyen nodos de puerta de enlace, nodos de administrador o ambos proporcionan conexiones de datos con alta disponibilidad para los clientes S3 y Swift.
- Los grupos DE ALTA DISPONIBILIDAD que incluyen solo los nodos de administrador proporcionan conexiones de alta disponibilidad con el administrador de grid y el administrador de inquilinos.
- Un grupo de alta disponibilidad que sólo incluye dispositivos SG100 o SG1000 y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad Inquilinos de S3 que usan S3 Select. Se recomienda a los grupos de ALTA DISPONIBILIDAD cuando se usa S3 Select, pero no es obligatorio.

### ¿Cómo se crea un grupo de alta disponibilidad?

1. Debe seleccionar una interfaz de red para uno o más nodos de administrador o nodos de puerta de enlace. Puede usar una interfaz de red de cuadrícula (eth0), una interfaz de red de cliente (eth2), una interfaz VLAN o una interfaz de acceso que haya agregado al nodo.

   > No puede agregar una interfaz a un grupo de alta disponibilidad si tiene una dirección IP asignada por DHCP.

2. Se especifica una interfaz para ser la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.
3. El orden de prioridad de las interfaces de copia de seguridad se determina.
4. Asigne una a 10 direcciones IP virtuales (VIP) al grupo. Las aplicaciones cliente pueden utilizar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para ver instrucciones, consulte Configuración de grupos de alta disponibilidad.

### ¿Cuál es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo ha se añaden a la interfaz principal, que es la primera interfaz en el orden de prioridad. Siempre que la interfaz principal siga estando disponible, se utiliza cuando los clientes se conectan a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz primaria es la interfaz "'activa'" del grupo.

Del mismo modo, durante el funcionamiento normal, cualquier interfaz con menor prioridad para el grupo ha actúa como interfaces «'backup'». Estas interfaces de backup no se utilizan a menos que la interfaz primaria (actualmente activa) deje de estar disponible.

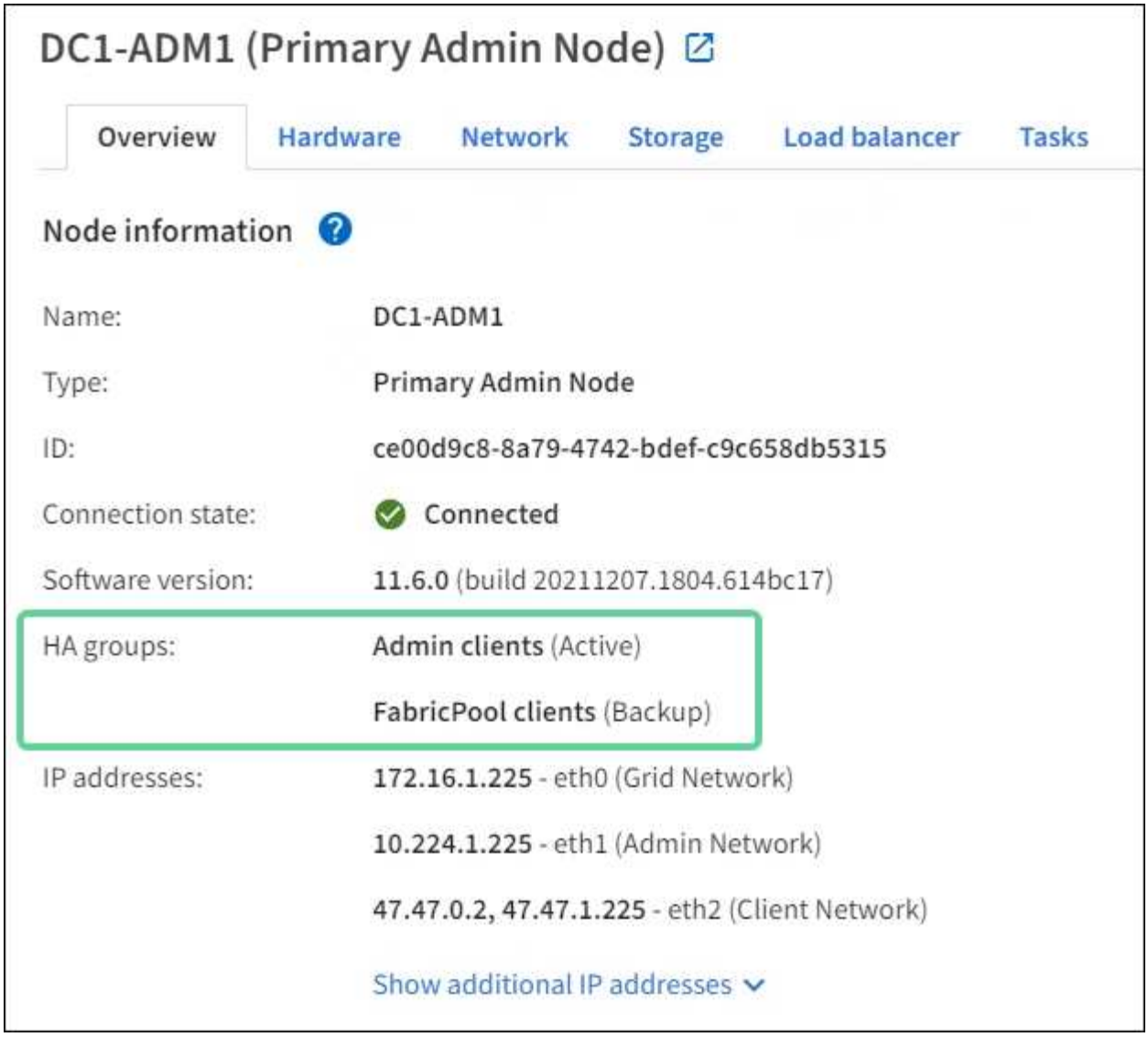
#### Ver el estado actual del grupo de alta disponibilidad de un nodo

Para ver si un nodo está asignado a un grupo ha y determinar su estado actual, seleccione **NODES** > ***node***.

Si la ficha **Descripción general** incluye una entrada para **grupos ha**, el nodo se asigna a los grupos ha enumerados. El valor después de que el nombre del grupo sea el estado actual del nodo del grupo de alta disponibilidad:

- **Activo**: El grupo ha se está alojando actualmente en este nodo.
- **Copia de seguridad**: El grupo ha no está utilizando actualmente este nodo; se trata de una interfaz de copia de seguridad.
- **Detenido**: El grupo ha no se puede alojar en este nodo porque el servicio de alta disponibilidad (keepalived) se ha detenido manualmente.
- **Fallo**: El grupo ha no se puede alojar en este nodo debido a una o más de las siguientes situaciones:
  - El servicio Load Balancer (nginx-gw) no se está ejecutando en el nodo.
  - La interfaz eth0 o VIP del nodo está inactiva.
  - El nodo está inactivo.

En este ejemplo, el nodo de administración principal se ha añadido a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa del grupo de clientes de administración y una interfaz de respaldo del grupo de clientes de FabricPool.




**¿Qué ocurre cuando falla la interfaz activa?**

La interfaz que aloja actualmente las direcciones VIP es la interfaz activa. Si el grupo ha incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se mueven a la primera interfaz de respaldo disponible en el orden de prioridad. Si falla esa interfaz, las direcciones VIP se mueven a la siguiente interfaz de respaldo disponible, etc.

La conmutación por error puede activarse por cualquiera de estas razones:

- El nodo en el que se configura la interfaz se desactiva.
- El nodo en el que se configura la interfaz pierde la conectividad con los demás nodos durante al menos 2 minutos.
- La interfaz activa se desactiva.
- El servicio Load Balancer se detiene.
- El servicio de alta disponibilidad se detiene.

Es posible que la conmutación al respaldo no se active por errores de red externos al nodo que aloja la interfaz activa. Del mismo modo, la conmutación por error no se activa con el fallo del servicio CLB (obsoleto) o los servicios para el administrador de grid o el administrador de inquilinos.

Por lo general, el proceso de recuperación tras fallos sólo se realiza en unos pocos segundos y es lo suficientemente rápido como para que las aplicaciones cliente tengan un impacto escaso y puedan confiar en los comportamientos normales de reintento para continuar con el funcionamiento.

Cuando se resuelve un fallo y hay una interfaz de mayor prioridad disponible de nuevo, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad disponible.

**¿Cómo se utilizan los grupos de alta disponibilidad?**

## Puede usar grupos de alta disponibilidad para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo de alta disponibilidad puede proporcionar conexiones administrativas de alta disponibilidad al administrador de grid o al administrador de inquilinos.
- Un grupo de alta disponibilidad puede proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift.
- Un grupo de alta disponibilidad que contiene una sola interfaz le permite proporcionar muchas direcciones VIP y establecer explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo proporcionan los mismos servicios. Cuando crea un grupo de alta disponibilidad, añada interfaces desde los tipos de nodos que proporcionan los servicios necesarios.

- **Admin Nodes**: Incluye el servicio Load Balancer y permite el acceso al Grid Manager o al arrendatario Manager.
- **Nodos de puerta de enlace**: Incluye el servicio Load Balancer y el servicio CLB (obsoleto).

| Objetivo del grupo de alta disponibilidad | Añada nodos de este tipo al grupo de alta disponibilidad |
|---|---|
| Acceso a Grid Manager | • Nodo de administración principal (**primario**)<br>• Nodos de administrador no primario<br><br>**Nota:** el nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal. |
| Acceso solo al administrador de inquilinos | • Nodos de administrador primario o no primario |
| Acceso al cliente de S3 o Swift: Servicio Load Balancer | • Nodos de administración<br>• Nodos de puerta de enlace |

| Objetivo del grupo de alta disponibilidad | Añada nodos de este tipo al grupo de alta disponibilidad |
| --- | --- |
| Acceso de clientes S3 para S3 Select | • Aparatos SG100 o SG1000<br>• Nodos de software basados en VMware<br><br>**Nota**: Se recomiendan los grupos DE HA cuando se usa S3 Select, pero no es necesario. |
| Acceso al cliente S3 o Swift: Servicio CLB<br><br>**Nota:** el servicio CLB está en desuso. | • Nodos de puerta de enlace |

#### Limitaciones en el uso de grupos de alta disponibilidad con Grid Manager o Intenant Manager

Si falla un servicio de Grid Manager o de arrendatario Manager, no se activa la conmutación por error del grupo de alta disponibilidad.

Si ha iniciado sesión en Grid Manager o en el arrendatario Manager cuando se produce la conmutación por error, ha cerrado sesión y debe volver a iniciar sesión para reanudar la tarea.

No se pueden realizar algunos procedimientos de mantenimiento cuando el nodo administrador principal no está disponible. Durante la conmutación por error, puede utilizar Grid Manager para supervisar el sistema StorageGRID.

#### Limitaciones del uso de grupos de alta disponibilidad con el servicio CLB

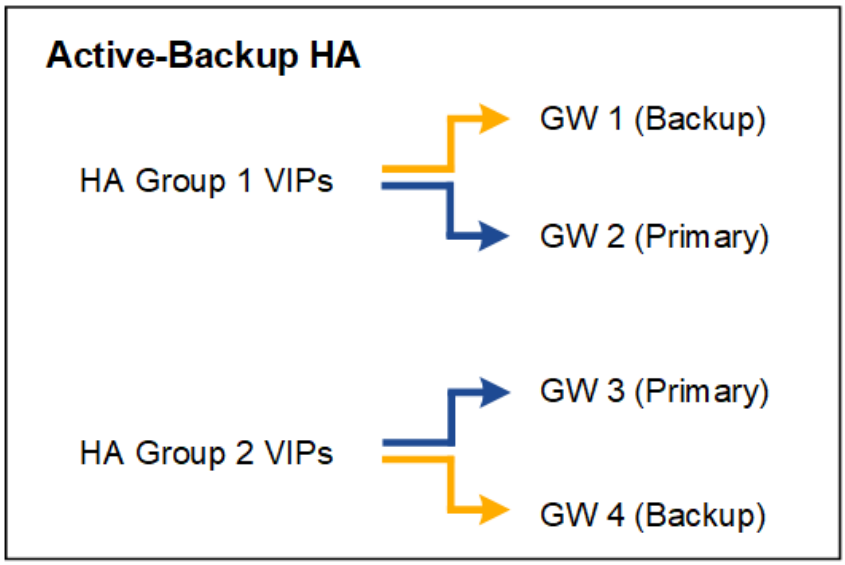
El error del servicio CLB no activa la conmutación por error dentro del grupo ha.

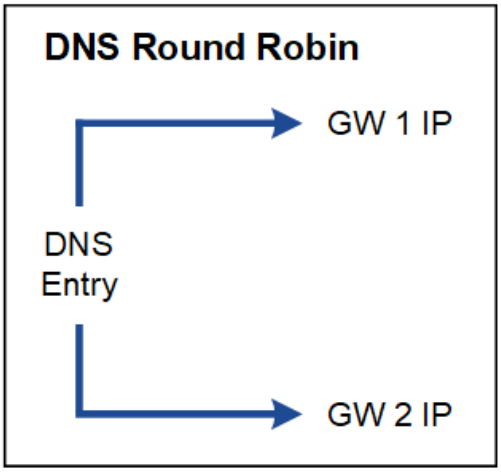
El servicio CLB está obsoleto.

### Opciones de configuración para grupos de alta disponibilidad

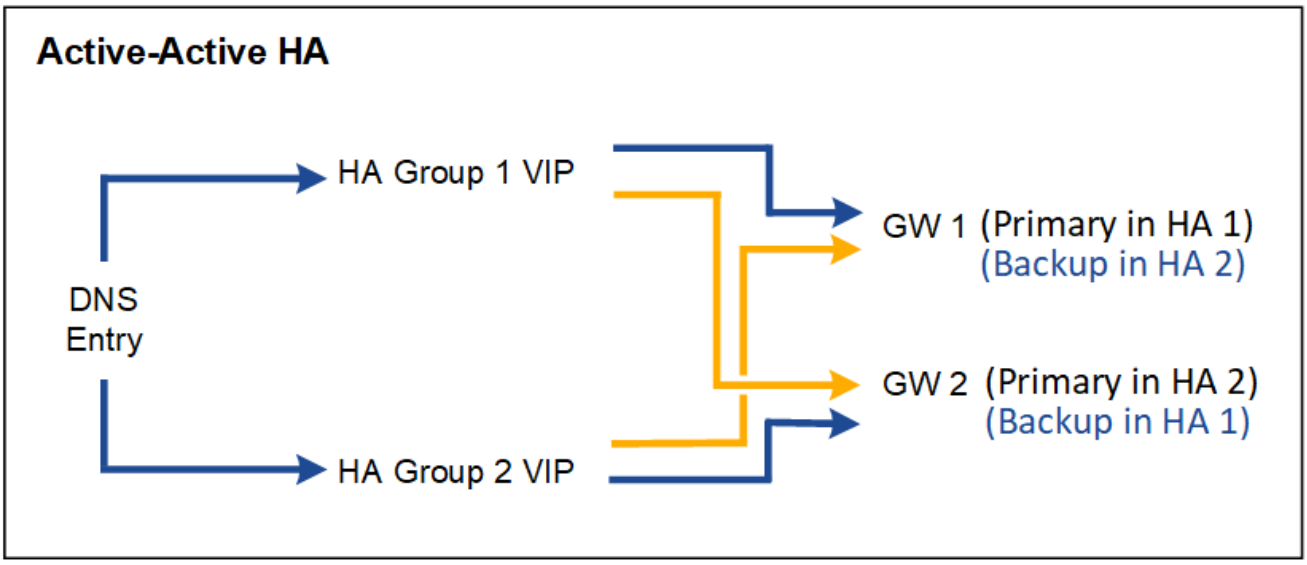
Los diagramas siguientes proporcionan ejemplos de diferentes formas de configurar grupos de alta disponibilidad. Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz primaria del grupo de alta disponibilidad y el amarillo indica la interfaz de backup del grupo de alta disponibilidad.




GW = Gateway Node
VIP = Virtual IP address




La tabla resume las ventajas de cada configuración de alta disponibilidad que se muestra en el diagrama.

| Configuración | Ventajas | Desventajas |
|---|---|---|
| Alta disponibilidad de Active-Backup | • Gestionada por StorageGRID sin dependencias externas.<br>• Rápida recuperación tras fallos. | • Solo un nodo de un grupo de alta disponibilidad está activo. Al menos un nodo por grupo de alta disponibilidad estará inactivo. |
| Operación por turnos DNS | • Mayor rendimiento total.<br>• Sin hosts inactivos. | • Conmutación al respaldo lenta, que puede depender del comportamiento del cliente.<br>• Requiere la configuración del hardware fuera de StorageGRID.<br>• Necesita una comprobación del estado implementada por el cliente. |

| Configuración | Ventajas | Desventajas |
| --- | --- | --- |
| Alta disponibilidad activo-activo | • El tráfico se distribuye entre varios grupos de alta disponibilidad.<br>• Alto rendimiento de agregado escalable con el número de grupos de alta disponibilidad.<br>• Rápida recuperación tras fallos. | • Más complejo de configurar.<br>• Requiere la configuración del hardware fuera de StorageGRID.<br>• Necesita una comprobación del estado implementada por el cliente. |

### Configuración de grupos de alta disponibilidad

Puede configurar grupos de alta disponibilidad para proporcionar acceso de alta disponibilidad a los servicios en nodos de administración o de puerta de enlace.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Si piensa utilizar una interfaz VLAN en un grupo de alta disponibilidad, ha creado la interfaz VLAN. Consulte Configure las interfaces VLAN.
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
  - **Red Hat Enterprise Linux o CentOS (antes de instalar el nodo)**: Crear archivos de configuración del nodo
  - **Ubuntu o Debian (antes de instalar el nodo)**: Crear archivos de configuración del nodo
  - **Linux (después de instalar el nodo)**: Linux: Añada tronco o interfaces de acceso a un nodo
  - **VMware (después de instalar el nodo)**: VMware: Añada tronco o interfaces de acceso a un nodo

#### Crear un grupo de alta disponibilidad

Cuando crea un grupo de alta disponibilidad, selecciona una o varias interfaces y las organiza por orden de prioridad. A continuación, debe asignar una o varias direcciones VIP al grupo.

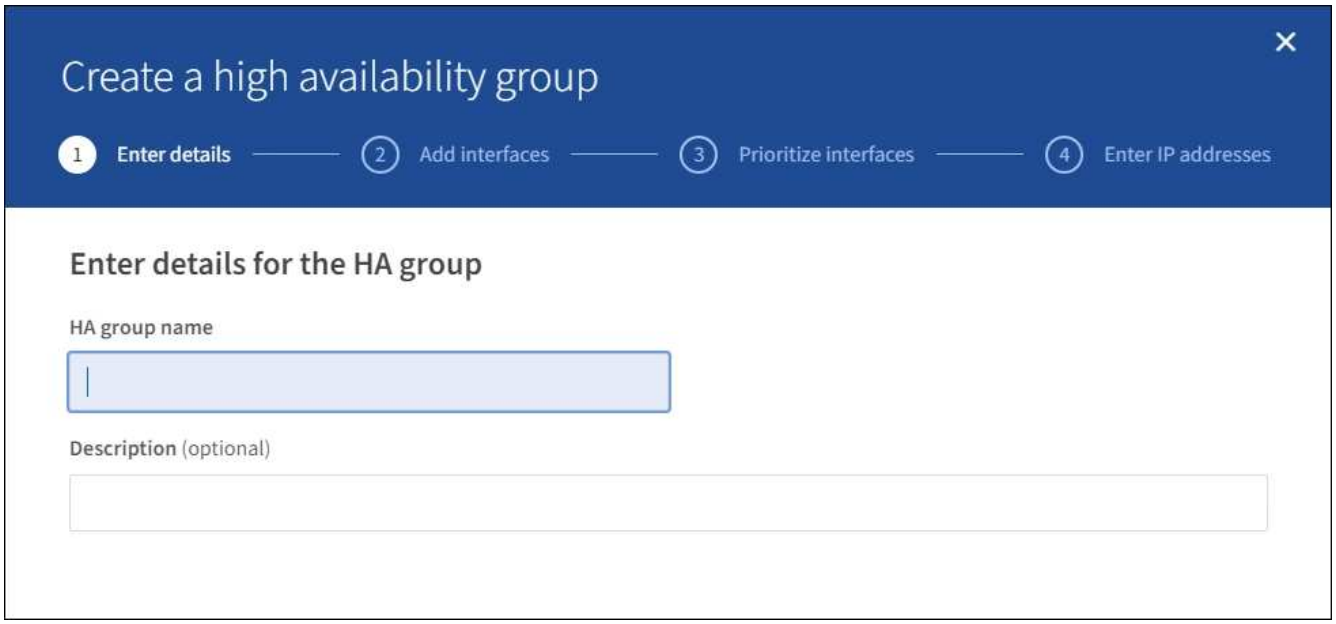
Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administrador se incluyan en un grupo de alta disponibilidad. Un grupo de alta disponibilidad solo puede usar una interfaz para cualquier nodo concreto; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de alta disponibilidad.

#### Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.

#### Introduzca los detalles del grupo de alta disponibilidad

1. Proporcione un nombre único para el grupo de alta disponibilidad.

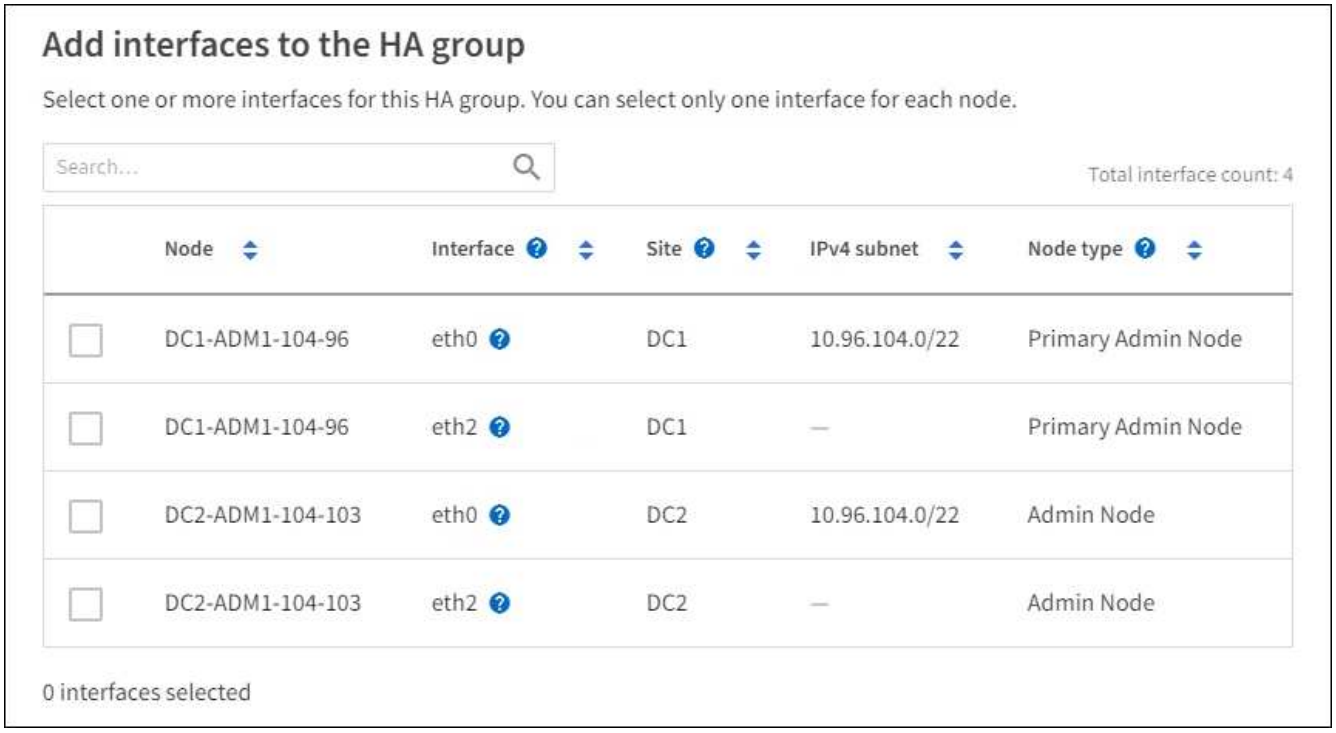



2. De forma opcional, puede introducir una descripción para el grupo de alta disponibilidad.
3. Seleccione **continuar**.

### Añada interfaces al grupo de alta disponibilidad

1. Seleccione una o varias interfaces para añadirlas a este grupo de alta disponibilidad.

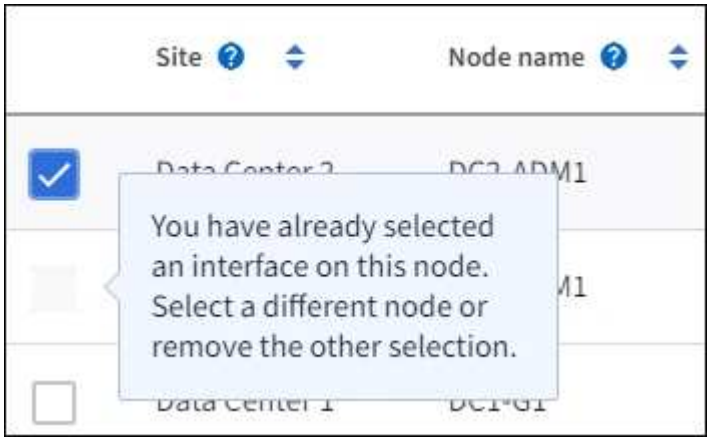
   Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.




Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

**Directrices para seleccionar interfaces**

- Debe seleccionar al menos una interfaz.
- Solo puede seleccionar una interfaz para un nodo.
- Si el grupo ha es para la protección de alta disponibilidad de los servicios Admin Node, que incluyen Grid Manager y el inquilino Manager, seleccione interfaces sólo en nodos de administrador.
- Si el grupo de alta disponibilidad está para la protección de alta disponibilidad de tráfico de cliente S3 o Swift, seleccione interfaces en nodos de administrador, nodos de puerta de enlace o ambos.
- Si el grupo ha es para la protección de alta disponibilidad del servicio CLB obsoleto, seleccione interfaces sólo en nodos de puerta de enlace.
- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación al respaldo, los servicios que proporciona el nodo que antes estaba activo podrían no estar disponibles en el nodo recién activo. Por ejemplo, un nodo de puerta de enlace de respaldo no puede ofrecer protección de alta disponibilidad de los servicios de nodo de administrador. Del mismo modo, un nodo de administrador de backup no puede realizar todos los procedimientos de mantenimiento que proporciona el nodo de administración principal.
- Si no puede seleccionar una interfaz, la casilla de verificación está desactivada. La sugerencia de herramienta proporciona más información.



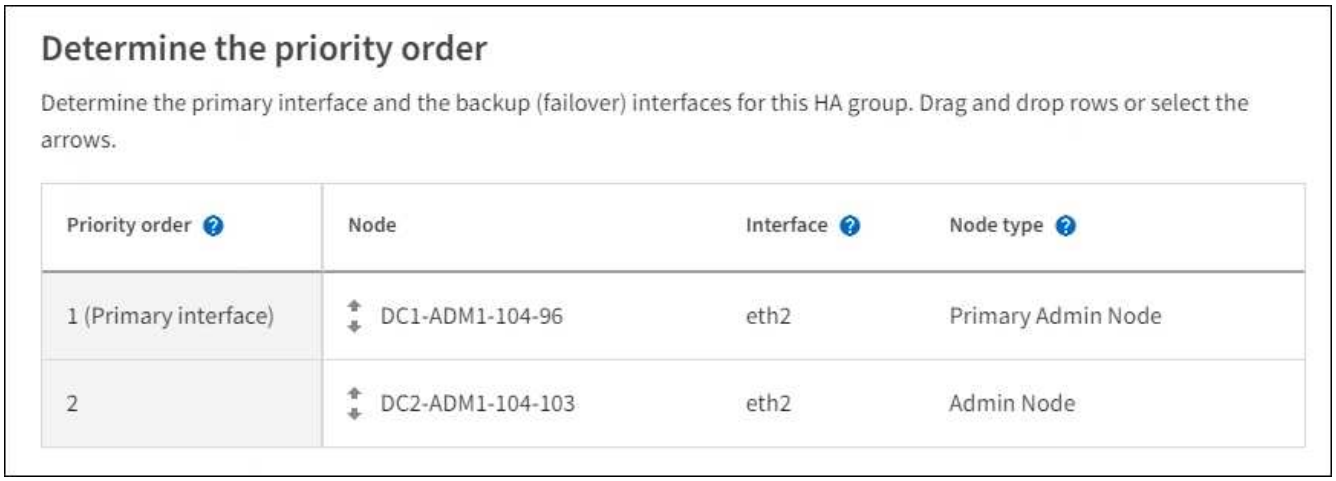

- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **continuar**.

**Determinar el orden de prioridad**

1. Determine la interfaz principal y cualquier interfaz de backup (conmutación al nodo de respaldo) para este grupo de alta disponibilidad.

   Arrastre y suelte filas para cambiar los valores de la columna **orden de prioridad**.




Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo ha incluye más de una interfaz y la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad disponible. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, etc.

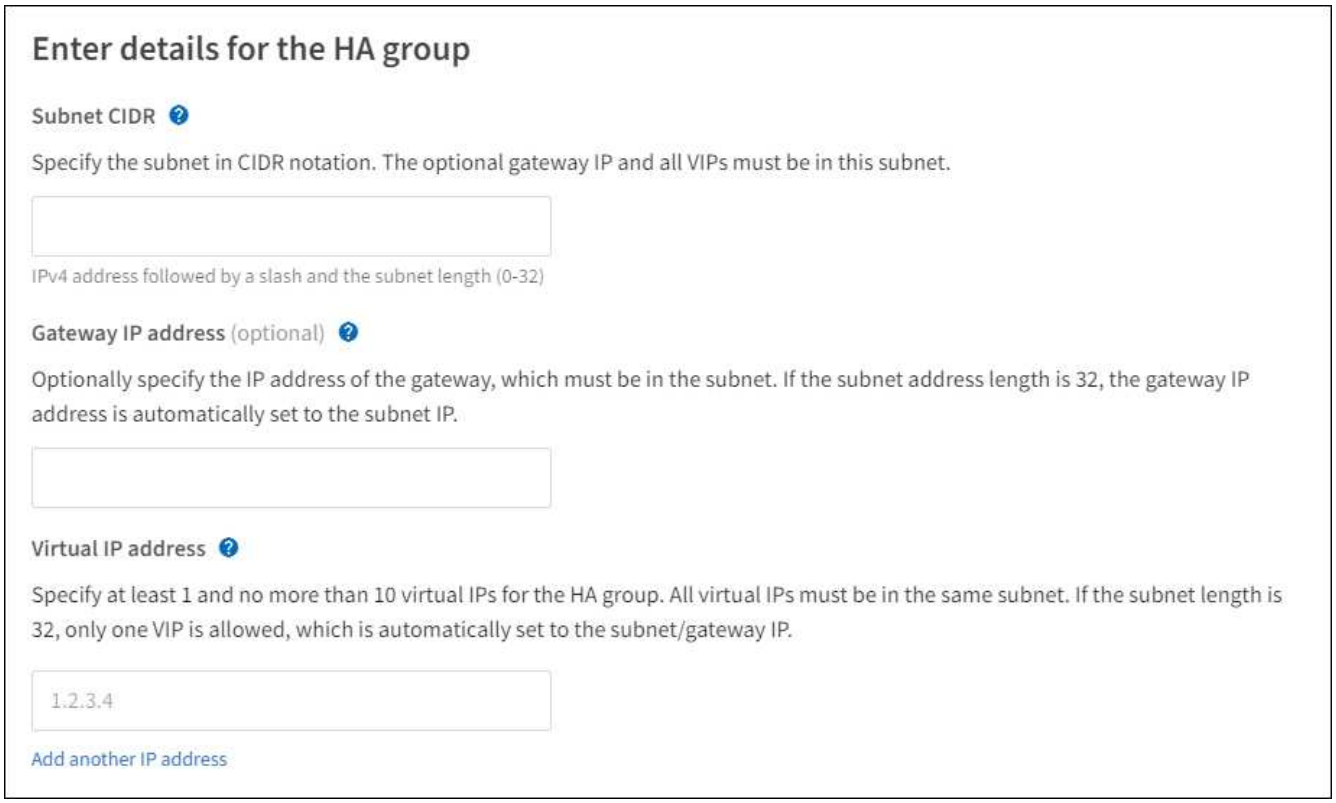
2. Seleccione **continuar**.

### Introduzca las direcciones IP

1. En el campo **CIDR de subred**, especifique la subred VIP en notación CIDR --una dirección IPv4 seguida de una barra y la longitud de subred (0-32).

   La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.

   Si utiliza un prefijo de 32 bits, la dirección de red VIP también funciona como dirección de puerta de enlace y dirección VIP.




2. De manera opcional, si alguno de los clientes S3, Swift, administrativos o de arrendatario accederá a estas direcciones VIP desde una subred diferente, introduzca la **dirección IP de la puerta de enlace**. La dirección de la puerta de enlace debe estar en la subred VIP.

   Los usuarios de cliente y administrador utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

3. Introduzca una o más **direcciones IP virtuales** para el grupo ha. Puede añadir hasta 10 direcciones IP. Todos los VIP deben estar dentro de la subred VIP.

   Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

4. Seleccione **Crear grupo ha** y seleccione **Finalizar**.

   El grupo ha se ha creado y ahora puede utilizar las direcciones IP virtuales configuradas.

> Espere hasta 15 minutos para que los cambios en un grupo de alta disponibilidad se apliquen a todos los nodos.

### Siguientes pasos

Si utilizará este grupo de ha para el equilibrio de carga, cree un extremo de equilibrio de carga para determinar el puerto y el protocolo de red y para conectar los certificados necesarios. Consulte Configurar puntos finales del equilibrador de carga.

#### Editar un grupo de alta disponibilidad

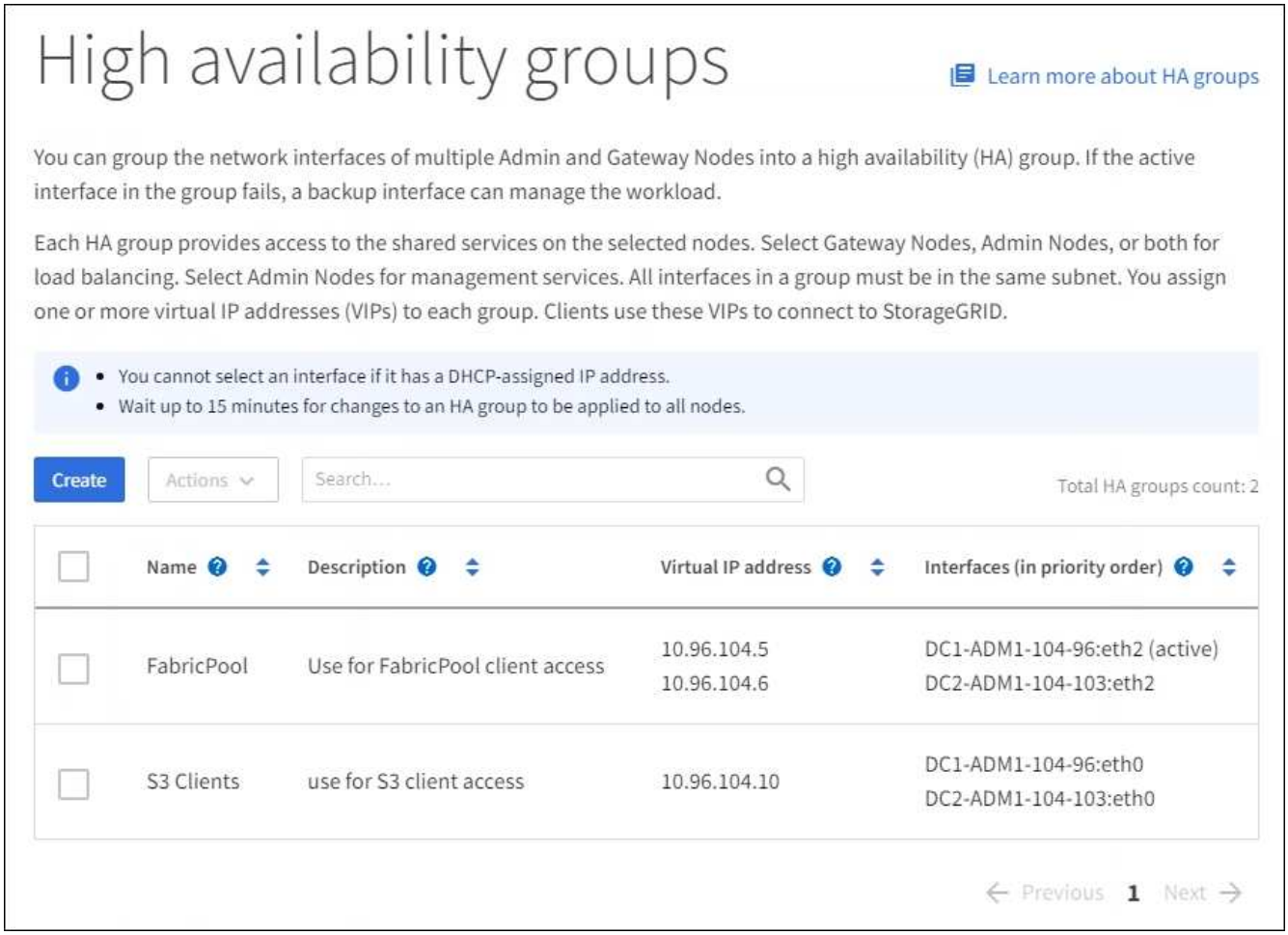
Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que deba editar un grupo de alta disponibilidad si desea quitar el nodo asociado a una interfaz seleccionada en un procedimiento de retirada del sitio o nodo.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.

   La página grupos de alta disponibilidad muestra todos los grupos de alta disponibilidad existentes.




2. Seleccione la casilla de comprobación del grupo de alta disponibilidad que desea editar.
3. Realice una de las siguientes acciones, según lo que desee actualizar:
   - Seleccione **acciones** > **Editar dirección IP virtual** para agregar o eliminar direcciones VIP.
   - Seleccione **acciones** > **Editar grupo ha** para actualizar el nombre o la descripción del grupo, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o quitar direcciones VIP.
4. Si ha seleccionado **Editar dirección IP virtual**:
   a. Actualice las direcciones IP virtuales del grupo de alta disponibilidad.
   b. Seleccione **Guardar**.
   c. Seleccione **Finalizar**.
5. Si ha seleccionado **Editar grupo ha**:
   a. Si lo desea, actualice el nombre o la descripción del grupo.
   b. Opcionalmente, active o anule la selección de las casillas de verificación para agregar o quitar interfaces.

Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal

c. Opcionalmente, arrastre y suelte filas para cambiar el orden de prioridad de la interfaz primaria y cualquier interfaz de copia de seguridad de este grupo ha.

d. De manera opcional, actualice las direcciones IP virtuales.

e. Seleccione **Guardar** y, a continuación, seleccione **Finalizar**.

Espere hasta 15 minutos para que los cambios en un grupo de alta disponibilidad se apliquen a todos los nodos.

#### Eliminar un grupo de alta disponibilidad

Puede eliminar uno o varios grupos de alta disponibilidad al mismo tiempo. Sin embargo, no puede eliminar un grupo ha si está enlazado a uno o más extremos de equilibrador de carga.

Para evitar que se produzcan interrupciones en el cliente, actualice las aplicaciones cliente S3 o Swift afectadas antes de quitar un grupo de alta disponibilidad. Actualice cada cliente para que se conecte mediante otra dirección IP, por ejemplo, la dirección IP virtual de un grupo ha diferente o la dirección IP configurada para una interfaz durante la instalación.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione la casilla de comprobación de cada grupo de alta disponibilidad que desea quitar. A continuación, seleccione **acciones** > **Eliminar grupo ha**.
3. Revise el mensaje y seleccione **Eliminar grupo ha** para confirmar su selección.

   Se eliminan todos los grupos de alta disponibilidad seleccionados. Aparecerá un banner verde de éxito en la página grupos de alta disponibilidad.

## Gestione el equilibrio de carga

### Gestionar el equilibrio de carga: Descripción general

Las funciones de equilibrio de carga de StorageGRID se pueden usar para manejar cargas de trabajo de procesamiento y recuperación de los clientes S3 y Swift. El equilibrio de carga maximiza la velocidad y la capacidad de conexión distribuyendo las cargas de trabajo y las conexiones entre varios nodos de almacenamiento.

Puede equilibrar las cargas de trabajo de clientes de las siguientes maneras:

- Use el servicio Load Balancer, que se instala en los nodos de administrador y de puerta de enlace. El servicio Load Balancer proporciona equilibrio de carga de capa 7 y realiza terminación TLS de solicitudes de cliente, inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento. Este es el mecanismo de equilibrio de carga recomendado.

  Consulte Cómo funciona el equilibrio de carga: Servicio de equilibrio de carga.

- Utilice el servicio de equilibrio de carga de conexión (CLB) obsoleto, que se instala sólo en nodos de puerta de enlace. El servicio CLB proporciona equilibrio de carga de capa 4 y soporta costes de enlace.

  Consulte Cómo funciona el equilibrio de carga: Servicio CLB (obsoleto).

- Integre un equilibrador de carga de terceros. Si desea obtener más información, póngase en contacto con el representante de cuenta de NetApp.

### Cómo funciona el equilibrio de carga: Servicio de equilibrio de carga

El servicio Load Balancer distribuye conexiones de red entrantes desde aplicaciones cliente hasta nodos de almacenamiento. Para habilitar el equilibrio de carga, debe configurar los extremos del equilibrador de carga mediante el Administrador de grid.

Puede configurar extremos de equilibrador de carga solo para nodos de administración o nodos de puerta de enlace, ya que estos tipos de nodos contienen el servicio Load Balancer. No se pueden configurar extremos para nodos de almacenamiento ni nodos de archivado.

Cada extremo de equilibrio de carga especifica un puerto, un protocolo de red (HTTP o HTTPS), un tipo de cliente (S3 o Swift) y un modo de enlace. Los extremos HTTPS requieren un certificado de servidor. Los modos de enlace permiten restringir la accesibilidad de los puertos de extremo a:

- Las direcciones IP virtuales (VIP) de grupos específicos de alta disponibilidad (ha)
- Interfaces de red específicas de nodos Admin y Gateway específicos

#### Consideraciones sobre el puerto

Los clientes pueden acceder a cualquiera de los extremos que configure en cualquier nodo que ejecute el servicio Load Balancer, con dos excepciones: Los puertos 80 y 443 están reservados en nodos de administrador, de modo que los extremos configurados en estos puertos admiten operaciones de balanceo de carga solo en nodos de puerta de enlace.

Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de Eliminar reasignaciones de puertos.

El servicio CLB está obsoleto.

#### Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente cuando se reenvía tráfico de S3 o Swift a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio Load Balancer envía más solicitudes a los nodos de almacenamiento con una mayor disponibilidad de CPU. La información de carga de CPU del nodo se actualiza cada pocos minutos, pero es posible que la ponderación se actualice con mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa de un uso del 100 % o no informa de su uso.

En algunos casos, la información acerca de la disponibilidad de CPU se limita al sitio donde se encuentra el servicio Load Balancer.

### Configurar puntos finales del equilibrador de carga

Los extremos de equilibrador de carga determinan los puertos y los protocolos de red que los clientes S3 y Swift pueden utilizar al conectarse al equilibrador de carga StorageGRID en los nodos de puerta de enlace y administración.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Si anteriormente ha reasignado un puerto que tiene intención de utilizar para el extremo de equilibrio de carga, tiene se ha eliminado el mapa de puertos.
- Ha creado cualquier grupo de alta disponibilidad que desee utilizar. Se recomiendan los grupos de ALTA DISPONIBILIDAD, pero no es obligatorio. Consulte Gestión de grupos de alta disponibilidad.
- Si el punto final del equilibrador de carga será utilizado por Inquilinos de S3 para S3 Select, No debe utilizar las direcciones IP ni las FQDN de ningún nodo de configuración básica. Sólo se permiten los dispositivos SG100 o SG1000 y los nodos de software basados en VMware para los extremos de equilibrador de carga utilizados para S3 Select.
- Ha configurado las interfaces VLAN que desea utilizar. Consulte Configure las interfaces VLAN.
- Si crea un extremo de HTTPS (recomendado), tiene la información del certificado de servidor.

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

  - Para cargar un certificado, necesita el certificado de servidor, la clave privada de certificado y, opcionalmente, un bundle de CA.
  - Para generar un certificado, se necesitan todos los nombres de dominio y las direcciones IP que utilizarán los clientes S3 o Swift para acceder al extremo. También debe conocer el asunto (nombre distintivo).
  - Si desea usar el certificado API de StorageGRID S3 y Swift (que también se puede usar para conexiones directamente a nodos de almacenamiento), ya sustituyó el certificado predeterminado por un certificado personalizado firmado por una autoridad de certificado externa. ConsulteConfigure los certificados API S3 y Swift.

    El certificado puede utilizar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y los nodos de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo: `*.storagegrid.example.com` utiliza el comodín * que se va a representar `adm1.storagegrid.example.com` y.. `gn1.storagegrid.example.com`. Consulte Configure los nombres de dominio de extremo API de S3.

#### Cree un extremo de equilibrador de carga

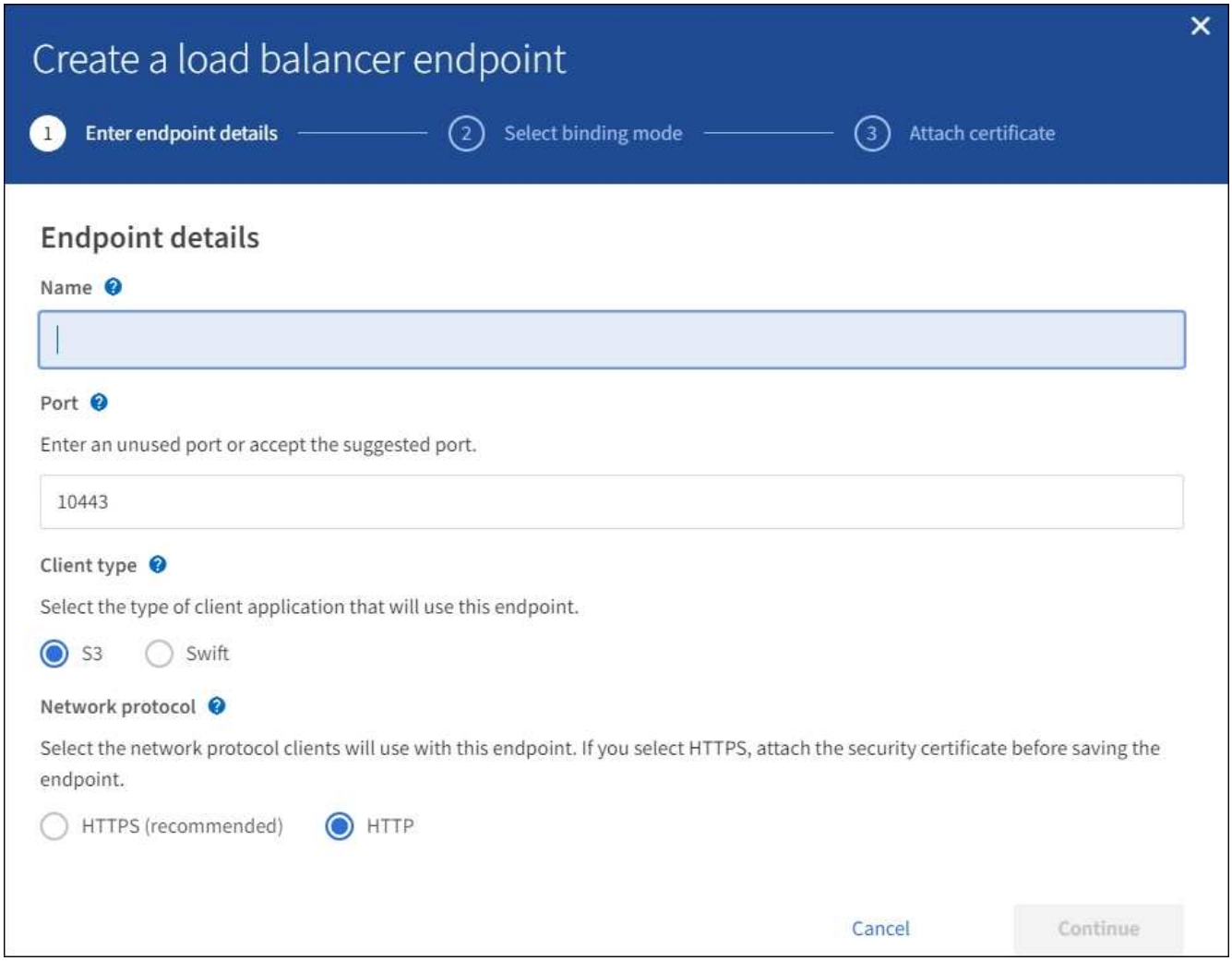
Cada extremo de equilibrio de carga especifica un puerto, un tipo de cliente (S3 o Swift) y un protocolo de red (HTTP o HTTPS).

#### Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Seleccione **Crear**.

### Introduzca los detalles de los extremos

1. Introduzca los detalles del extremo.




| Campo | Descripción |
|---|---|
| Nombre | Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints. |
| Puerto | Los clientes de puertos utilizarán para conectarse al servicio Load Balancer en los nodos de administración y de puerta de enlace.<br><br>Acepte el número de puerto sugerido o introduzca cualquier puerto externo que no utilice otro servicio de cuadrícula. Introduzca un valor entre 1 y 65535.<br><br>Si introduce **80** o **443**, el punto final sólo se configura en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administrador.<br><br>Consulte Directrices sobre redes para obtener información acerca de los puertos externos. |
| Tipo de cliente | Tipo de aplicación cliente que utilizará este extremo, ya sea **S3** o **Swift**. |

| Campo | Descripción |
| --- | --- |
| Protocolo de red | El protocolo de red que utilizarán los clientes al conectarse a este extremo.<br>• Seleccione **HTTPS** para una comunicación segura cifrada con TLS (recomendado). Debe asociar un certificado de seguridad para poder guardar el extremo.<br>• Seleccione **HTTP** para una comunicación no cifrada y menos segura. Utilice HTTP sólo para una cuadrícula que no sea de producción. |

2. Seleccione **continuar**.

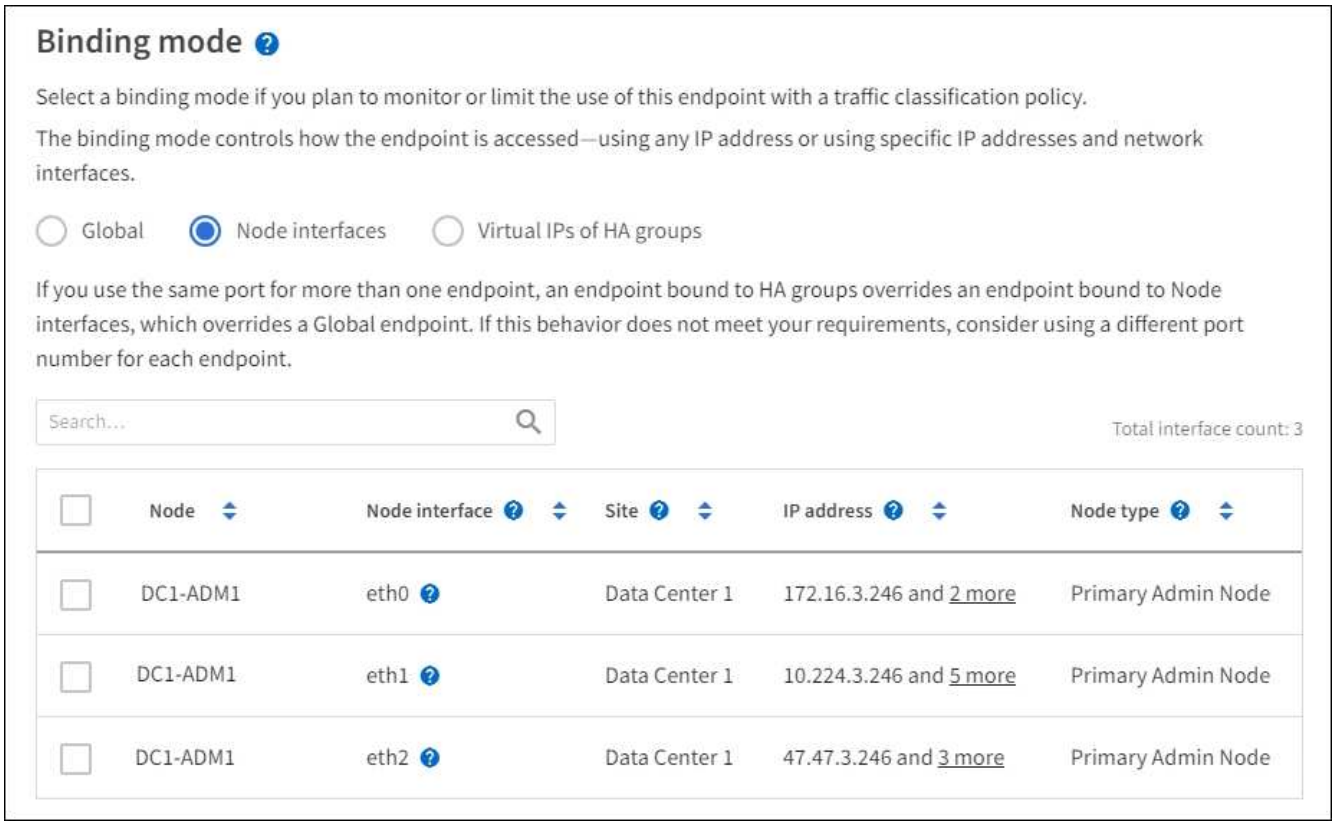
### Seleccione el modo de encuadernación

1. Seleccione un modo de enlace para que el extremo controle cómo se accede al extremo.

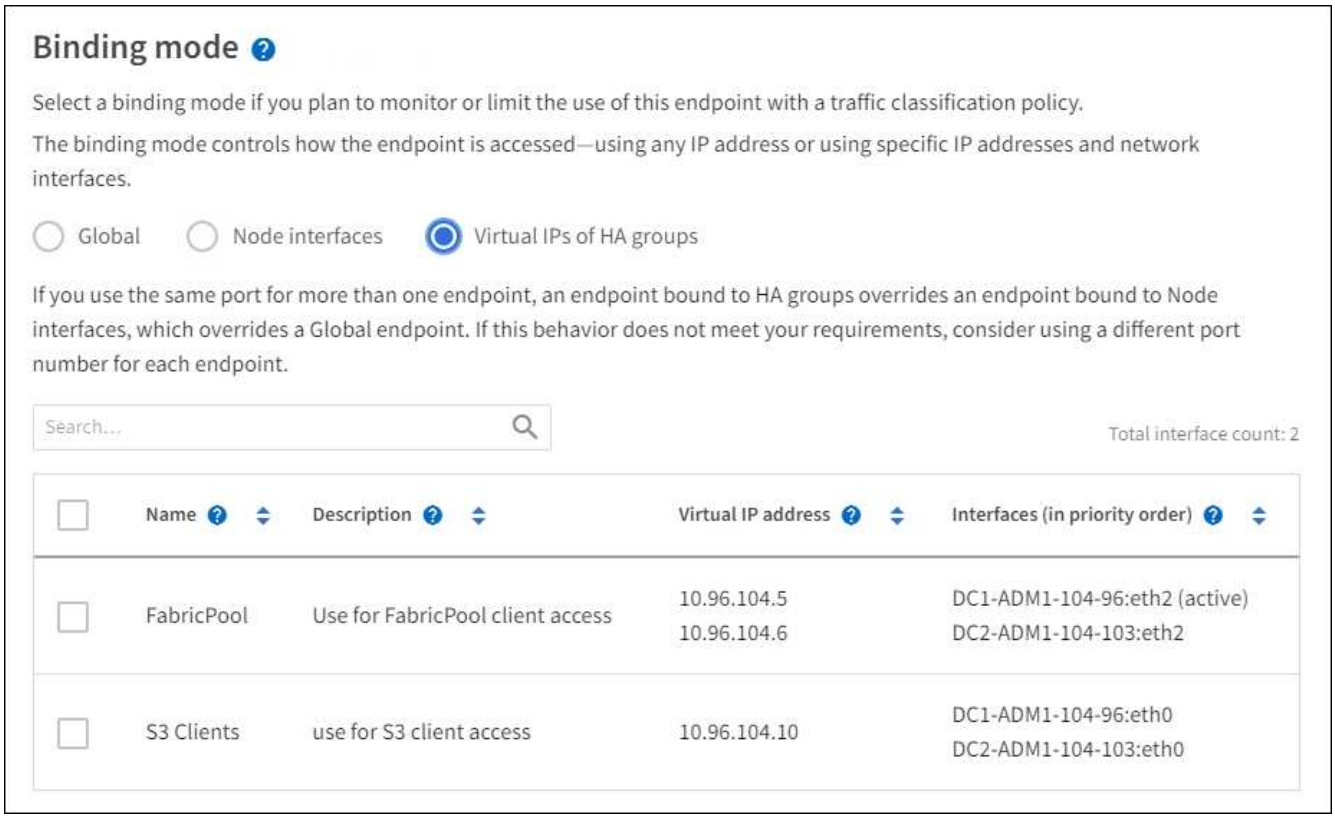
| Opción | Descripción |
| --- | --- |
| Global (predeterminado) | Los clientes pueden acceder al extremo utilizando un nombre de dominio completo (FQDN), la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, o la dirección IP virtual de cualquier grupo de alta disponibilidad de cualquier red.<br>Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo. |
| Interfaces de nodos | Los clientes deben usar la dirección IP de un nodo e interfaz de red seleccionados para acceder a este extremo. |
| IP virtuales de grupos de alta disponibilidad | Los clientes deben utilizar una dirección IP virtual de un grupo de alta disponibilidad para acceder a este extremo.<br>Los extremos con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de alta disponibilidad que seleccione para los extremos no se superpongan.<br>Los extremos con este modo pueden usar el mismo número de puerto siempre que las interfaces que seleccione para los extremos no se superpongan. |

> Si utiliza el mismo puerto para más de un extremo, un punto final que utiliza el modo **IP virtuales de grupos de alta disponibilidad** anula un punto final utilizando el modo **interfaces de nodo**, que anula un punto final utilizando el modo **Global**.

2. Si ha seleccionado **interfaces de nodo**, seleccione una o más interfaces de nodo para cada nodo de administración o nodo de puerta de enlace que desee asociar con este extremo.




3. Si ha seleccionado **IP virtuales de grupos ha**, seleccione uno o más grupos ha.




4. Si está creando un extremo **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el nuevo punto final del equilibrador de carga. A continuación, vaya a. Después de terminar. De lo contrario, seleccione **continuar** para adjuntar el certificado.

### Adjunte el certificado

1. Si está creando un extremo **HTTPS**, seleccione el tipo de certificado de seguridad que desea asociar al extremo.

   El certificado protege las conexiones entre los clientes S3 y Swift y el servicio Load Balancer en los nodos de Admin Node o de Gateway.

   - **Cargar certificado**. Seleccione esta opción si tiene certificados personalizados para cargar.
   - **Generar certificado**. Seleccione esta opción si tiene los valores necesarios para generar un certificado personalizado.
   - **Utilice los certificados StorageGRID S3 y Swift**. Seleccione esta opción si desea usar el certificado API global S3 y Swift, que también se puede usar para las conexiones directamente con nodos de almacenamiento.

     No puede seleccionar esta opción a menos que haya sustituido el certificado API predeterminado S3 y Swift, que está firmado por la CA de grid, con un certificado personalizado firmado por una entidad de certificación externa. ConsulteConfigure los certificados API S3 y Swift.

2. Si no utiliza el certificado StorageGRID S3 y Swift, cargue o genere el certificado.

**Cargue el certificado**

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor**: El archivo de certificado de servidor personalizado en codificación 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 **Crear**. + se crea el punto final del equilibrador de carga. El certificado personalizado se usa en todas las conexiones nuevas posteriores entre los clientes de S3 y Swift y el extremo.

**Generar certificado**

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

- **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
- **IP**: Una o varias direcciones IP que se incluirán en el certificado.
- **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
- **Días válidos**: Número de días después de la creación que expira el certificado.

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 **Crear**.

Se crea el punto final del equilibrador de carga. El certificado personalizado se usa para todas las conexiones nuevas posteriores entre los clientes de S3 y Swift y este extremo.

**[[después de terminar]]después de terminar**

1. Si utiliza un sistema de nombres de dominio (DNS), asegúrese de que el DNS incluye un registro para asociar el nombre de dominio completo de StorageGRID a cada dirección IP que utilizarán los clientes para realizar conexiones.

   La dirección IP que introduzca en el registro DNS depende de si se utiliza un grupo de alta disponibilidad de nodos con balanceo de carga:

   - Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de dicho grupo de alta disponibilidad.
   - Si no está utilizando un grupo de alta disponibilidad, los clientes se conectarán al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de cualquier nodo de puerta de enlace o nodo de administración.

     También debe asegurarse de que el registro DNS hace referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.

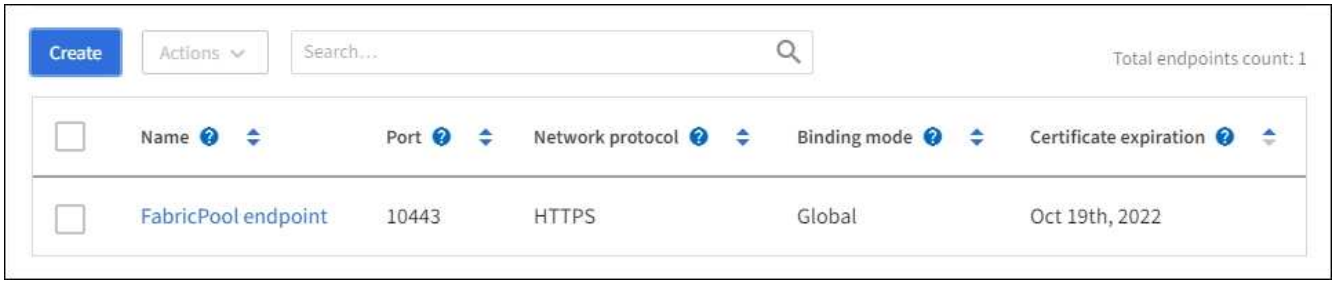
2. Proporcione a los clientes S3 y Swift la información necesaria para conectarse al extremo:
   - Número de puerto
   - Nombre de dominio o dirección IP completos
   - Los detalles de certificado necesarios

#### Ver y editar puntos finales del equilibrador de carga

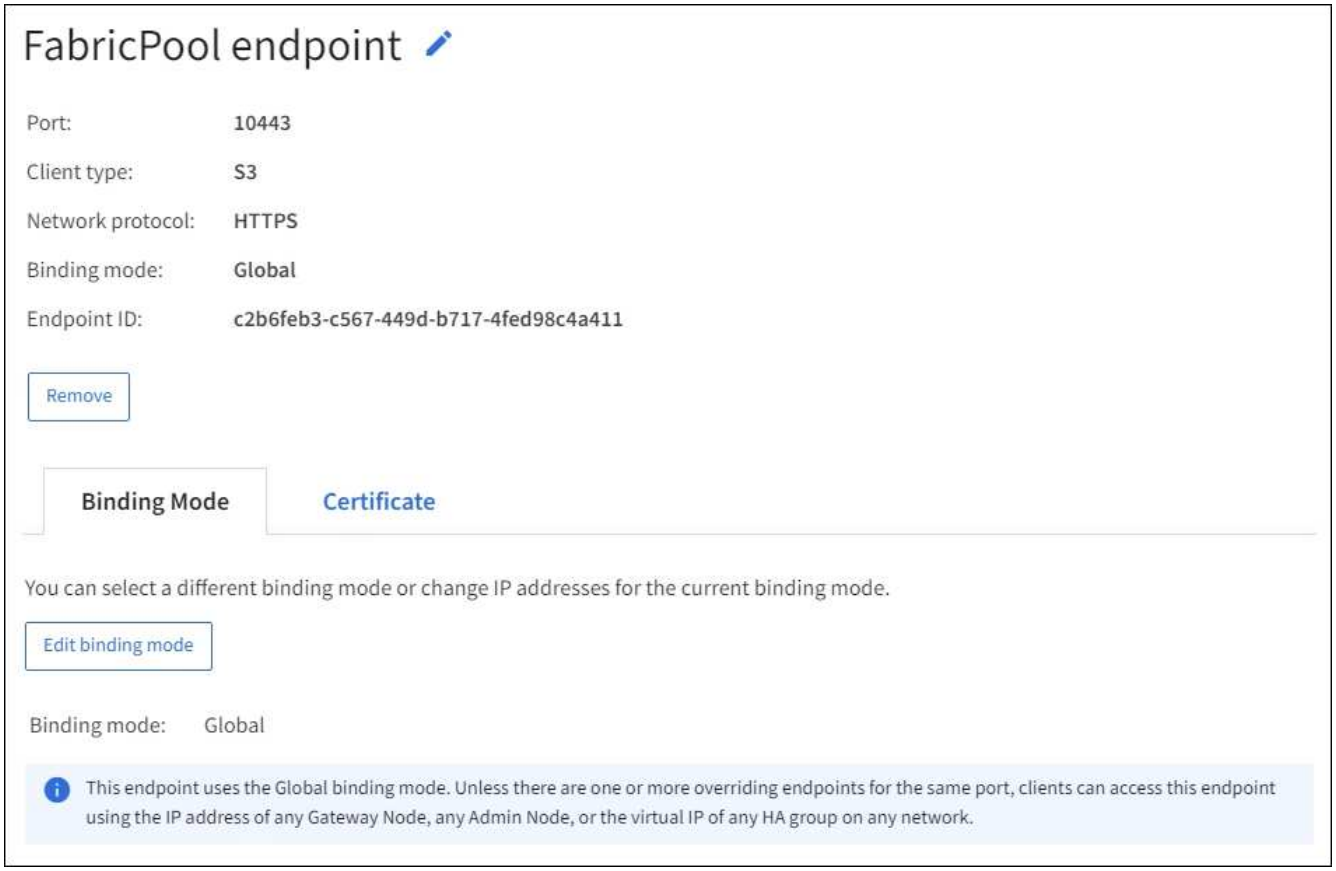
Puede ver detalles de los extremos de equilibrador de carga existentes, incluidos los metadatos de certificado para un extremo protegido. También puede cambiar el nombre de un extremo o el modo de enlace y actualizar los certificados asociados.

No puede cambiar el tipo de servicio (S3 o Swift), el puerto o el protocolo (HTTP o HTTPS).

- Para ver información básica de todos los puntos finales del equilibrador de carga, revise la tabla de la página puntos finales del equilibrador de carga.



- Para ver todos los detalles acerca de un extremo específico, incluidos los metadatos del certificado, seleccione el nombre del extremo en la tabla.




- Para editar un punto final, utilice el menú **acciones** de la página puntos finales del equilibrador de carga o la página de detalles de un punto final específico.

> Después de editar un extremo, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

| Tarea | Menú Actions | Detalles |
|---|---|---|
| Editar el nombre del extremo | a. Seleccione la casilla de verificación del extremo.<br>b. Seleccione **acciones** > **Editar nombre de punto final**.<br>c. Introduzca el nuevo nombre.<br>d. Seleccione **Guardar**. | a. Seleccione el nombre del extremo para mostrar los detalles.<br>b. Seleccione el icono de edición .<br>c. Introduzca el nuevo nombre.<br>d. Seleccione **Guardar**. |

| Tarea | Menú Actions | Detalles |
| --- | --- | --- |
| Edite el modo de enlace de punto final | a. Seleccione la casilla de verificación del extremo.<br>b. Seleccione **acciones** > **Editar modo de enlace de punto final**.<br>c. Actualice el modo de enlace según sea necesario.<br>d. Seleccione **Guardar cambios**. | a. Seleccione el nombre del extremo para mostrar los detalles.<br>b. Seleccione **Editar modo de enlace**.<br>c. Actualice el modo de enlace según sea necesario.<br>d. Seleccione **Guardar cambios**. |
| Editar certificado de extremo | a. Seleccione la casilla de verificación del extremo.<br>b. Seleccione **acciones** > **Editar certificado de punto final**.<br>c. Cargue o genere un nuevo certificado personalizado o comience a usar el certificado global S3 y Swift, según sea necesario.<br>d. Seleccione **Guardar cambios**. | a. Seleccione el nombre del extremo para mostrar los detalles.<br>b. Seleccione la ficha **Certificado**.<br>c. Seleccione **Editar certificado**.<br>d. Cargue o genere un nuevo certificado personalizado o comience a usar el certificado global S3 y Swift, según sea necesario.<br>e. Seleccione **Guardar cambios**. |

#### Retire los extremos del equilibrador de carga

Puede eliminar uno o varios puntos finales mediante el menú **acciones** o puede eliminar un único punto final de la página de detalles.

> Para evitar que se produzcan interrupciones en el cliente, actualice las aplicaciones cliente S3 o Swift afectadas antes de eliminar un extremo de equilibrio de carga. Actualice cada cliente para que se conecte utilizando un puerto asignado a otro extremo de equilibrador de carga. Asegúrese de actualizar también la información de certificado necesaria.

- Para eliminar uno o varios puntos finales:
  a. En la página Load Balancing, seleccione la casilla de verificación de cada extremo que desee quitar.
  b. Seleccione **acciones** > **Quitar**.
  c. Seleccione **OK**.
- Para eliminar un extremo de la página de detalles:
  a. Desde la página Load equilibrador. seleccione el nombre del extremo.
  b. Seleccione **Quitar** en la página de detalles.
  c. Seleccione **OK**.

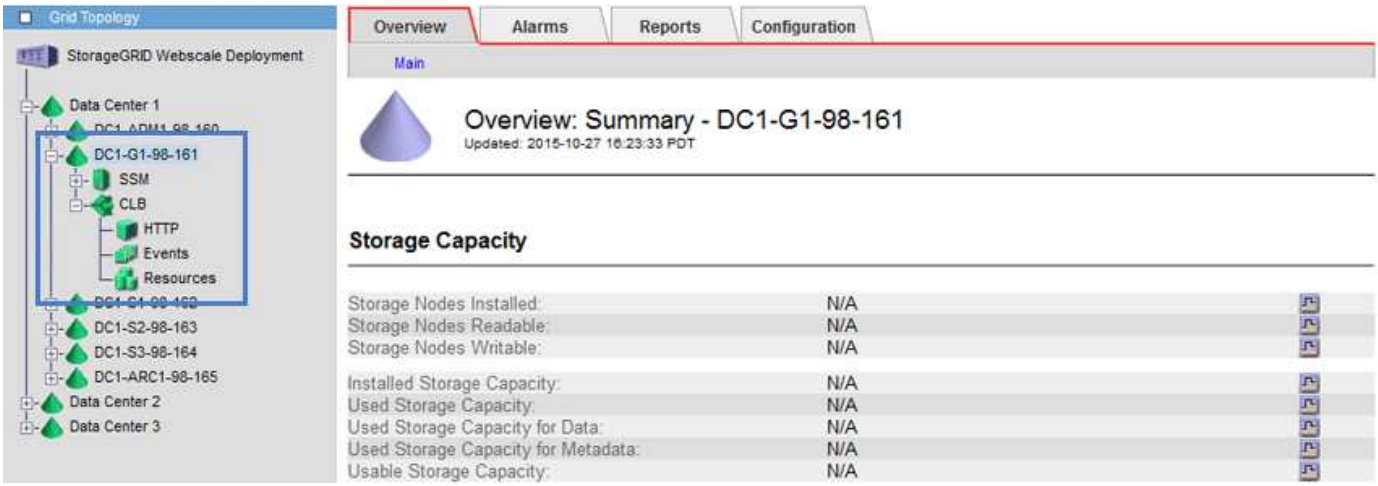
### Cómo funciona el equilibrio de carga: Servicio CLB (obsoleto)

El servicio Connection Load Balancer (CLB) en los nodos de Gateway queda obsoleto. El servicio Load Balancer es ahora el mecanismo de equilibrio de carga recomendado.

El servicio CLB utiliza el equilibrio de carga de capa 4 para distribuir las conexiones de red TCP entrantes de

las aplicaciones cliente al nodo de almacenamiento óptimo en función de la disponibilidad, la carga del sistema y el coste de enlace configurado por el administrador. Cuando se elige el nodo de almacenamiento óptimo, el servicio CLB establece una conexión de red bidireccional y reenvía el tráfico hacia y desde el nodo elegido. El CLB no considera la configuración de red de red de cuadrícula al dirigir las conexiones de red entrantes.

Para ver información sobre el servicio CLB, seleccione **SUPPORT** > **Tools** > **Grid topolog** y, a continuación, expanda un nodo Gateway hasta que pueda seleccionar **CLB** y las opciones que aparecen a continuación.




Si decide utilizar el servicio CLB, debe considerar la configuración de los costes de enlace para su sistema StorageGRID.

- ¿Cuáles son los costes de enlace
- Actualizar costes de enlace

## Configure los nombres de dominio de extremo API de S3

Para admitir solicitudes de estilo alojado virtuales S3, debe usar Grid Manager para configurar la lista de nombres de dominio de extremo a los que se conectan los clientes S3.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha confirmado que no hay una actualización de grid en curso.

> No realice ningún cambio en la configuración del nombre de dominio cuando se esté realizando una actualización de la cuadrícula.

**Acerca de esta tarea**

Para habilitar a los clientes que usen nombres de dominio extremo de S3, debe realizar todas las siguientes acciones:

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el certificado que utiliza el cliente para las conexiones HTTPS a StorageGRID esté firmado para todos los nombres de dominio que el cliente necesita.

Por ejemplo, si el extremo es `s3.company.com`, Debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluye `s3.company.com` Nombre alternativo (SAN) del asunto comodín del extremo y del extremo: `*.s3.company.com`.

- Configure el servidor DNS que utiliza el cliente. Incluya registros DNS para las direcciones IP que utilizan los clientes para realizar conexiones y asegúrese de que los registros hagan referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.

> Los clientes se pueden conectar a StorageGRID mediante la dirección IP de un nodo de puerta de enlace, un nodo de administrador o un nodo de almacenamiento, o bien mediante la conexión a la dirección IP virtual de un grupo de alta disponibilidad. Debe comprender cómo se conectan las aplicaciones cliente a la cuadrícula para que incluya las direcciones IP correctas en los registros DNS.

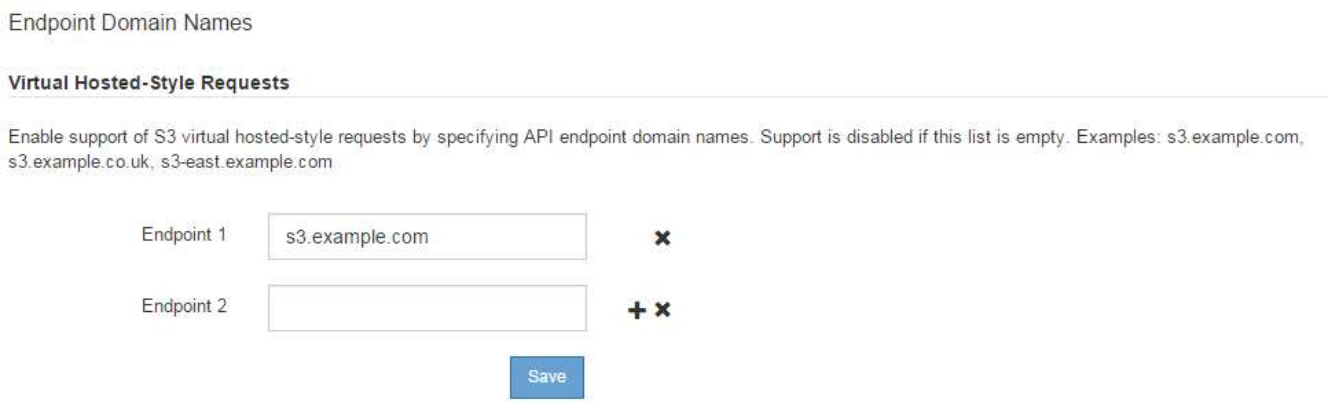
Los clientes que usan conexiones HTTPS (recomendadas) a la cuadrícula pueden usar cualquiera de los siguientes certificados:

- Los clientes que se conectan a un extremo de equilibrador de carga pueden utilizar un certificado personalizado para ese extremo. Cada punto final de equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de punto final.
- Los clientes que se conectan a un extremo de equilibrio de carga, directamente a un nodo de almacenamiento o directamente al servicio CLB obsoleto en un nodo de puerta de enlace pueden personalizar el certificado de API S3 y Swift global para incluir todos los nombres de dominio de extremo necesarios.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **nombres de dominio**.

   Aparece la página Endpoint Domain Names.




2. Introduzca la lista de nombres de dominio de extremo de API de S3 en los campos **Endpoint**. Utilice la ➕ con el icono para añadir campos adicionales.

   Si esta lista está vacía, se deshabilita la compatibilidad con las solicitudes de estilo alojado virtuales de S3.

3. Seleccione **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de extremo requeridos.
   - Si los clientes se conectan a un extremo de equilibrador de carga que utiliza su propio certificado,

actualice el certificado asociado al extremo.

- Si los clientes se conectan a un extremo de equilibrio de carga que usa el certificado de API global S3 y Swift, directamente en los nodos de almacenamiento o al servicio CLB en los nodos de puerta de enlace, actualice el certificado de la API global S3 y Swift.

5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombres de dominio de extremo.

**Resultado**

Ahora, cuando los clientes utilizan el extremo `bucket.s3.company.com`, El servidor DNS resuelve el punto final correcto y el certificado autentica el punto final como se esperaba.

**Información relacionada**

- Use S3
- Ver direcciones IP
- Configuración de grupos de alta disponibilidad
- Configure los certificados API S3 y Swift
- Configurar puntos finales del equilibrador de carga

## Habilite HTTP para las comunicaciones del cliente

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para todas las conexiones a nodos de almacenamiento o al servicio CLB obsoleto en nodos de puerta de enlace. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea de producción.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

Complete esta tarea solo si los clientes S3 y Swift necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento o al servicio CLB obsoleto en los nodos de puerta de enlace.

No es necesario completar esta tarea para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio Load Balancer (ya que puede configurar cada extremo de Load Balancer para usar HTTP o HTTPS). Consulte la información sobre la configuración de puntos finales del equilibrador de carga para obtener más información.

Consulte Resumen: Direcciones IP y puertos para conexiones cliente Para conocer los puertos que utilizan los clientes S3 y Swift al conectarse a los nodos de almacenamiento o al servicio CLB obsoleto a través de HTTP o HTTPS

> Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red , active la casilla de verificación **Activar conexión HTTP** .

3. Seleccione **Guardar**.

**Información relacionada**

- Configurar puntos finales del equilibrador de carga
- Use S3
- Use Swift

## Controlar qué operaciones de cliente están permitidas

Puede seleccionar la opción de cuadrícula evitar modificación de cliente para denegar operaciones específicas de cliente HTTP.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

Evitar modificación de cliente es un valor para todo el sistema. Cuando se selecciona la opción impedir modificación de cliente, se deniegan las siguientes solicitudes:

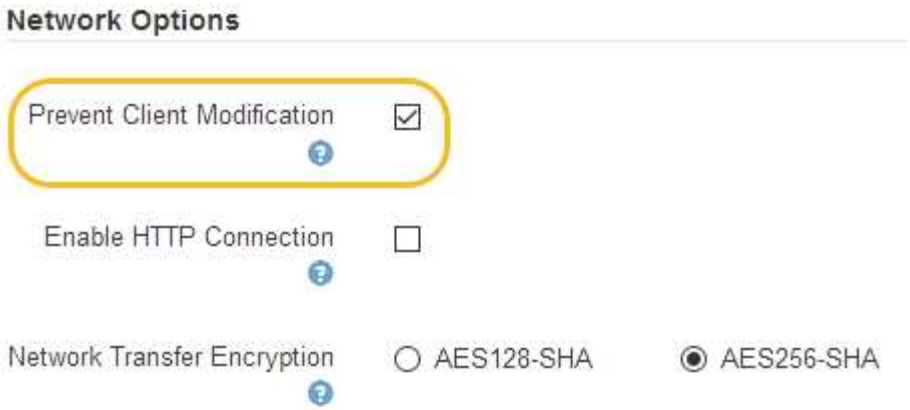
- **API REST S3**
  - Eliminar solicitudes de bloques
  - Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

> Este ajuste no se aplica a bloques con versiones habilitadas. El control de versiones ya evita modificaciones en los datos de objetos, los metadatos definidos por el usuario y el etiquetado de objetos.

- **API REST de Swift**
  - Eliminar solicitudes de contenedor
  - Solicitudes para modificar cualquier objeto existente. Por ejemplo, se deniegan las siguientes operaciones: Put Overwrite, Delete, Metadata Update, etc.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red, active la casilla de verificación **evitar modificación de cliente**.




3. Seleccione **Guardar**.

# Administrar redes y conexiones

## Directrices para redes StorageGRID

Puede utilizar Grid Manager para configurar y administrar redes y conexiones StorageGRID.

Consulte Configure las conexiones de clientes S3 y Swift Para aprender a conectar clientes S3 o Swift.

### Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Para obtener más información acerca de la topología de red, consulte Directrices sobre redes.

#### Red Grid

Obligatorio. La red de red se utiliza para todo el tráfico interno de StorageGRID. Proporciona conectividad entre todos los nodos de la cuadrícula, en todos los sitios y subredes.

#### Red de administración

Opcional. La red de administración suele utilizarse para la administración y el mantenimiento del sistema. También se puede utilizar para el acceso a protocolos de cliente. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios.

#### Red cliente

Opcional. La red cliente es una red abierta que se suele utilizar para proporcionar acceso a aplicaciones cliente S3 y Swift, de modo que la red Grid se pueda aislar y proteger. La red de cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

### Directrices

- Cada nodo de grid StorageGRID requiere una interfaz de red dedicada, una dirección IP, una máscara de subred y una puerta de enlace para cada red a la que está asignado.
- Un nodo de grid no puede tener más de una interfaz en una red.
- Se admite una sola puerta de enlace, por red y cada nodo de grid, y debe estar en la misma subred que el nodo. Si es necesario, puede implementar un enrutamiento más complejo en la puerta de enlace.
- En cada nodo, cada red asigna una interfaz de red específica.

| Red | Nombre de la interfaz |
|---|---|
| Cuadrícula | eth0 |
| Admin (opcional) | eth1 |
| Cliente (opcional) | eth2 |

- Si el nodo está conectado a un dispositivo StorageGRID, se utilizan puertos específicos para cada red. Para obtener más información, consulte las instrucciones de instalación del dispositivo.
- La ruta predeterminada se genera automáticamente, por nodo. Si eth2 está habilitado, 0.0.0.0/0 utiliza la red cliente en eth2. Si eth2 no está habilitado, 0.0.0.0/0 utiliza la red de cuadrícula en eth0.
- La red cliente no se pone en funcionamiento hasta que el nodo de grid se ha Unido a la cuadrícula
- La red de administrador se puede configurar durante la puesta en marcha del nodo de grid para permitir el acceso a la interfaz de usuario de la instalación antes de que la cuadrícula esté totalmente instalada.

### Interfaces opcionales

Opcionalmente, se pueden añadir interfaces adicionales a un nodo. Por ejemplo, puede agregar una interfaz troncal a un nodo de administración o de puerta de enlace, para poder utilizar Interfaces VLAN para segregar el tráfico que pertenece a diferentes aplicaciones o arrendatarios. O bien, puede que desee añadir una interfaz de acceso para utilizarla en un Grupo de alta disponibilidad.

Para añadir enlaces troncales o interfaces de acceso, consulte lo siguiente:

- **VMware (después de instalar el nodo)**: VMware: Añada tronco o interfaces de acceso a un nodo
- **RHEL o CentOS (antes de instalar el nodo)**: Crear archivos de configuración del nodo
- **Ubuntu o Debian (antes de instalar el nodo)**: Crear archivos de configuración del nodo
- **RHEL, CentOS, Ubuntu o Debian (después de instalar el nodo)**: Linux: Añada tronco o interfaces de acceso a un nodo

## Ver direcciones IP

Puede ver la dirección IP de cada nodo de grid en el sistema StorageGRID. A continuación, puede usar esta dirección IP para iniciar sesión en el nodo de grid en la línea de comandos y realizar varios procedimientos de mantenimiento.

### Lo que necesitará

Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

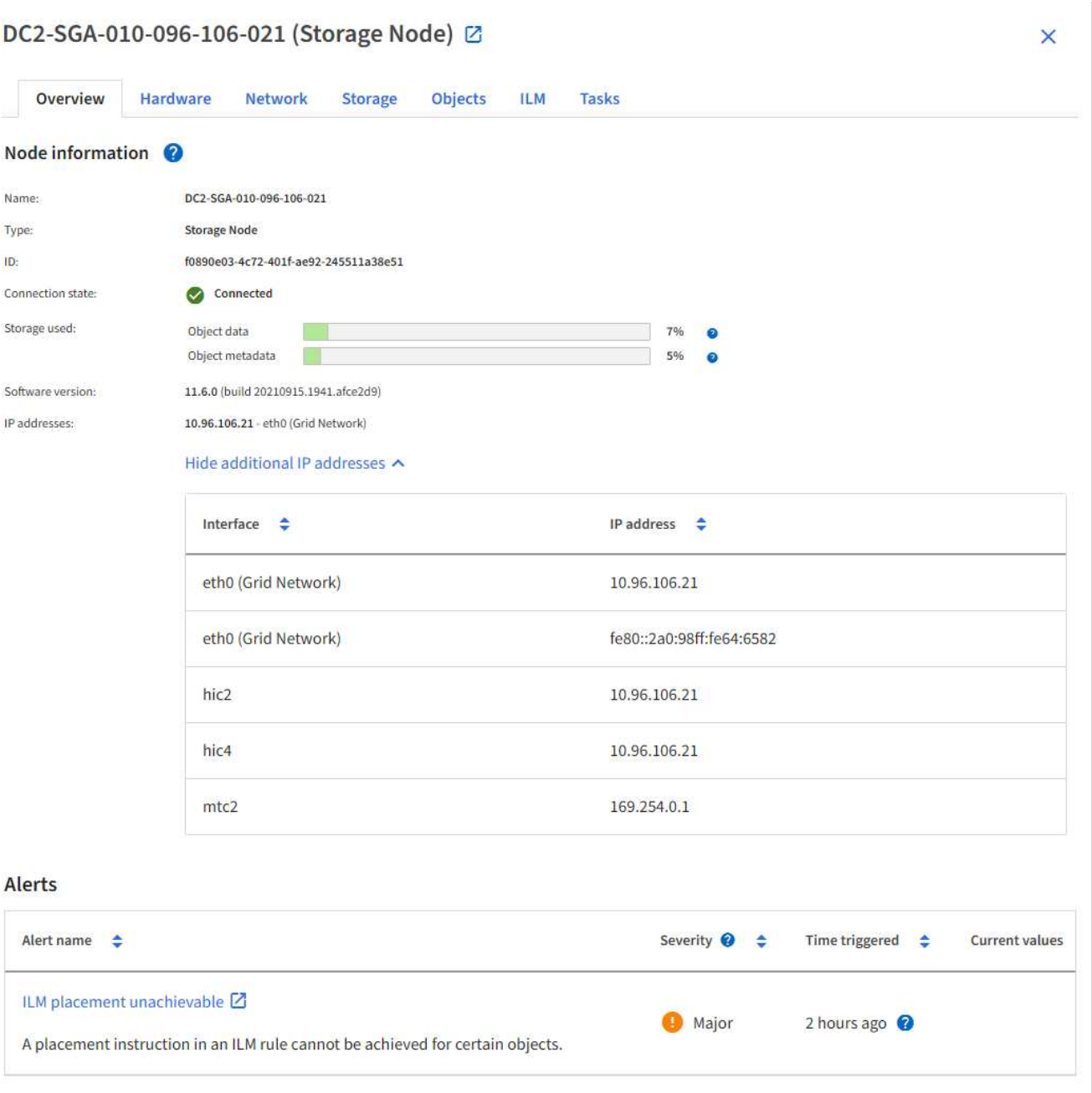
**Acerca de esta tarea**

Para obtener información acerca del cambio de direcciones IP, consulte Recuperación y mantenimiento.

**Pasos**

1. Seleccione **NODES** > ***grid node*** > **Descripción general**.
2. Seleccione **Mostrar más** a la derecha del título direcciones IP.

   Las direcciones IP de ese nodo de grid se enumeran en una tabla.




## Cifrados compatibles para conexiones TLS salientes

El sistema StorageGRID es compatible con un conjunto limitado de conjuntos de cifrado para conexiones TLS (seguridad de la capa de transporte) con los sistemas externos

utilizados para la federación de identidades y los pools de almacenamiento en cloud.

#### Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3 para conexiones a sistemas externos que se utilizan para la federación de identidades y los pools de almacenamiento en cloud.

Se han seleccionado los cifrados TLS compatibles con sistemas externos para garantizar la compatibilidad con una gama de sistemas externos. La lista supera la lista de cifrados que se admiten con aplicaciones cliente S3 o Swift.

> Las opciones de configuración de TLS, como las versiones del protocolo, los cifrados, los algoritmos de intercambio de claves y los algoritmos MAC no se pueden configurar en StorageGRID. Si tiene solicitudes específicas sobre esta configuración, póngase en contacto con su representante de cuenta de NetApp.

#### Paquetes de cifrado TLS 1.2 admitidos

Se admiten los siguientes conjuntos de cifrado TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

#### Paquetes de cifrado TLS 1.3 admitidos

Se admiten los siguientes conjuntos de cifrado TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

## Cambie el cifrado de transferencia de red

El sistema StorageGRID utiliza Seguridad de la capa de transporte (TLS) para proteger el tráfico de control interno entre los nodos de la cuadrícula. La opción Network Transfer Encryption (cifrado de transferencia de red) establece el algoritmo utilizado por TLS para cifrar el tráfico de control entre los nodos de la cuadrícula. Esta configuración no afecta al cifrado de datos.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

De forma predeterminada, el cifrado de transferencia de red utiliza el algoritmo AES256-SHA. El tráfico de control también se puede cifrar utilizando el algoritmo AES128-SHA.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red, cambie el cifrado de transferencia de red a **AES128-SHA** o **AES256-SHA** (predeterminado).

3. Seleccione **Guardar**.

## Administrar directivas de clasificación de tráfico

### Administrar directivas de clasificación de tráfico

Para mejorar sus ofertas de calidad de servicio (QoS), puede crear normativas de clasificación del tráfico para identificar y supervisar distintos tipos de tráfico de red. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Las políticas de clasificación del tráfico se aplican a los extremos en el servicio StorageGRID Load Balancer para los nodos de puerta de enlace y los nodos de administración. Para crear directivas de clasificación de tráfico, debe haber creado ya puntos finales de equilibrador de carga.

#### Reglas de coincidencia

Cada directiva de clasificación de tráfico contiene una o más reglas coincidentes para identificar el tráfico de red relacionado con una o varias de las siguientes entidades:

- Cucharones
- Clientes
- Subredes (subredes IPv4 que contienen al cliente)
- Puntos finales (puntos finales del equilibrador de carga)

StorageGRID supervisa el tráfico que coincide con cualquier regla dentro de la política de acuerdo con los objetivos de la regla. Cualquier tráfico que coincida con cualquier regla de una directiva se gestiona mediante dicha directiva. A la inversa, puede establecer reglas que coincidan con todo el tráfico excepto una entidad especificada.

#### Limitación del tráfico

Opcionalmente, puede establecer límites para una directiva en función de los siguientes parámetros:

- Ancho de banda del agregado en
- Ancho de banda del agregado agotado
- Solicitudes de lectura simultáneas
- Solicitudes de escritura simultáneas
- Ancho de banda por solicitud en
- Ancho de banda por solicitud agotado
- Tasa de solicitud de lectura
- Tasa de solicitudes de escritura

Los valores límite se aplican por cada equilibrador de carga. Si el tráfico se distribuye de forma simultánea entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de velocidad que especifique.

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado.

Para límites de ancho de banda agregados o por solicitud, las solicitudes se transmiten de entrada o salida a la velocidad establecida. StorageGRID sólo puede aplicar una velocidad, por lo que la política más específica, por tipo de matrcher, es la aplicada. Para todos los demás tipos de límites, las solicitudes de clientes se retrasan 250 milisegundos y reciben una respuesta de reducción lenta de 503 para las solicitudes que exceden cualquier límite de directiva coincidente.

En Grid Manager, puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

#### Utilice las políticas de clasificación del tráfico con los SLA

Puede utilizar políticas de clasificación del tráfico junto con los límites de capacidad y protección de datos para aplicar acuerdos de nivel de servicio (SLA) que ofrezcan detalles sobre la capacidad, la protección de datos y el rendimiento.

Los límites de clasificación del tráfico se implementan por equilibrador de carga. Si el tráfico se distribuye de forma simultánea entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de velocidad que especifique.

El siguiente ejemplo muestra tres niveles de un acuerdo de nivel de servicio. Puede crear políticas de clasificación del tráfico para alcanzar los objetivos de rendimiento de cada nivel de SLA.

| Nivel de servicio | Capacidad | Protección de datos | Rendimiento | Coste |
|---|---|---|---|---|
| Oro | 1 PB de almacenamiento permitido | Regla de 3 copia de ILM | 25 000 solicitudes/s<br><br>Ancho de banda de 5 GB/s (40 Gbps) | por mes |

| Nivel de servicio | Capacidad | Protección de datos | Rendimiento | Coste |
|---|---|---|---|---|
| Plata | Capacidad de almacenamiento de 250 TB | 2 regla de copia de ILM | 10 000 solicitudes/s<br><br>Ancho de banda de 1.25 GB/s (10 Gbps) | $$ al mes |
| Bronce | Capacidad de almacenamiento de 100 TB | 2 regla de copia de ILM | 5 000 solicitudes/s<br><br>Ancho de banda de 1 GB/s (8 Gbps) | $ al mes |

### Cree directivas de clasificación de tráfico

Cree políticas de clasificación de tráfico si desea supervisar y, opcionalmente, limitar el tráfico de red por bloque, inquilino, subred IP o extremo de equilibrador de carga. De manera opcional, puede establecer límites para una política en función del ancho de banda, el número de solicitudes simultáneas o la tasa de solicitudes.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Ha creado cualquier punto final de equilibrador de carga que desee que coincida.
- Ha creado los inquilinos que desea que coincidan.

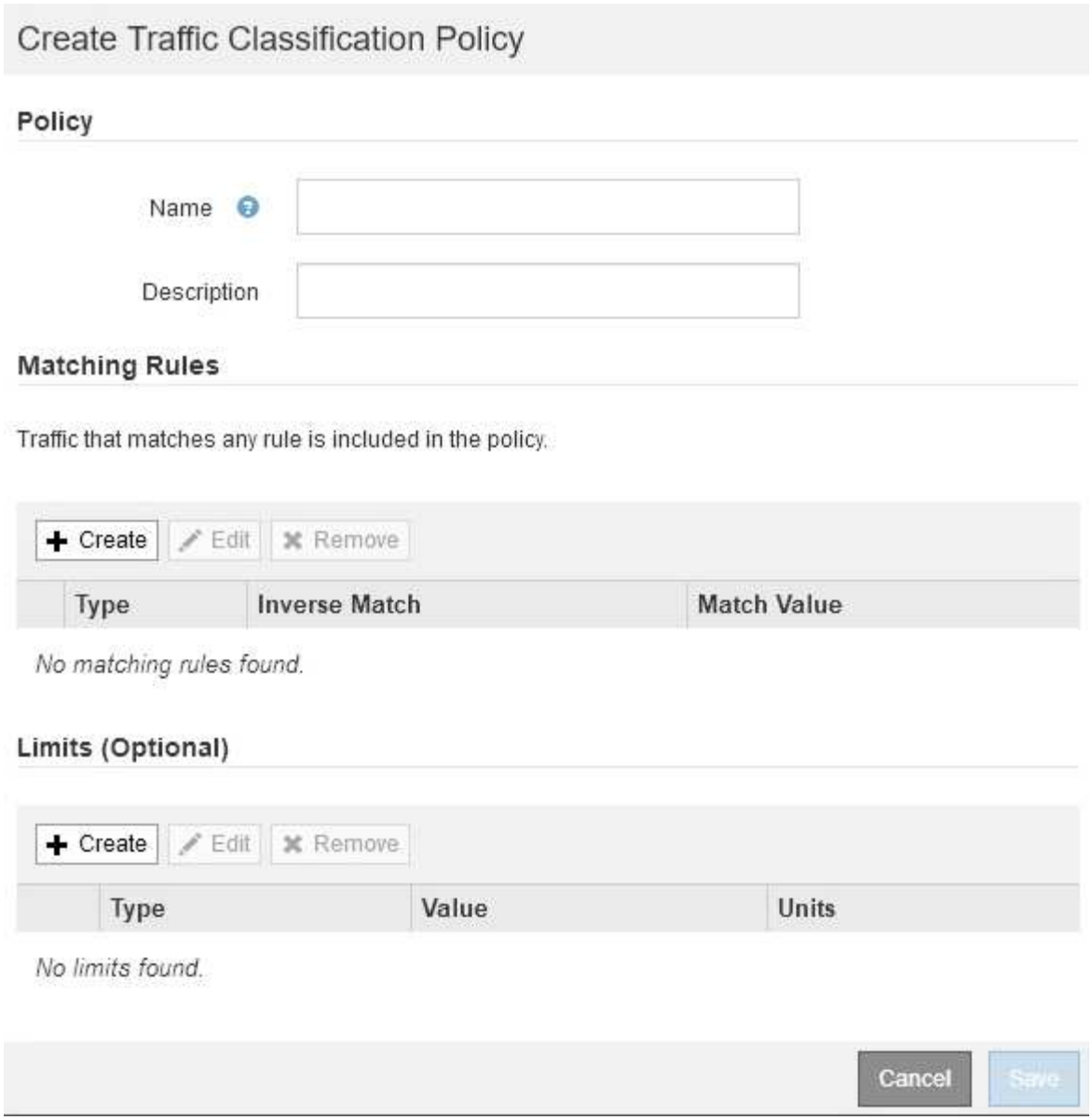
#### Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico.

2. Seleccione **Crear**.

   Aparece el cuadro de diálogo Crear directiva de clasificación de tráfico.




3. En el campo **Nombre**, escriba un nombre para la directiva.

   Introduzca un nombre descriptivo para poder reconocer la política.

4. Opcionalmente, agregue una descripción para la directiva en el campo **Descripción**.

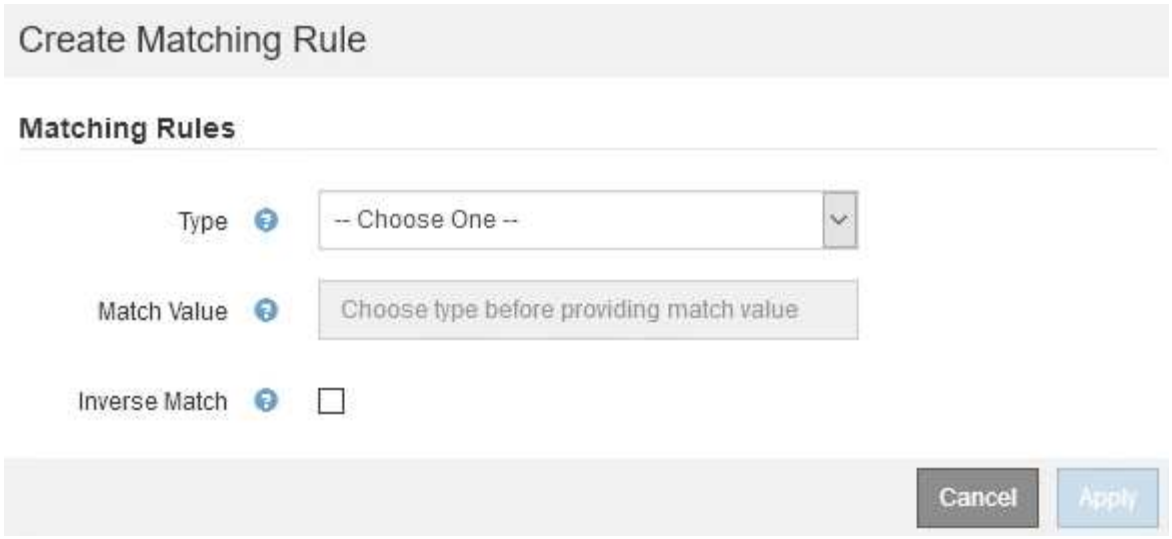
   Por ejemplo, describa a qué se aplica esta política de clasificación del tráfico y a qué se limitará.

5. Cree una o varias reglas coincidentes para la política.

   Las reglas coincidentes controlan qué entidades se verán afectadas por esta directiva de clasificación de tráfico. Por ejemplo, seleccione arrendatario si desea que esta directiva se aplique al tráfico de red de un arrendatario específico. O seleccione Endpoint si desea que esta directiva se aplique al tráfico de red en un extremo de equilibrio de carga específico.

   a. Seleccione **Crear** en la sección **Reglas coincidentes**.

      Aparece el cuadro de diálogo Crear regla de coincidencia.




b. En la lista desplegable **Tipo**, seleccione el tipo de entidad que se incluirá en la regla de coincidencia.

c. En el campo **valor de coincidencia**, escriba un valor de coincidencia basado en el tipo de entidad elegido.

   - Bucket: Introduzca un nombre de bloque.
   - Bucket Regex: Introduzca una expresión regular que se utilizará para coincidir con un conjunto de nombres de bloques.

     La expresión regular no está anclada. Utilice el delimitador ^ para que coincida al principio del nombre del bloque y utilice el delimitador $ para que coincida al final del nombre.

   - CIDR: Introduzca una subred IPv4, en notación CIDR, que coincida con la subred deseada.
   - Extremo: Seleccione un extremo de la lista de extremos existentes. Estos son los puntos finales de equilibrador de carga definidos en la página de extremos de equilibrador de carga. Consulte Configurar puntos finales del equilibrador de carga.
   - Inquilino: Seleccione un inquilino de la lista de arrendatarios existentes. La coincidencia de inquilinos se basa en la propiedad del bloque al que se va a acceder. El acceso anónimo a un bloque coincide con el inquilino al que pertenece el bloque.

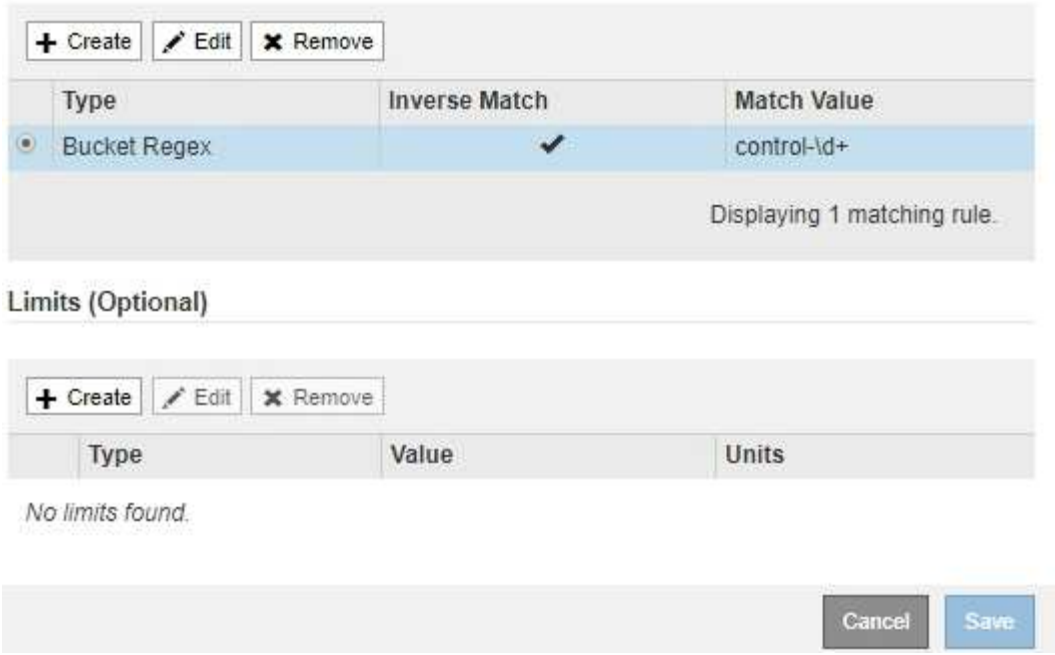
d. Si desea hacer coincidir todo el tráfico de red *excepto* que sea coherente con el valor Type and Match que acaba de definir, active la casilla de verificación **Inverse** . De lo contrario, deje la casilla de verificación sin seleccionar.

   Por ejemplo, si desea que esta directiva se aplique a todos los puntos finales del equilibrador de carga excepto uno, especifique el punto final del equilibrador de carga que se excluirá y seleccione **Inverse**.

   > Para una directiva que contiene varios matchers donde al menos uno es un matcher inverso, tenga cuidado de no crear una política que coincida con todas las solicitudes.

e. Seleccione **aplicar**.

   La regla se crea y se muestra en la tabla Reglas coincidentes.




a. Repita estos pasos para cada regla que desee crear para la política.

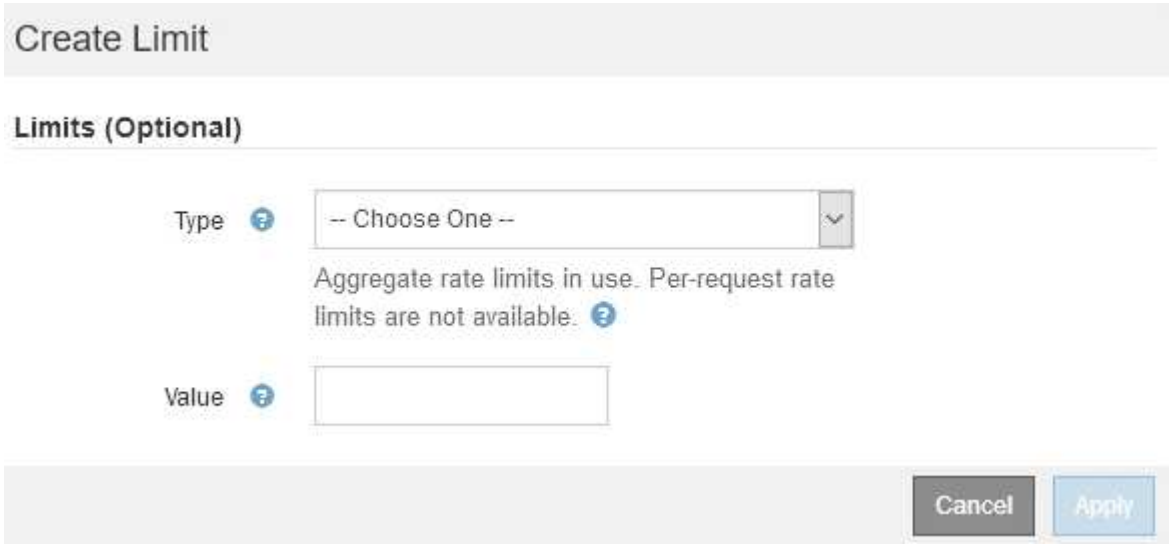
> El tráfico que coincide con cualquier regla se gestiona mediante la directiva.

6. De manera opcional, crear límites para la política.

> Aunque no cree límites, StorageGRID recopila métricas para poder supervisar el tráfico de red que se ajuste a la directiva.

a. Seleccione **Crear** en la sección **límites**.

Se muestra el cuadro de diálogo Crear límite.




b. En el menú desplegable **Tipo**, seleccione el tipo de límite que desea aplicar a la directiva.

En la siguiente lista, **in** hace referencia al tráfico de clientes S3 o Swift en el equilibrador de carga StorageGRID, y **OUT** hace referencia al tráfico desde el equilibrador de carga a clientes S3 o Swift.

- Ancho de banda del agregado en
- Ancho de banda del agregado agotado
- Solicitudes de lectura simultáneas
- Solicitudes de escritura simultáneas
- Ancho de banda por solicitud en
- Ancho de banda por solicitud agotado
- Tasa de solicitud de lectura
- Tasa de solicitudes de escritura

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado.

Para los límites de ancho de banda, StorageGRID aplica la política que mejor se adapte al tipo de conjunto de límites. Por ejemplo, si tiene una directiva que limita el tráfico en una sola dirección, entonces el tráfico en la dirección opuesta será ilimitado, aunque haya tráfico que coincida con las directivas adicionales que tengan límites de ancho de banda. StorageGRID implementa coincidencias «mejores» para límites de ancho de banda en el siguiente orden:

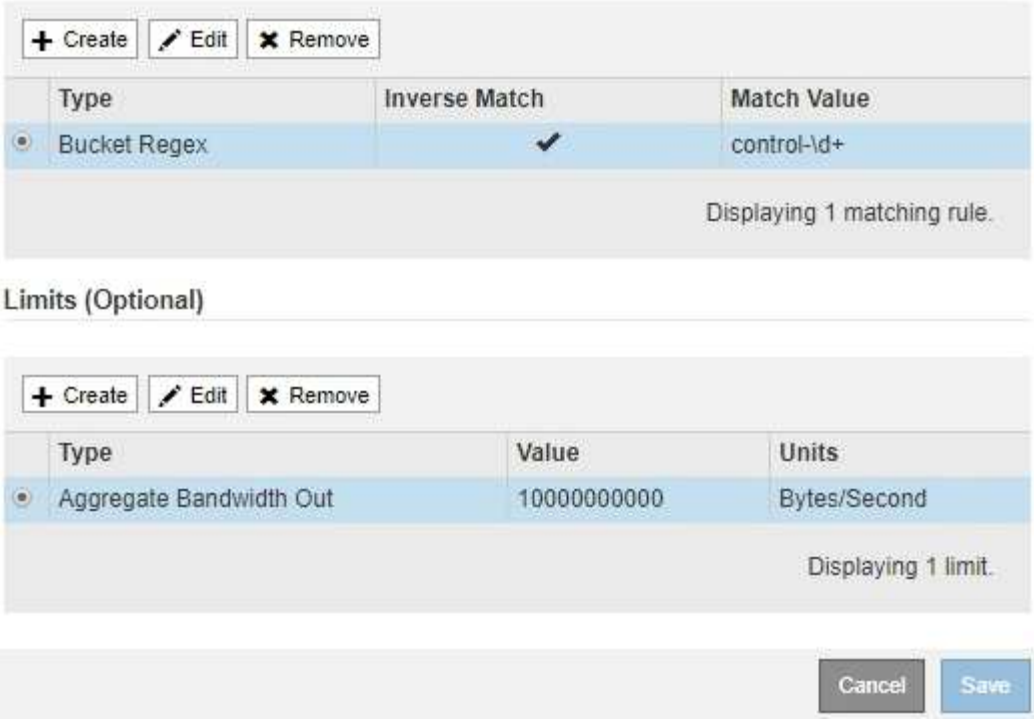
- Dirección IP exacta (/máscara 32)
- Nombre exacto del cucharón
- Regex. Cucharón
- Inquilino
- Extremo
- Coincidencias CIDR no exactas (no /32)
- Coincidencias inversas

c. En el campo **valor**, introduzca un valor numérico para el tipo de límite elegido.

   Las unidades esperadas se muestran cuando se selecciona un límite.

d. Seleccione **aplicar**.

   El límite se crea y se muestra en la tabla límites.



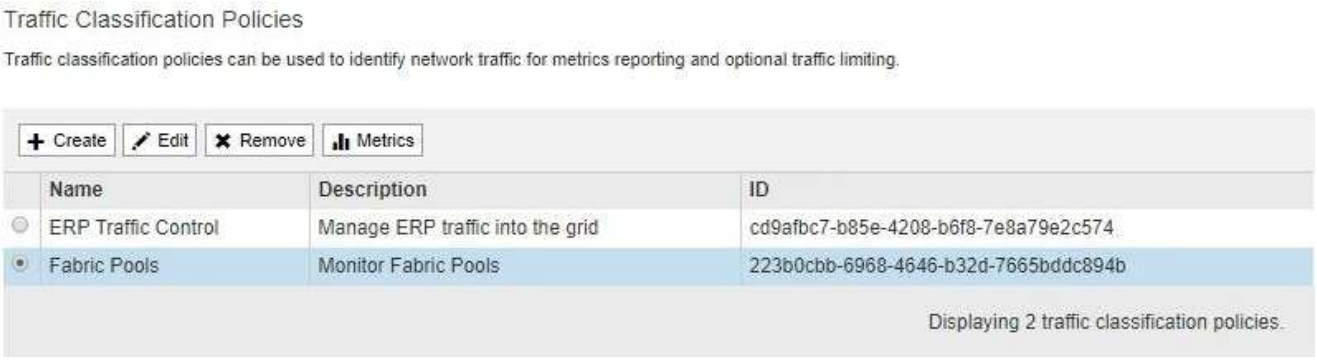

e. Repita estos pasos para cada límite que desee agregar a la directiva.

   Por ejemplo, si desea crear un límite de ancho de banda de 40 Gbps para un nivel de acuerdo de nivel de servicio, cree un límite de ancho de banda del agregado en el límite y un límite de ancho de banda de agregado en y establezca cada uno de entre 1 y 40 Gbps.

   Para convertir megabytes por segundo a gigabits por segundo, multiplique por ocho. Por ejemplo, 125 MB/s equivale a 1,000 Mbps o 1 Gbps.

7. Cuando termine de crear reglas y límites, seleccione **Guardar**.

   La directiva se guarda y se muestra en la tabla Directivas de clasificación del tráfico.




   El tráfico del cliente S3 y Swift ahora se gestiona de acuerdo con las políticas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera. Consulte Ver las métricas de tráfico de red.

### Edite una directiva de clasificación de tráfico

Puede editar una directiva de clasificación de tráfico para cambiar su nombre o

descripción, o para crear, editar o eliminar cualquier regla o límite para la directiva.

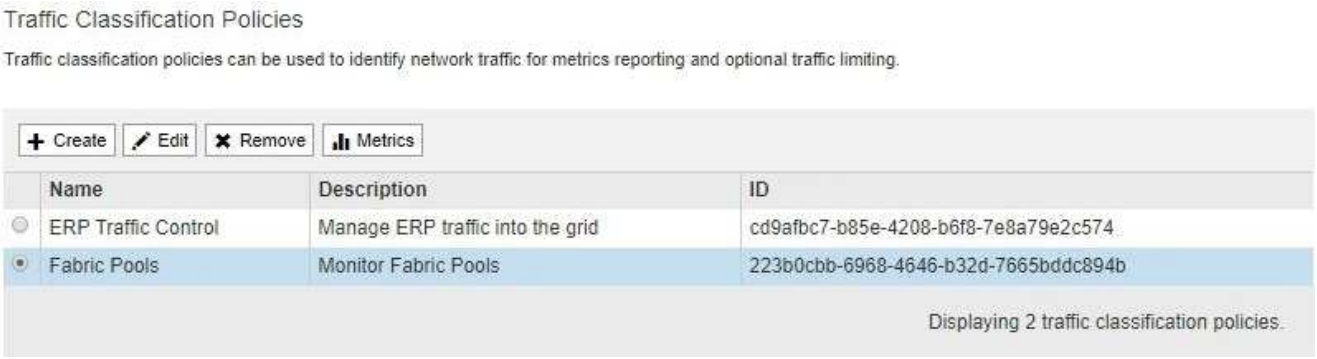
**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

**Pasos**

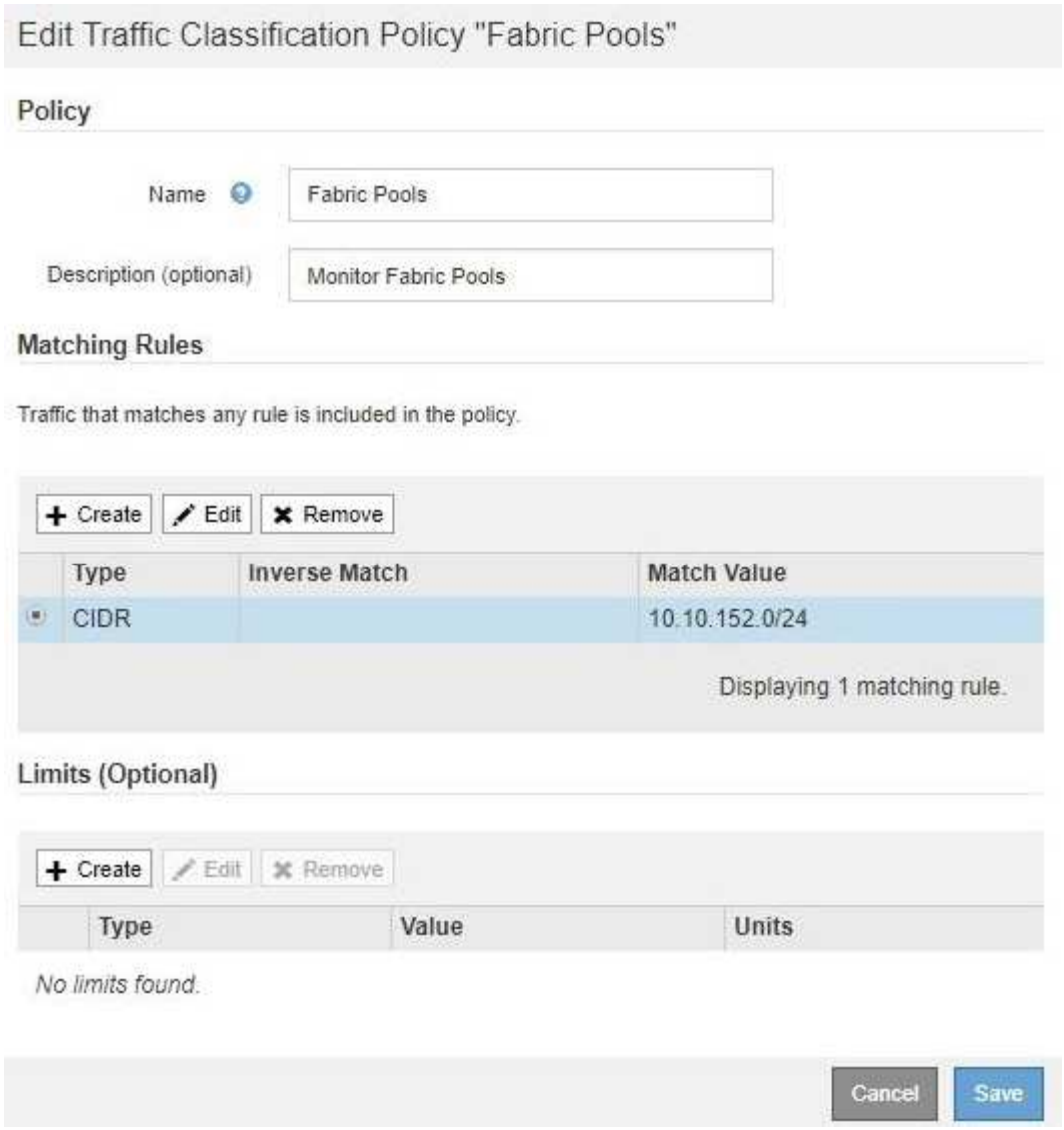
1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.




2. Seleccione el botón de opción situado a la izquierda de la directiva que desea editar.
3. Seleccione **Editar**.

   Aparece el cuadro de diálogo Editar directiva de clasificación del tráfico.




4. Cree, edite o elimine reglas y límites coincidentes según sea necesario.
   a. Para crear una regla o un límite coincidente, seleccione **Crear** y siga las instrucciones para crear una regla o crear un límite.
   b. Para editar una regla o un límite coincidente, seleccione el botón de opción para la regla o límite, seleccione **Editar** en la sección **Reglas coincidentes** o la sección **límites** y siga las instrucciones para crear una regla o crear un límite.
   c. Para eliminar una regla o un límite coincidente, seleccione el botón de opción de la regla o límite y seleccione **Quitar**. A continuación, seleccione **Aceptar** para confirmar que desea eliminar la regla o el límite.
5. Cuando haya terminado de crear o editar una regla o un límite, seleccione **aplicar**.
6. Cuando termine de editar la directiva, seleccione **Guardar**.

   Los cambios realizados en la directiva se guardan y el tráfico de red se gestiona de acuerdo con las directivas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

### Eliminar una directiva de clasificación de tráfico

Si ya no necesita una directiva de clasificación del tráfico, puede eliminarla.

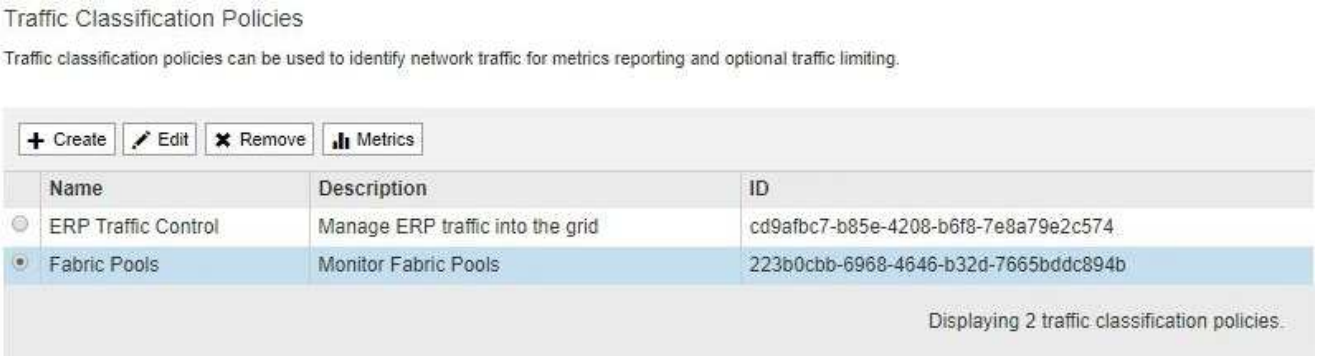
**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.




2. Seleccione el botón de opción situado a la izquierda de la directiva que desea eliminar.
3. Seleccione **Quitar**.

   Aparecerá un cuadro de diálogo Advertencia.

4. Seleccione **Aceptar** para confirmar que desea eliminar la directiva.

   La directiva se elimina.

### Ver las métricas de tráfico de red

Puede supervisar el tráfico de red mediante la visualización de los gráficos disponibles en la página Directivas de clasificación del tráfico.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz o Cuentas de inquilino.

**Acerca de esta tarea**

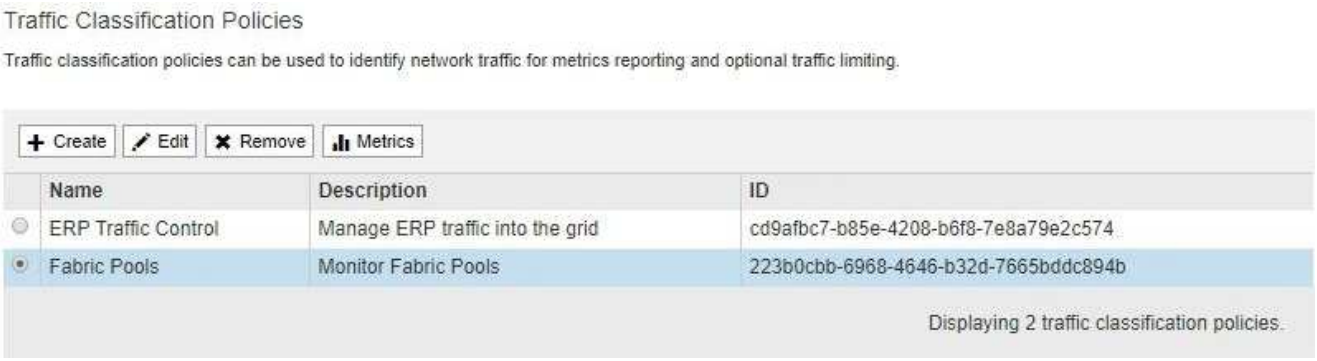
Para cualquier directiva de clasificación de tráfico existente, puede ver las métricas del servicio Load Balancer para determinar si la directiva limita correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si es necesario ajustar la política.

Incluso si no se establecen límites para una política de clasificación del tráfico, se recopilan las métricas y los gráficos proporcionan información útil para comprender las tendencias del tráfico.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.




   Los botones **Crear**, **Editar** y **Quitar** están desactivados si tiene el permiso Cuentas de arrendatario pero no tiene el permiso acceso raíz.

2. Seleccione el botón de opción situado a la izquierda de la política para la que desea ver las métricas.
3. Seleccione **métricas**.

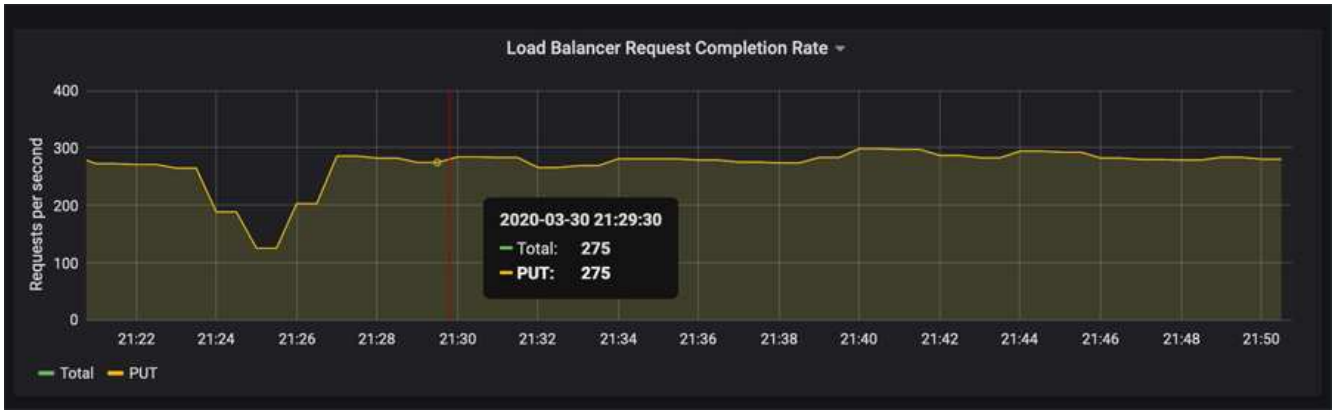
   Se abrirá una nueva ventana del explorador y aparecerán los gráficos de la directiva de clasificación del tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Puede seleccionar otras directivas para visualizarlas mediante el menú desplegable **Policy**.

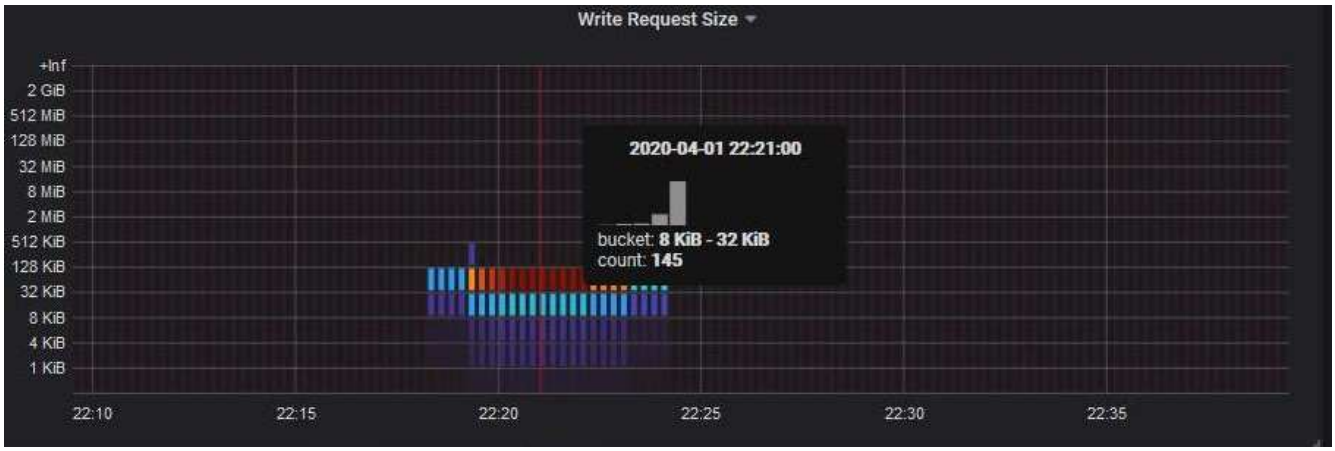
Los siguientes gráficos están incluidos en la página web.

- Tráfico de solicitud del equilibrador de carga: Este gráfico proporciona una media móvil de 3 minutos del rendimiento de los datos transmitidos entre los extremos del equilibrador de carga y los clientes que realizan las solicitudes, en bits por segundo.
- Tasa de finalización de solicitudes de equilibrador de carga: Este gráfico proporciona una media de movimiento de 3 minutos del número de solicitudes completadas por segundo, desglosadas por tipo de solicitud (GET, PUT, HEAD y DELETE). Este valor se actualiza cuando se han validado los encabezados de una nueva solicitud.
- Tasa de respuesta de error: Este gráfico proporciona un promedio móvil de 3 minutos del número de respuestas de error devueltas a clientes por segundo, desglosado por el código de respuesta de error.
- Duración media de la solicitud (sin error): Este gráfico proporciona una media móvil de 3 minutos de duración de la solicitud, desglosada por tipo de solicitud (GET, PUT, HEAD y DELETE). Cada duración de la solicitud comienza cuando el servicio Load Balancer analiza una cabecera de solicitud y finaliza cuando se devuelve el cuerpo de respuesta completo al cliente.
- Tasa de solicitud de escritura por tamaño de objeto: Este mapa térmico proporciona una media móvil de 3 minutos de la velocidad a la que se completan las solicitudes de escritura en función del tamaño del objeto. En este contexto, las solicitudes de escritura se refieren sólo a SOLICITUDES PUT.
- Tasa de solicitud de lectura por tamaño de objeto: Este mapa térmico proporciona una media móvil de 3 minutos de la velocidad a la que se completan las solicitudes de lectura en función del tamaño del objeto. En este contexto, las solicitudes de lectura se refieren sólo a OBTENER solicitudes. Los colores del mapa térmico indican la frecuencia relativa de un tamaño de objeto dentro de un gráfico individual. Los colores más frescos (por ejemplo, púrpura y azul) indican tasas relativas más bajas, y los colores más cálidos (por ejemplo, naranja y rojo) indican tasas relativas más altas.

4. Pase el cursor por un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.




5. Pase el cursor por encima de un mapa térmico para ver una ventana emergente que muestra la fecha y hora de la muestra, los tamaños de objeto agregados al recuento y el número de solicitudes por segundo durante ese período de tiempo.




6. Utilice el menú desplegable **Política** de la parte superior izquierda para seleccionar una directiva diferente.

   Se muestran los gráficos de la política seleccionada.

7. También puede acceder a los gráficos desde el menú **SUPPORT**.
   a. Seleccione **SUPPORT** > **Tools** > **Metrics**.
   b. En la sección **Grafana** de la página, seleccione **Directiva de clasificación de tráfico**.
   c. Seleccione la política del menú desplegable que hay en la esquina superior izquierda de la página.

      Las directivas de clasificación del tráfico se identifican por su ID. Los ID de directiva se muestran en la página Directivas de clasificación de tráfico.

8. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

**Información relacionada**

Supervisión y solución de problemas

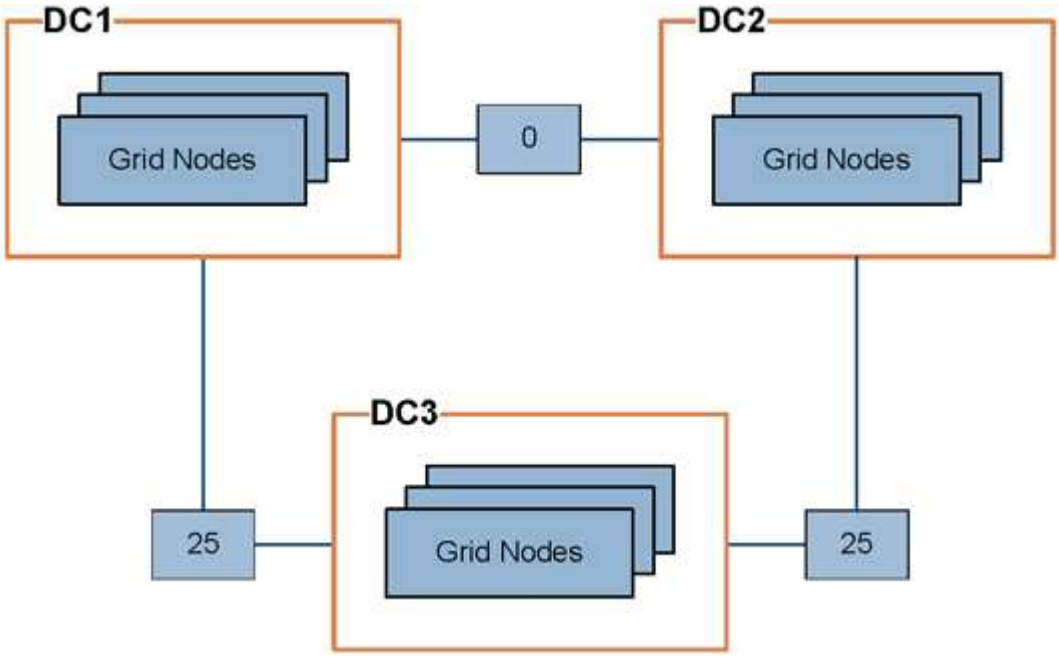
## Gestionar costes de enlaces

### ¿Cuáles son los costes de enlace

Los costes de enlace le permiten priorizar qué sitio de centro de datos proporciona un servicio solicitado cuando existen dos o más centros de datos. Puede ajustar los costes de vínculo para reflejar la latencia entre los sitios.

- Los costes de enlace se utilizan para priorizar qué copia de objetos se utiliza para llevar a cabo las recuperaciones de objetos.
- Los costes de enlace los utiliza la API de gestión de grid y la API de gestión de inquilinos para determinar qué servicios StorageGRID internos utilizar.
- Los costes de enlace se utilizan en el servicio de equilibrador de carga de conexión (CLB) obsoleto de los nodos de puerta de enlace para dirigir las conexiones de cliente. Consulte Cómo funciona el equilibrio de carga: Servicio CLB.

El diagrama muestra una cuadrícula de tres sitios con costes de enlace configurados entre sitios:




- El servicio CLB de los nodos Gateway distribuye igualmente las conexiones de cliente a todos los nodos de almacenamiento del mismo sitio del centro de datos y a cualquier sitio del centro de datos con un coste de enlace de 0.

  En el ejemplo, un nodo de puerta de enlace en el sitio del centro de datos 1 (DC1) distribuye igualmente conexiones de cliente a nodos de almacenamiento en DC1 y a nodos de almacenamiento en DC2. Un nodo de puerta de enlace en DC3 envía conexiones de cliente sólo a los nodos de almacenamiento en DC3.

- Al recuperar un objeto que existe como varias copias replicadas, StorageGRID recupera la copia en el centro de datos que tiene el coste de enlace más bajo.

  En el ejemplo, si una aplicación cliente en DC2 recupera un objeto almacenado en DC1 y DC3, el objeto se recupera de DC1, ya que el coste del vínculo de DC1 a D2 es 0, que es inferior al coste del vínculo de DC3 a DC2 (25).

Los costes de enlace son números relativos arbitrarios sin unidad de medida específica. Por ejemplo, un costo

de enlace de 50 se utiliza de forma menos preferente que un costo de enlace de 25. En la tabla se muestran los costes de los enlaces más utilizados.

| Enlace | Coste del enlace | Notas |
|---|---|---|
| Entre sitios físicos del centro de datos | 25 (predeterminado) | Centros de datos conectados por un enlace WAN. |
| Entre las ubicaciones lógicas del centro de datos en la misma ubicación física | 0 | Centros de datos lógicos en el mismo edificio físico o campus conectados por una LAN. |

### Actualizar costes de enlace

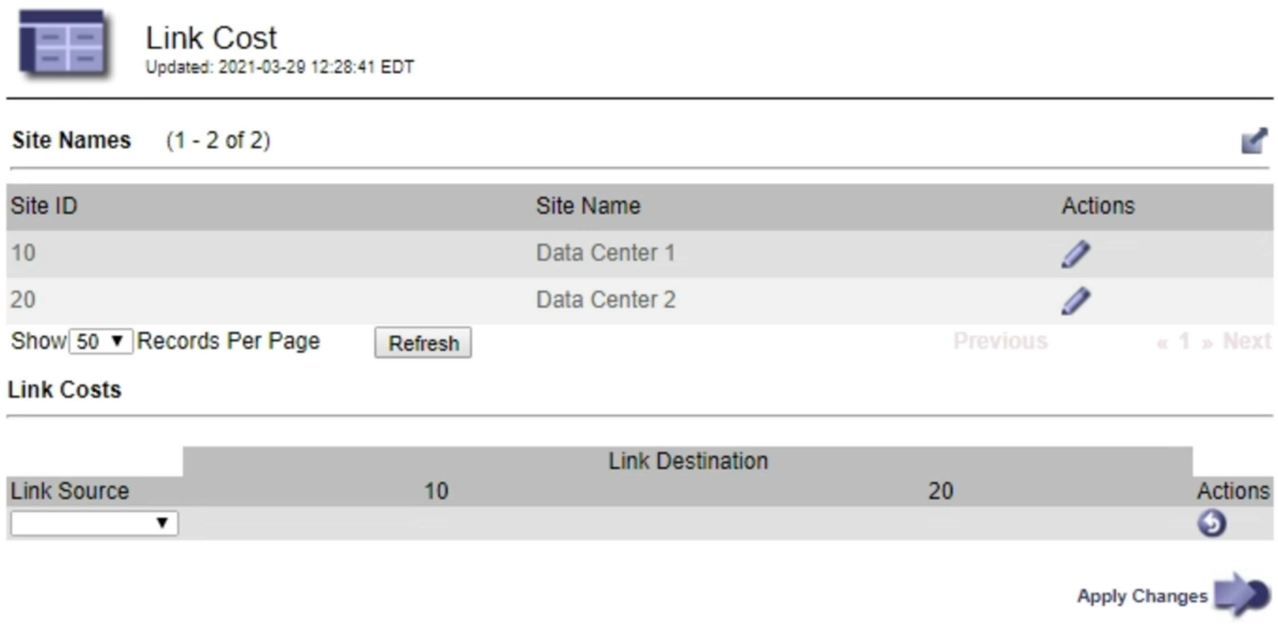
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Configuración de página de topología de cuadrícula.

#### Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **coste de enlace**.




2. Seleccione un sitio en **origen de enlace** e introduzca un valor de coste entre 0 y 100 en **destino de enlace**.

   No se puede cambiar el coste del vínculo si el origen es el mismo que el destino.

   Para cancelar los cambios, seleccione **Revert**.

3. Seleccione **aplicar cambios**.

# Utilice AutoSupport

## ¿Qué es AutoSupport?

La función AutoSupport permite que el sistema StorageGRID envíe mensajes de estado y estado al soporte técnico.

El uso de AutoSupport puede acelerar significativamente la detección y resolución de problemas. El soporte técnico también puede supervisar las necesidades de almacenamiento del sistema y ayudarle a determinar si necesita añadir nodos o sitios nuevos. De manera opcional, puede configurar los mensajes de AutoSupport para que se envíen a un destino adicional.

### Información incluida en los mensajes de AutoSupport

Los mensajes de AutoSupport incluyen información como la siguiente:

- Versión del software StorageGRID
- Versión del sistema operativo
- Información de atributos a nivel de sistema y ubicación
- Alertas y alarmas recientes (sistema heredado)
- Estado actual de todas las tareas de cuadrícula, incluidos los datos históricos
- Uso de la base de datos del nodo de administrador
- Número de objetos perdidos o faltantes
- Ajustes de configuración de cuadrícula
- Entidades NMS
- Política de ILM activa
- Archivo de especificación de grid aprovisionado
- Métricas de diagnóstico

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante. Si AutoSupport no está habilitado, aparecerá un mensaje en el Panel de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport.

Si cierra el mensaje, no volverá a aparecer hasta que se borre la caché del explorador, aunque AutoSupport permanezca deshabilitado.

### ¿Qué es Active IQ?

Active IQ es un asesor digital basado en cloud que aprovecha el análisis predictivo y los conocimientos de la comunidad de la base instalada de NetApp. Sus evaluaciones de riesgos continuas, las alertas predictivas, las directrices prescriptivas y las acciones automatizadas le ayudan a evitar problemas antes de que se produzcan, lo que mejora el estado del sistema y aumenta la disponibilidad del sistema.

Debe habilitar AutoSupport si desea usar las consolas y la funcionalidad de Active IQ del sitio de soporte de NetApp.

"Documentación del asesor digital de Active IQ"

### Protocolos para enviar mensajes AutoSupport

Puede elegir uno de los tres protocolos para enviar mensajes de AutoSupport:

- HTTPS
- HTTP
- SMTP

Si envía mensajes de AutoSupport mediante HTTPS o HTTP, puede configurar un servidor proxy no transparente entre los nodos de administrador y el soporte técnico.

Si utiliza SMTP como protocolo para mensajes de AutoSupport, debe configurar un servidor de correo SMTP.

### Opciones de AutoSupport

Puede utilizar cualquier combinación de las siguientes opciones para enviar mensajes de AutoSupport al soporte técnico:

- **Semanal**: Envía automáticamente mensajes de AutoSupport una vez por semana. Valor predeterminado: Activado.
- **Desencadenada por eventos**: Envía automáticamente mensajes AutoSupport cada hora o cuando se producen eventos significativos del sistema. Valor predeterminado: Activado.
- **A petición**: Permita que el servicio de asistencia técnica solicite que el sistema StorageGRID envíe mensajes AutoSupport automáticamente, lo que resulta útil cuando está trabajando activamente en un problema (requiere el protocolo de transmisión HTTPS AutoSupport). Ajuste predeterminado: Desactivado.
- **Desencadenado por el usuario**: Envía manualmente mensajes AutoSupport en cualquier momento.

### Información relacionada

"Soporte de NetApp"

## Configure AutoSupport

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante.

### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz u otra configuración de cuadrícula.

- Si utilizará el protocolo HTTPS o HTTP para enviar mensajes AutoSupport, ha proporcionado acceso saliente a Internet al nodo de administración principal, ya sea directamente o mediante un servidor proxy (no se necesitan conexiones entrantes).
- Si usará el protocolo HTTPS o HTTP y desea utilizar un servidor proxy, ya lo tiene Se configuró un servidor proxy de administrador.
- Si utilizará SMTP como protocolo para mensajes de AutoSupport, configuró un servidor de correo SMTP. La misma configuración del servidor de correo se utiliza para las notificaciones de correo electrónico de alarma (sistema heredado).

### Especifique el protocolo para los mensajes de AutoSupport

Puede utilizar cualquiera de los siguientes protocolos para enviar mensajes de AutoSupport:

- **HTTPS**: Es la configuración predeterminada y recomendada para nuevas instalaciones. El protocolo HTTPS utiliza el puerto 443. Si desea habilitar la función AutoSupport On Demand, debe usar el protocolo HTTPS.
- **HTTP**: Este protocolo no es seguro, a menos que se utilice en un entorno de confianza donde el servidor proxy se convierte a HTTPS al enviar datos a través de Internet. El protocolo HTTP utiliza el puerto 80.
- **SMTP**: Utilice esta opción si desea que se envíen mensajes de AutoSupport por correo electrónico. Si utiliza SMTP como protocolo para mensajes AutoSupport, debe configurar un servidor de correo SMTP en la página Configuración de correo electrónico heredado (**SUPPORT** > **Alarmas (heredado)** > **Configuración de correo electrónico heredado**).

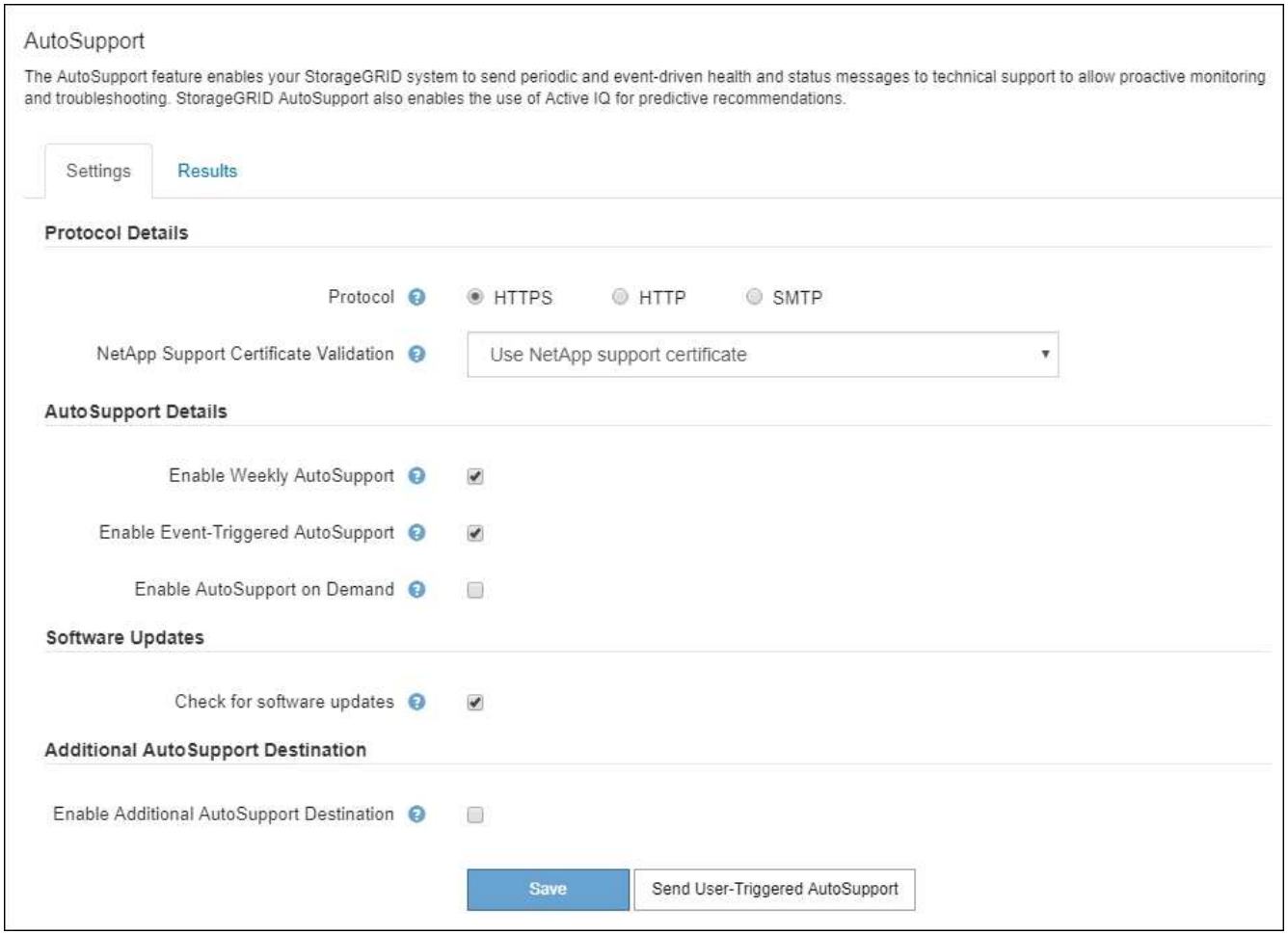
> ⓘ SMTP era el único protocolo disponible para mensajes de AutoSupport antes de la versión de StorageGRID 11.2. Si instaló inicialmente una versión anterior de StorageGRID, es posible que SMTP sea el protocolo seleccionado.

El protocolo configurado se utiliza para enviar todos los tipos de mensajes de AutoSupport.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.

   Aparece la página AutoSupport y la ficha **Configuración** está seleccionada.



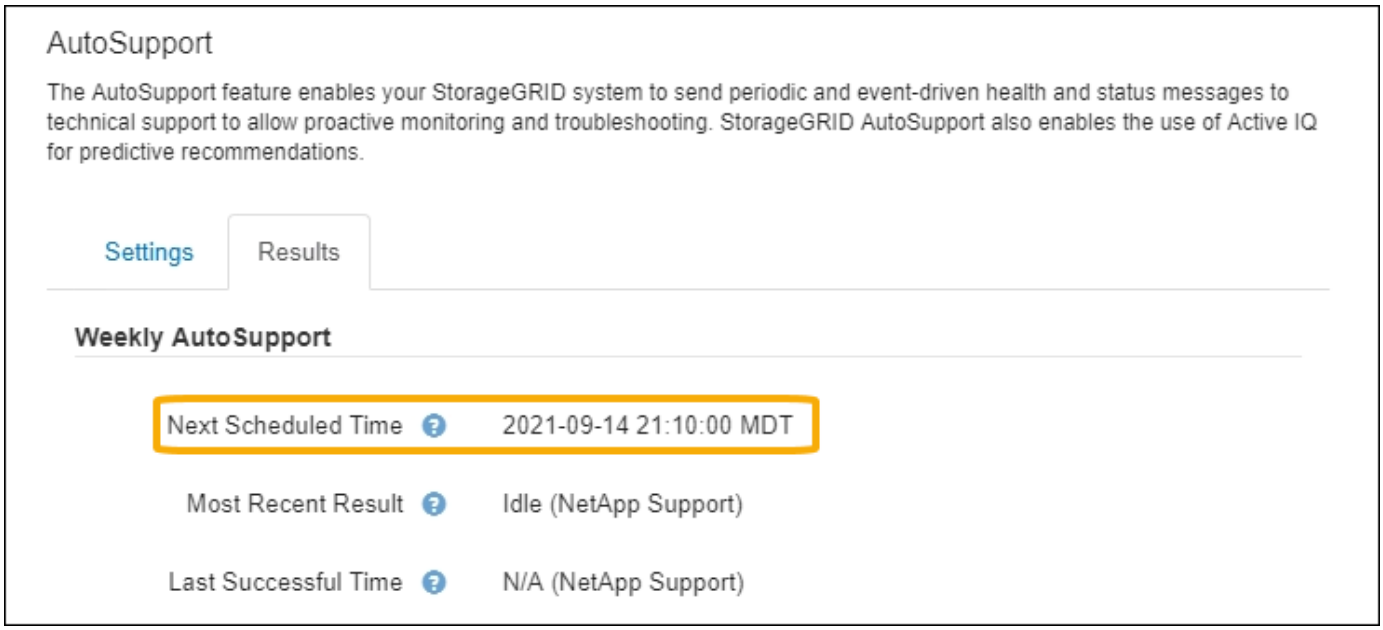

2. Seleccione el protocolo que desea utilizar para enviar mensajes de AutoSupport.
3. Si seleccionó **HTTPS**, seleccione si desea utilizar un certificado TLS para proteger la conexión con el servidor de soporte de NetApp.
   - **Utilizar el certificado de soporte de NetApp** (predeterminado): La validación del certificado garantiza la seguridad de la transmisión de mensajes AutoSupport. El certificado de soporte de NetApp ya está instalado con el software StorageGRID.
   - **No verificar certificado**: Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.
4. Seleccione **Guardar**.

   Todos los mensajes semanales, activados por el usuario y activados por un evento se envían mediante el protocolo seleccionado.

### Desactivar los mensajes semanales de AutoSupport

De manera predeterminada, el sistema StorageGRID se configura para que envíe un mensaje de AutoSupport al soporte de NetApp una vez por semana.

Para determinar cuándo se enviará el mensaje semanal de AutoSupport, vaya a la ficha **AutoSupport** > **resultados**. En la sección **AutoSupport** semanal, consulte el valor de **próxima hora programada**.




Puede deshabilitar el envío automático de mensajes semanales de AutoSupport en cualquier momento.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Anule la selección de la casilla de verificación **Activar AutoSupport semanal**.
3. Seleccione **Guardar**.

### Deshabilite los mensajes de AutoSupport activados por un evento

De forma predeterminada, el sistema StorageGRID se configura para enviar un mensaje de AutoSupport al soporte de NetApp cuando se produce una alerta importante u otro evento significativo del sistema.

Puede deshabilitar los mensajes de AutoSupport activados por eventos en cualquier momento.

> Los mensajes de AutoSupport activados por los eventos también se suprimen cuando se suprimen las notificaciones de correo electrónico de todo el sistema. (Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de visualización**. A continuación, seleccione **notificación Suprimir todo**.)

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Anule la selección de la casilla de verificación **Activar AutoSupport** desencadenado por eventos.
3. Seleccione **Guardar**.

### Habilite AutoSupport bajo demanda

AutoSupport On Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente.

De manera predeterminada, AutoSupport On Demand está deshabilitado. Al habilitar esta función, el soporte técnico puede solicitar que el sistema StorageGRID envíe mensajes de AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de sondeo para AutoSupport en consultas bajo demanda.

El soporte técnico no puede habilitar o deshabilitar AutoSupport bajo demanda.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Seleccione **HTTPS** para el protocolo.
3. Active la casilla de verificación **Activar AutoSupport semanal**.
4. Active la casilla de verificación **Activar AutoSupport a petición**.
5. Seleccione **Guardar**.

   AutoSupport On Demand está habilitado y el soporte técnico puede enviar solicitudes AutoSupport On Demand a StorageGRID.

### Desactive las comprobaciones de actualizaciones de software

De forma predeterminada, StorageGRID se pone en contacto con NetApp para determinar si hay actualizaciones de software disponibles para su sistema. Si hay disponible una revisión o versión nueva de StorageGRID, se muestra la nueva versión en la página actualización de StorageGRID.

Según sea necesario, puede desactivar opcionalmente la comprobación de actualizaciones de software. Por ejemplo, si el sistema no tiene acceso WAN, debe desactivar la comprobación para evitar errores de descarga.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Deseleccione la casilla de verificación **Buscar actualizaciones de software**.
3. Seleccione **Guardar**.

### Añada un destino de AutoSupport adicional

Cuando se habilita AutoSupport, se envían mensajes de estado y estado al soporte de NetApp. Puede especificar un destino adicional para todos los mensajes de AutoSupport.

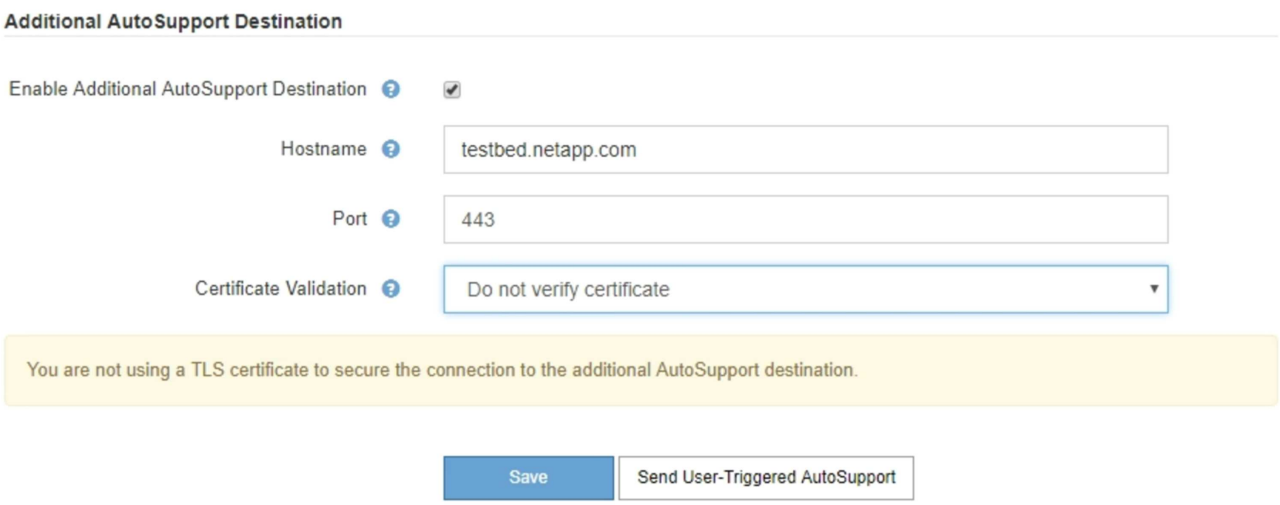
Para comprobar o cambiar el protocolo utilizado para enviar mensajes AutoSupport, consulte las instrucciones a. Especifique el protocolo para los mensajes de AutoSupport.

> No se puede utilizar el protocolo SMTP para enviar mensajes de AutoSupport a un destino adicional.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Seleccione **Activar destino AutoSupport adicional**.

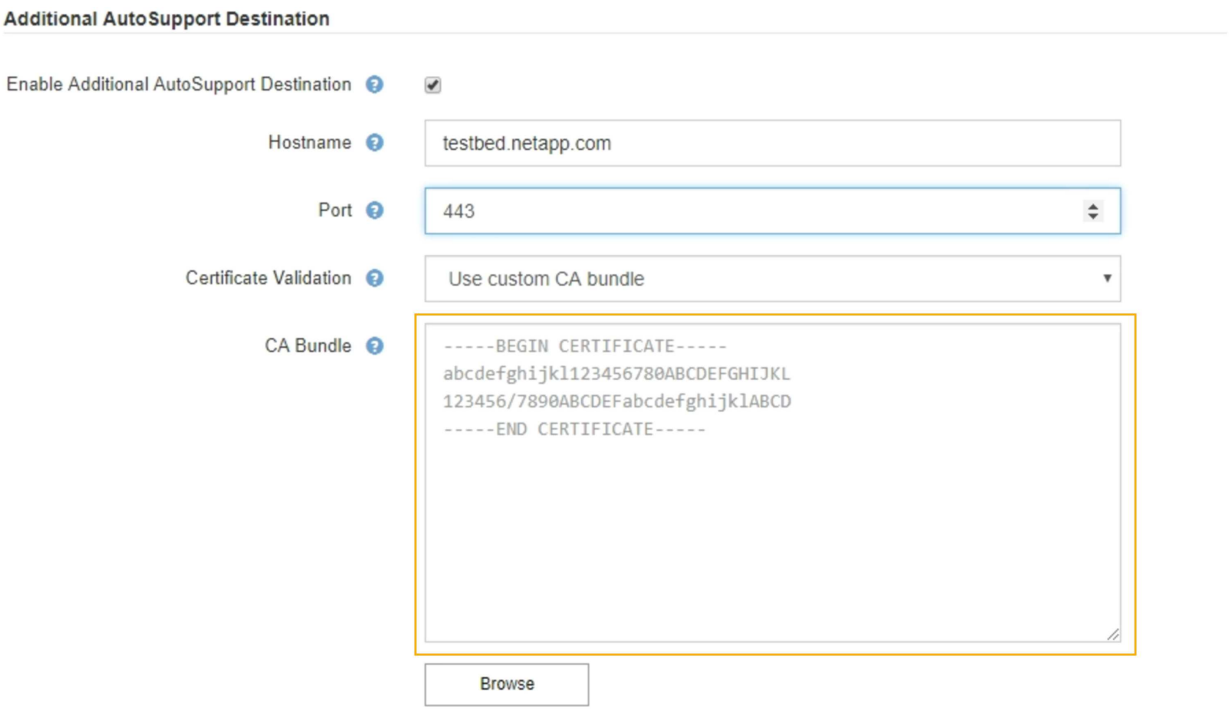
   Aparecerán los campos destino AutoSupport adicional.




3. Introduzca el nombre de host o la dirección IP del servidor de un servidor de destino AutoSupport adicional.

   Puede introducir solo un destino adicional.

4. Introduzca el puerto utilizado para conectarse a un servidor de destino AutoSupport adicional (el puerto predeterminado es el 80 para HTTP o el puerto 443 para HTTPS).
5. Para enviar los mensajes de AutoSupport con validación de certificados, seleccione **usar paquete de CA personalizado** en el menú desplegable **validación de certificados**. A continuación, realice una de las siguientes acciones:
   - Utilice una herramienta de edición para copiar y pegar todo el contenido de cada uno de los archivos de certificados de CA codificados con PEM en el campo **paquete de CA**, concatenado en el orden de la cadena de certificados. Debe incluir `----BEGIN CERTIFICATE----` y.. `----END CERTIFICATE----` en su selección.



◦ Seleccione **examinar**, desplácese hasta el archivo que contiene los certificados y, a continuación, seleccione **Abrir** para cargar el archivo. La validación de certificados garantiza la seguridad de la transmisión de mensajes de AutoSupport.

6. Para enviar sus mensajes AutoSupport sin validación de certificados, seleccione **no verificar certificado** en el menú desplegable **validación de certificados**.

   Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.

   Aparece un mensaje de precaución: "No está utilizando un certificado TLS para garantizar la conexión al destino AutoSupport adicional".

7. Seleccione **Guardar**.

   Todos los futuros mensajes de AutoSupport semanales, activados por un evento y activados por el usuario se enviarán al destino adicional.

## Active manualmente un mensaje de AutoSupport

Con el fin de ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID, puede activar manualmente el envío de un mensaje de AutoSupport.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz u otra configuración de cuadrícula.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Seleccione **Enviar AutoSupport desencadenado por el usuario**.

   StorageGRID intenta enviar un mensaje de AutoSupport al soporte técnico. Si el intento se realiza correctamente, se actualizan los valores **resultado más reciente** y **tiempo más reciente** de la ficha **resultados**. Si hay algún problema, el valor del **resultado más reciente** se actualiza a "error" y StorageGRID no intenta volver a enviar el mensaje AutoSupport.

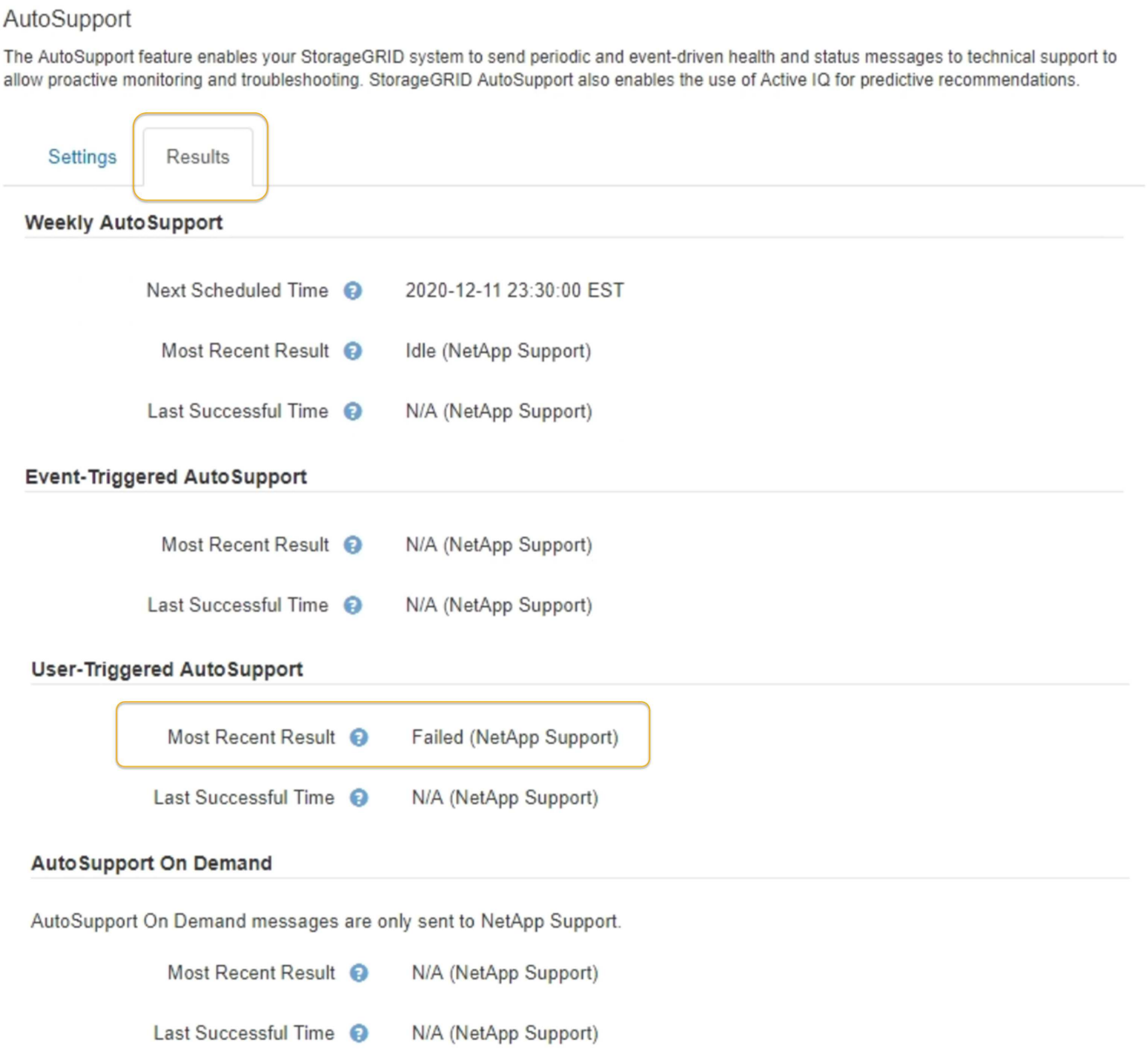
   > Después de enviar un mensaje AutoSupport activado por el usuario, actualice la página AutoSupport en el explorador después de 1 minuto para acceder a los resultados más recientes.

## Solucionar los problemas de los mensajes de AutoSupport

Si se produce un error al intentar enviar un mensaje de AutoSupport, el sistema StorageGRID realiza distintas acciones según el tipo de mensaje de AutoSupport. Puede comprobar el estado de los mensajes de AutoSupport seleccionando **ASISTENCIA** > **Herramientas** > **AutoSupport** > **resultados**.

Los mensajes de AutoSupport activados por un evento se suprimen cuando se suprimen las notificaciones de correo electrónico de todo el sistema. (Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de visualización**. A continuación, seleccione **notificación Suprimir todo**.)

Cuando el mensaje AutoSupport no se envía, aparece "'failed'" en la ficha **resultados** de la página **AutoSupport**.




### Fallo de mensaje semanal de AutoSupport

Si un mensaje semanal de AutoSupport no se envía, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo de resultado más reciente a Reintentando.
2. Intenta reenviar el mensaje AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de errores de envío, actualiza el atributo de resultado más reciente a error.

4. Intenta enviar de nuevo un mensaje de AutoSupport a la siguiente hora programada.
5. Mantiene la programación normal de AutoSupport si el mensaje falla porque el servicio NMS no está disponible y si se envía un mensaje antes de pasar siete días.
6. Cuando el servicio NMS está disponible de nuevo, envía un mensaje AutoSupport inmediatamente si no se ha enviado un mensaje durante siete días o más.

#### Error de mensaje AutoSupport activado por el usuario o activado por eventos

Si un mensaje AutoSupport activado por el usuario o activado por un evento no se puede enviar, el sistema StorageGRID lleva a cabo las siguientes acciones:

1. Muestra un mensaje de error si se conoce el error. Por ejemplo, si un usuario selecciona el protocolo SMTP sin proporcionar la configuración de correo electrónico correcta, se muestra el siguiente error: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. No intenta volver a enviar el mensaje.
3. Registra el error en `nms.log`.

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico está en ejecución (**SUPPORT** > **Alarmas (heredado)** > **> Configuración de correo electrónico heredado**). El siguiente mensaje de error puede aparecer en la página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Obtenga información acerca de cómo configurar los ajustes del servidor de correo electrónico en supervisar y solucionar problemas de instrucciones.

#### Corrija un error en un mensaje de AutoSupport

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico se está ejecutando. El siguiente mensaje de error puede aparecer en la página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

## Envíe mensajes de AutoSupport de E-Series a través de StorageGRID

Puede enviar mensajes de AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administrador de StorageGRID en lugar de hacerlo con el puerto de gestión del dispositivo de almacenamiento.

#### Lo que necesitará

- Se ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de administrador de dispositivo de almacenamiento o acceso raíz.

> Debe tener el firmware 8.70 (11.7) de SANtricity o superior para acceder a SANtricity System Manager mediante Grid Manager.

#### Acerca de esta tarea

Los mensajes de AutoSupport de E-Series contienen detalles del hardware de almacenamiento y son más

específicos que otros mensajes de AutoSupport que envía el sistema StorageGRID.

Configurar una dirección de servidor proxy especial en System Manager de SANtricity para que los mensajes de AutoSupport se transmitan a través de un nodo de administración de StorageGRID sin usar el puerto de gestión del dispositivo. Los mensajes AutoSupport transmitidos de esta manera respetan la configuración de proxy de administrador y remitente preferido que se puede haber configurado en el Administrador de grid.

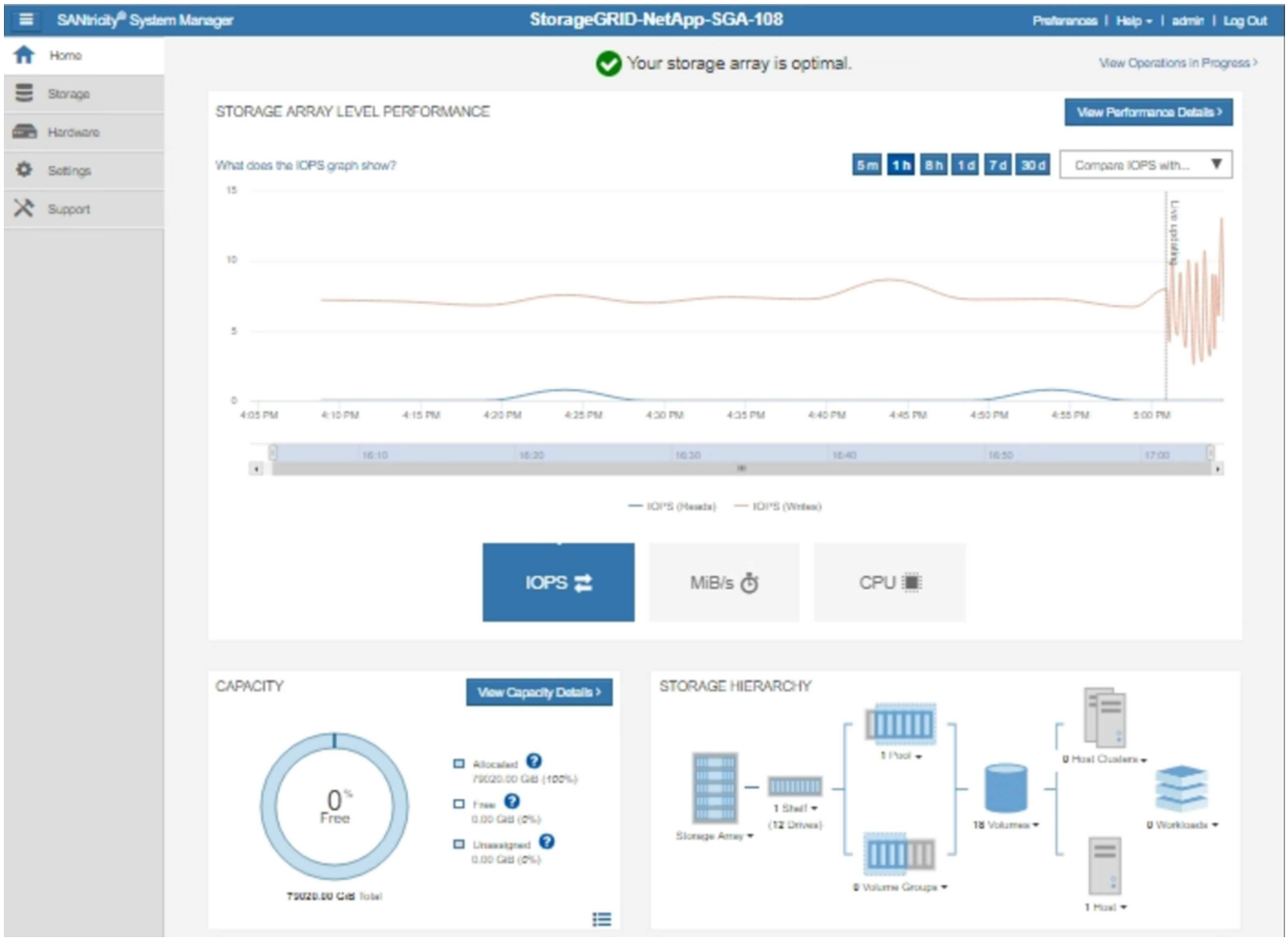
Si desea configurar el servidor proxy de administración en Grid Manager, consulte Configure los ajustes del proxy de administración.

> Este procedimiento solo se utiliza para configurar un servidor proxy StorageGRID para los mensajes de AutoSupport E-Series. Si quiere más información sobre la configuración de la serie AutoSupport de E-Series, consulte "Documentación de SANtricity y E-Series de NetApp".

**Pasos**

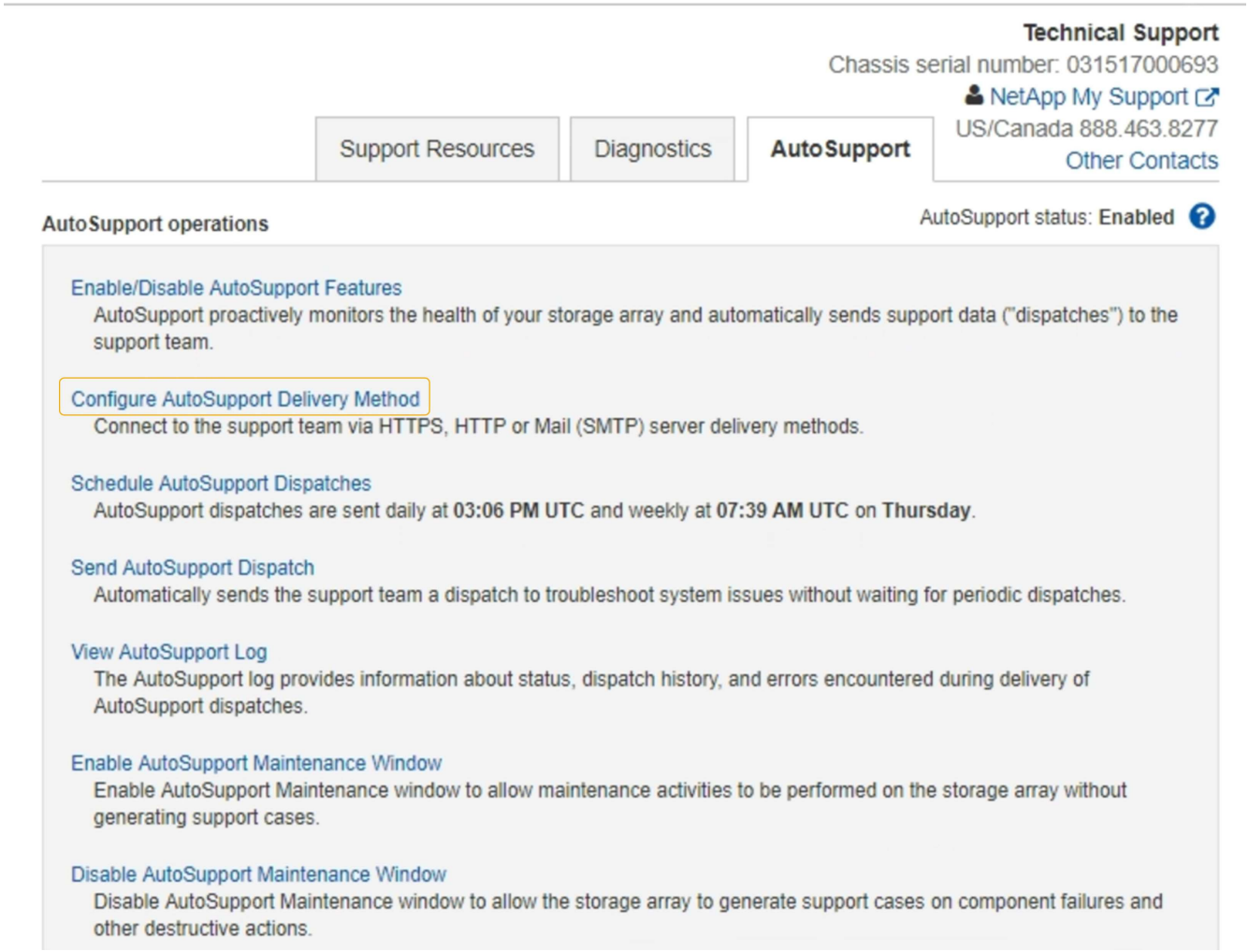
1. En Grid Manager, seleccione **NODES**.
2. En la lista de nodos que aparece a la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione **Administrador del sistema SANtricity**.

   Se mostrará la página de inicio de SANtricity System Manager.



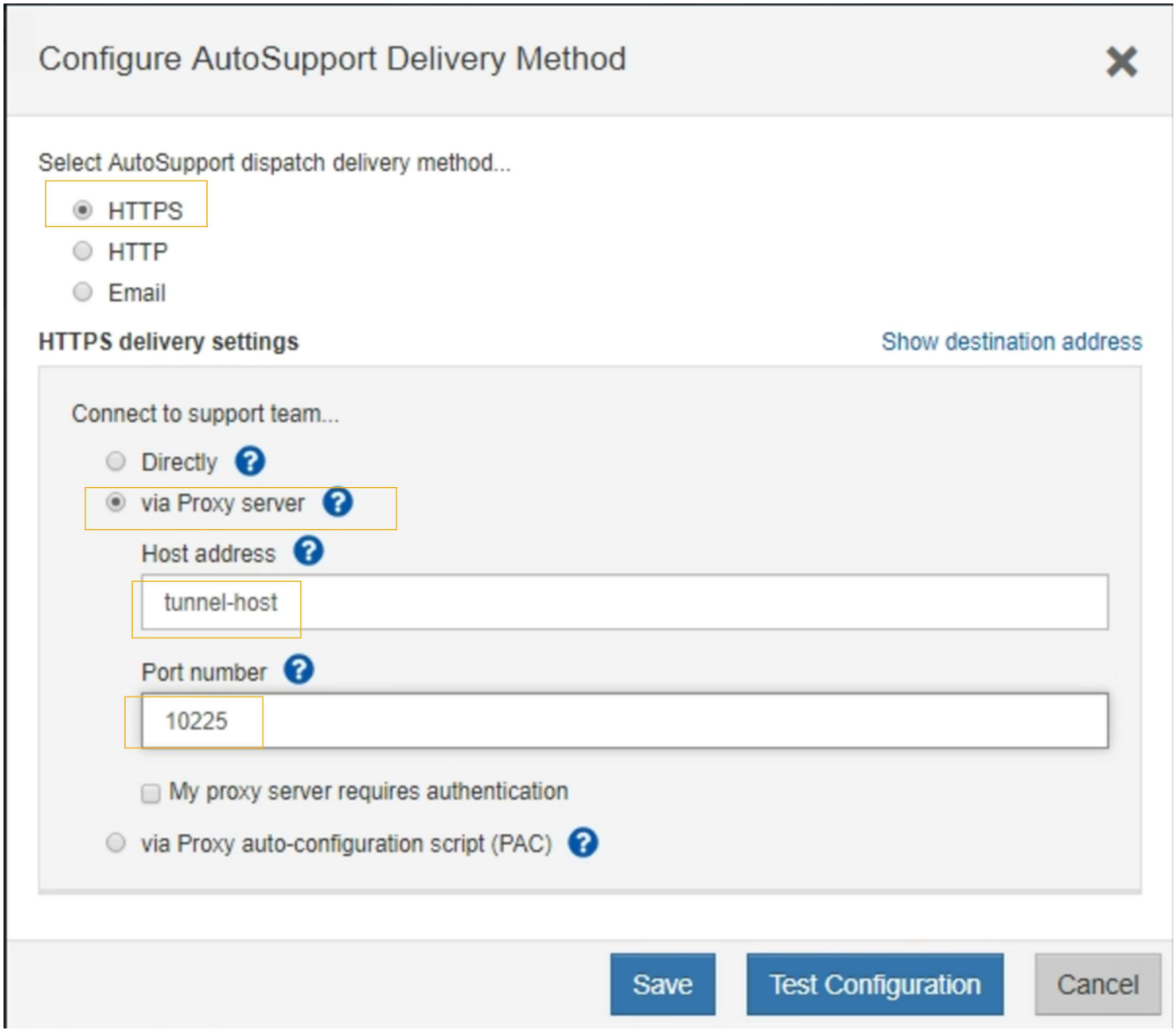

4. Seleccione **SUPPORT** > **Support Center** > **AutoSupport**.

Se muestra la página de operaciones AutoSupport.




5. Seleccione **Configurar método de entrega de AutoSupport**.

   Se muestra la página Configurar método de entrega de AutoSupport.




6. Seleccione **HTTPS** para el método de entrega.

   El certificado que permite el protocolo HTTPS está preinstalado.

7. Seleccione **a través del servidor proxy**.
8. Introduzca `tunnel-host` Para la **Dirección de host**.

   `tunnel-host` Es la dirección especial que usa un nodo de administrador para enviar mensajes de AutoSupport E-Series.

9. Introduzca `10225` Para el **número de puerto**.

   `10225` Es el número de puerto del servidor del proxy StorageGRID que recibe mensajes de AutoSupport de la controladora E-Series del dispositivo.

10. Seleccione **Configuración de prueba** para probar el enrutamiento y la configuración del servidor proxy AutoSupport.

    Si es correcto, aparecerá un mensaje en un banner verde: "'se ha verificado la configuración de

AutoSupport'".

Si la prueba falla, se muestra un mensaje de error en un banner rojo. Compruebe la configuración de DNS y las redes de StorageGRID, asegúrese de que el nodo de administrador del remitente preferido se pueda conectar al sitio de soporte de NetApp y vuelva a intentar la prueba.

11. Seleccione **Guardar**.

    Se guardará la configuración y aparecerá un mensaje de confirmación: "'se ha configurado el método de entrega de AutoSupport'".

# Gestione nodos de almacenamiento

## Acerca de la gestión de nodos de almacenamiento

Los nodos de almacenamiento proporcionan servicios y capacidad de almacenamiento en disco. La gestión de nodos de almacenamiento conlleva lo siguiente:

- Gestión de las opciones de almacenamiento
- Comprender qué son las marcas de agua del volumen de almacenamiento y cómo se pueden utilizar anulaciones de Marca de agua para controlar cuando los nodos de almacenamiento pasan a ser de sólo lectura
- Supervisar y gestionar el espacio usado para los metadatos de objetos
- Configuración de la configuración global de los objetos almacenados
- Aplicar las opciones de configuración del nodo de almacenamiento
- Gestión de nodos de almacenamiento completos

## ¿Qué es un nodo de almacenamiento?

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Cada sistema StorageGRID debe tener al menos tres nodos de almacenamiento. Si tiene varios sitios, cada sitio dentro del sistema StorageGRID también debe tener tres nodos de almacenamiento.

Un nodo de almacenamiento incluye los servicios y procesos necesarios para almacenar, mover, verificar y recuperar metadatos y datos de objetos en el disco. Puede ver información detallada sobre los nodos de almacenamiento en la página **NODES**.

### ¿Qué es el servicio ADC?

El servicio de controlador de dominio administrativo (ADC) autentica los nodos de grid y sus conexiones entre sí. El servicio ADC está alojado en cada uno de los tres primeros nodos de almacenamiento de un sitio.

El servicio ADC mantiene la información de topología, incluida la ubicación y disponibilidad de los servicios. Cuando un nodo de cuadrícula requiere información de otro nodo de cuadrícula o una acción que debe realizar otro nodo de cuadrícula, se pone en contacto con un servicio de ADC para encontrar el mejor nodo de cuadrícula para procesar su solicitud. Además, el servicio ADC conserva una copia de los paquetes de configuración de la implementación StorageGRID, lo que permite que cualquier nodo de la cuadrícula recupere la información de configuración actual.puede ver la información de ADC de un nodo de almacenamiento en la página Topología de la cuadrícula (**SUPPORT** > **topología de la cuadrícula**).

Para facilitar las operaciones distribuidas e iaterradas, cada servicio ADC sincroniza certificados, paquetes de configuración e información sobre servicios y topología con los otros servicios ADC del sistema StorageGRID.

En general, todos los nodos de grid mantienen una conexión al menos a un servicio de ADC. De este modo se garantiza que los nodos grid accedan siempre a la información más reciente. Cuando los nodos de grid se conectan, almacenan en caché los certificados de otros nodos de grid, lo que permite a los sistemas seguir funcionando con nodos de grid conocidos incluso cuando un servicio de ADC no está disponible. Los nuevos nodos de grid solo pueden establecer conexiones mediante un servicio ADC.

La conexión de cada nodo de cuadrícula permite al servicio ADC recopilar información de topología. Esta información sobre los nodos de grid incluye la carga de CPU, el espacio en disco disponible (si tiene almacenamiento), los servicios admitidos y el ID de sitio del nodo de grid. Otros servicios solicitan al servicio ADC información de topología a través de consultas de topología. El servicio ADC responde a cada consulta con la información más reciente recibida del sistema StorageGRID.

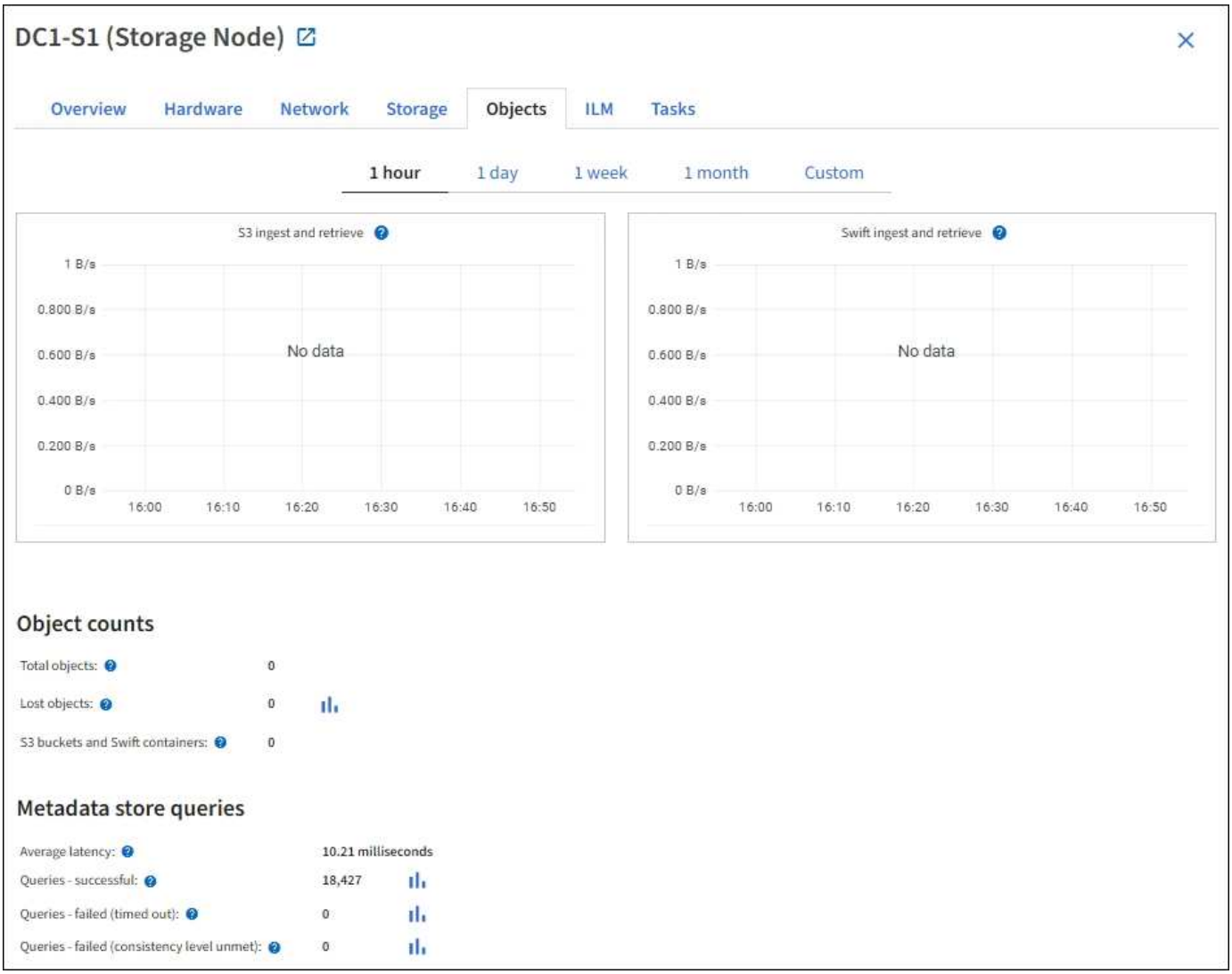
## ¿Qué es el servicio DDS?

Alojado por un nodo de almacenamiento, el servicio almacén de datos distribuidos (DDS) interactúa con la base de datos de Cassandra para realizar tareas en segundo plano en los metadatos de objeto almacenados en el sistema StorageGRID.

#### El número de objetos

El servicio DDS realiza un seguimiento del número total de objetos ingeridos en el sistema StorageGRID, así como del número total de objetos ingeridos a través de cada una de las interfaces compatibles del sistema (S3 o Swift).

Puede ver el número total de objetos en la página Nodes > la pestaña Objects de cualquier nodo de almacenamiento.




#### Consultas

Puede identificar el tiempo medio que tarda en ejecutar una consulta en el almacén de metadatos a través del servicio DDS específico, el número total de consultas correctas y el número total de consultas que han fallado debido a un problema de tiempo de espera.

Se recomienda revisar la información de consulta para supervisar el estado del almacén de metadatos, Cassandra, lo que afecta al rendimiento de procesamiento y recuperación del sistema. Por ejemplo, si la latencia de una consulta media es lenta y el número de consultas con errores debido a tiempos de espera es elevado, es posible que el almacén de metadatos encuentre una carga mayor o realice otra operación.

También puede ver el número total de consultas que han fallado debido a los fallos de consistencia. Los fallos de nivel de coherencia se deben a un número insuficiente de almacenes de metadatos disponibles en el momento en que se realiza una consulta a través del servicio DDS específico.

Puede utilizar la página Diagnósticos para obtener información adicional sobre el estado actual de la cuadrícula. Consulte Ejecutar diagnóstico.

#### Garantías y controles de coherencia

StorageGRID garantiza la coherencia de lectura tras escritura para los objetos recién creados. Cualquier OPERACIÓN DE OBTENER después de una operación DE PUT completada correctamente podrá leer los

datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones siguen siendo coherentes en la actualidad.

### ¿Qué es el servicio LDR?

Alojado por cada nodo de almacenamiento, el servicio de router de distribución local (LDR) gestiona el transporte de contenido para el sistema StorageGRID. El transporte de contenido abarca numerosas tareas, como el almacenamiento de datos, el enrutamiento y la gestión de solicitudes. El servicio LDR realiza la mayor parte del trabajo duro del sistema StorageGRID al manejar cargas de transferencia de datos y funciones de tráfico de datos.

El servicio LDR se encarga de las siguientes tareas:

- Consultas
- Actividad de gestión de la vida útil de la información (ILM)
- Eliminación de objetos
- Almacenamiento de datos de objetos
- Transferencias de datos de objetos desde otro servicio LDR (nodo de almacenamiento)
- Gestión del almacenamiento de datos
- Interfaces de protocolo (S3 y Swift)

El servicio LDR también gestiona la asignación de objetos S3 y Swift a los "'Content Hands' (UUID) únicos que el sistema StorageGRID asigna a cada objeto ingerido.

#### Consultas

Las consultas de LDR incluyen consultas de ubicación de objetos durante las operaciones de recuperación y archivado. Puede identificar el tiempo medio que tarda en ejecutar una consulta, el número total de consultas correctas y el número total de consultas que han fallado debido a un problema de tiempo de espera.

Puede revisar la información de consulta para supervisar el estado del almacén de metadatos, lo que afecta al rendimiento de procesamiento y recuperación del sistema. Por ejemplo, si la latencia de una consulta media es lenta y el número de consultas con errores debido a tiempos de espera es elevado, es posible que el almacén de metadatos encuentre una carga mayor o realice otra operación.

También puede ver el número total de consultas que han fallado debido a los fallos de consistencia. Los fallos de nivel de consistencia se deben a un número insuficiente de almacenes de metadatos disponibles en el momento en que se realiza una consulta a través del servicio LDR específico.

Puede utilizar la página Diagnósticos para obtener información adicional sobre el estado actual de la cuadrícula. Consulte Ejecutar diagnóstico.

#### Actividad de ILM

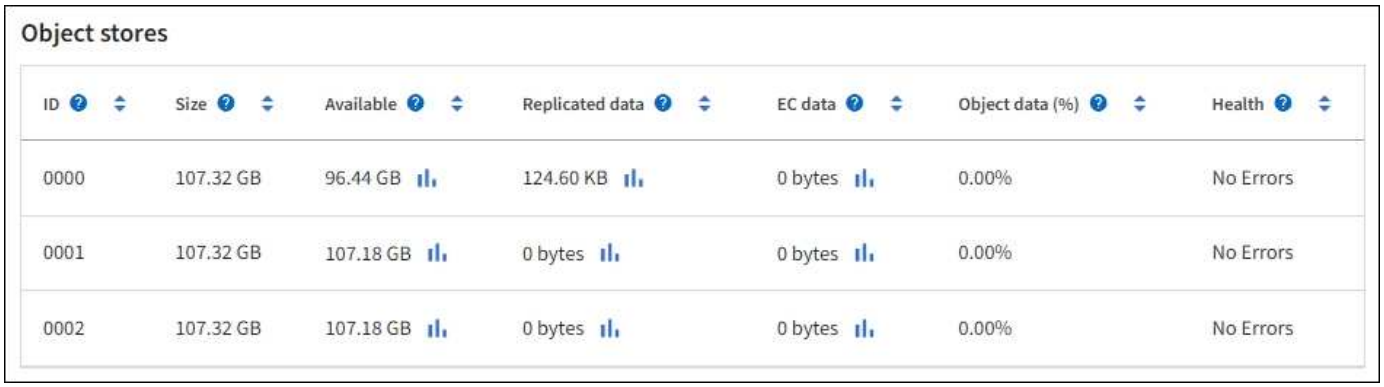
Las métricas de gestión de ciclo de vida de la información (ILM) permiten supervisar la velocidad a la que se evalúan los objetos para la implementación de ILM. Puede ver estas métricas en el Panel o en **NODES** > ***Storage Node*** > **ILM**.

#### Almacenes de objetos

El almacenamiento de datos subyacente de un servicio LDR se divide en un número fijo de almacenes de objetos (también conocidos como volúmenes de almacenamiento). Cada almacén de objetos es un punto de

montaje independiente.

Puede ver los almacenes de objetos de un nodo de almacenamiento en la página nodos > pestaña Storage.



Object stores

| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

Los almacenes de objetos de un nodo de almacenamiento se identifican mediante un número hexadecimal entre 0000 y 002F, que se conoce como el ID del volumen. El espacio se reserva en el primer almacén de objetos (volumen 0) para los metadatos de objetos en una base de datos de Cassandra; todo el espacio restante en ese volumen se usa para los datos de objetos. El resto de almacenes de objetos se utilizan exclusivamente para datos de objetos, lo que incluye copias replicadas y fragmentos codificados para borrado.

Para garantizar hasta el uso de espacio para las copias replicadas, los datos de objetos para un objeto determinado se almacenan en un almacén de objetos en función del espacio de almacenamiento disponible. Cuando uno o varios almacenes de objetos se llenan de capacidad, los almacenes de objetos restantes siguen almacenando objetos hasta que no hay más espacio en el nodo de almacenamiento.

#### Protección de metadatos

Los metadatos de objetos son información relacionada con un objeto o una descripción de él; por ejemplo, el tiempo de modificación del objeto o la ubicación de almacenamiento. StorageGRID almacena metadatos de objetos en una base de datos de Cassandra, que se conecta con el servicio LDR.

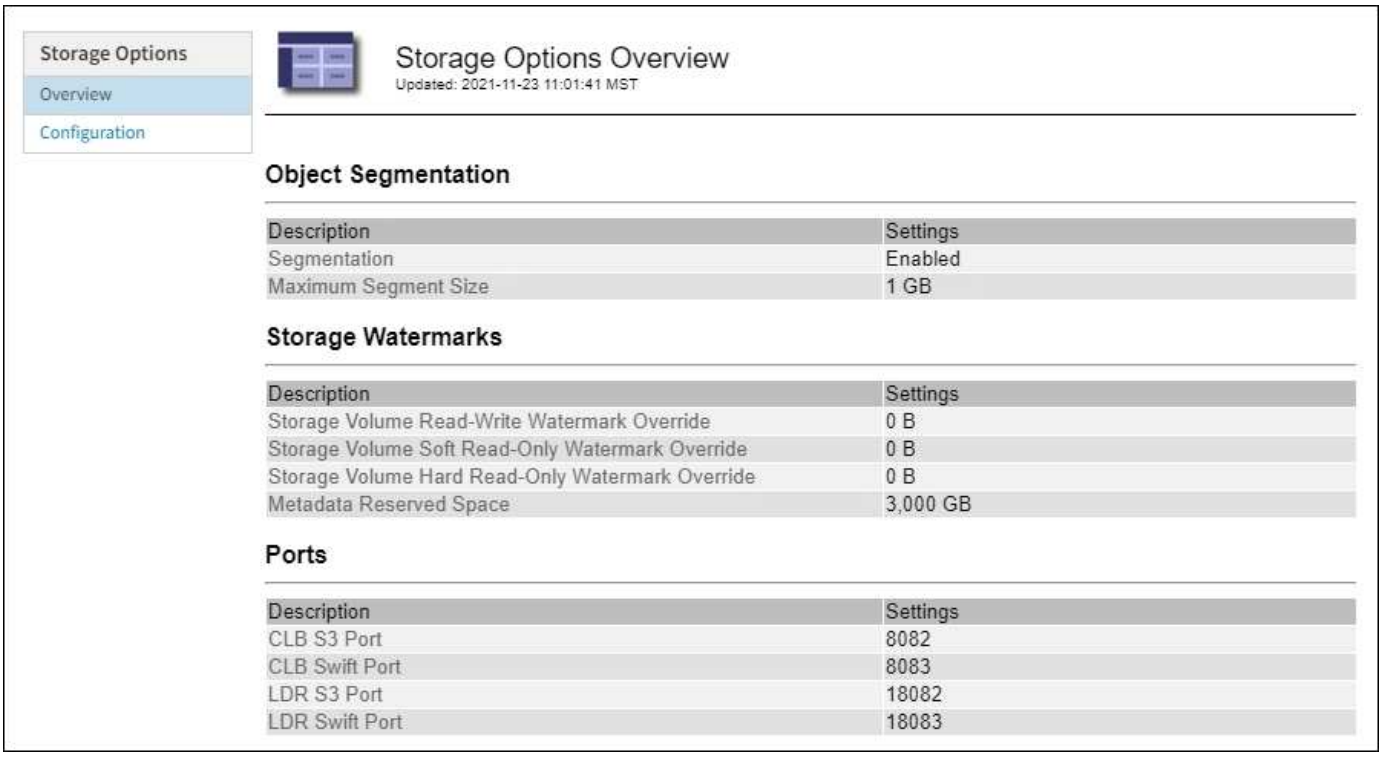
Para garantizar la redundancia y, por lo tanto, la protección contra la pérdida, se mantienen tres copias de metadatos de objetos en cada sitio. Las copias se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio. Esta replicación no puede configurarse y se realiza de forma automática.

Gestione el almacenamiento de metadatos de objetos

## Gestionar opciones de almacenamiento

Las opciones de almacenamiento incluyen la configuración de segmentación de objetos, los valores actuales para las marcas de agua del volumen de almacenamiento y la configuración de espacio reservado de metadatos. También es posible ver los puertos S3 y Swift que utiliza el servicio CLB obsoleto en los nodos de puerta de enlace y el servicio LDR en los nodos de almacenamiento.

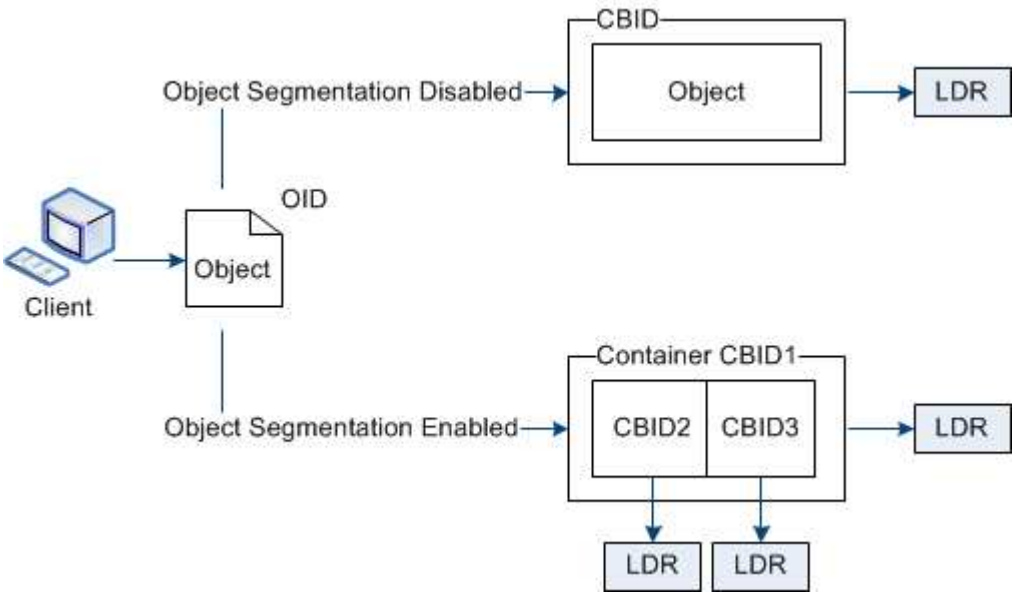
Para obtener información acerca de las asignaciones de puertos, consulte Resumen: Direcciones IP y puertos para conexiones cliente.




**¿Qué es la segmentación de objetos?**

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos de tamaño fijo más pequeños para optimizar el uso del almacenamiento y los recursos para objetos grandes. La carga de varias partes de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando un objeto se procesa en el sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que enumera la información de encabezado de todos los segmentos como contenido.




Al recuperar un contenedor de segmentos, el servicio LDR reúne el objeto original de sus segmentos y devuelve el objeto al cliente.

El contenedor y los segmentos no están almacenados necesariamente en el mismo nodo de almacenamiento. El contenedor y los segmentos pueden almacenarse en cualquier nodo de almacenamiento dentro del pool de almacenamiento especificado en la regla de ILM.

El sistema StorageGRID trata cada segmento de forma independiente y contribuye al recuento de atributos como objetos gestionados y objetos almacenados. Por ejemplo, si un objeto almacenado en el sistema StorageGRID se divide en dos segmentos, el valor de objetos gestionados aumenta en tres una vez completada la ingesta, de la siguiente manera:

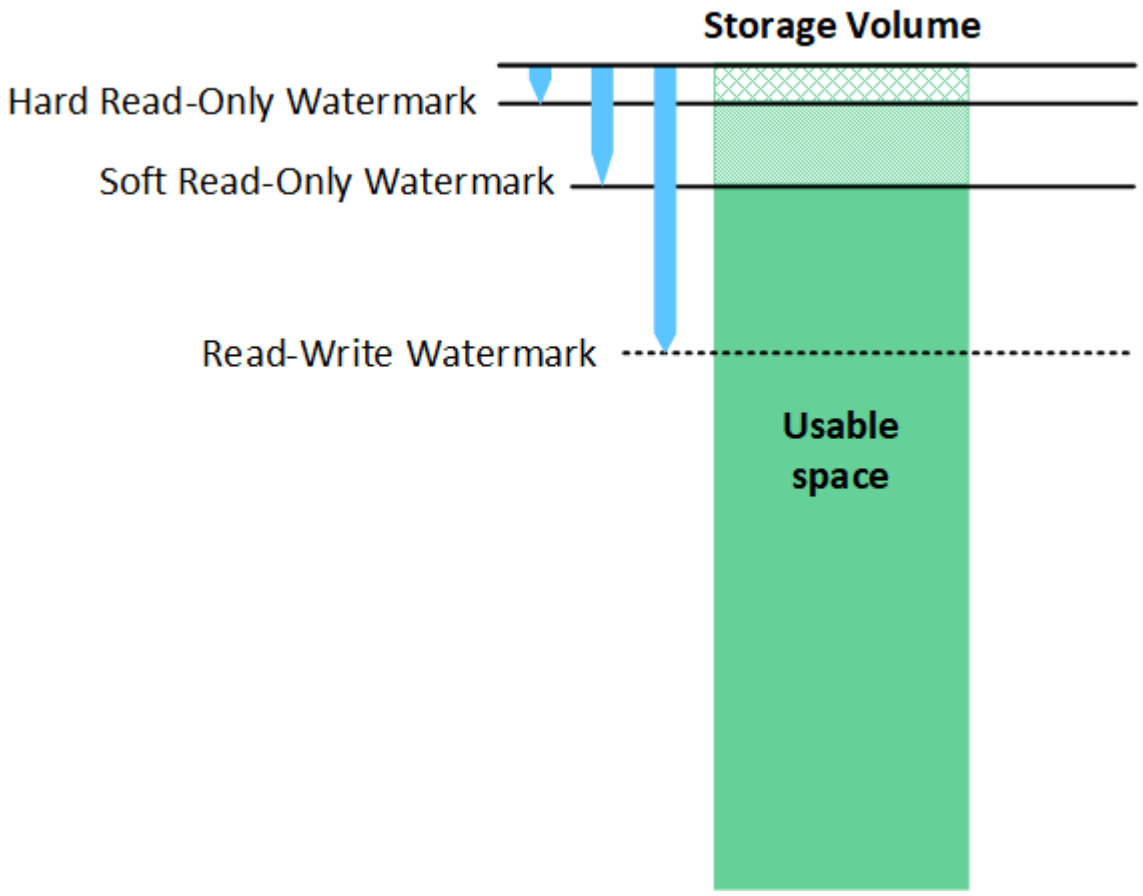
contenedor de segmentos + segmento 1 + segmento 2 = tres objetos almacenados

Puede mejorar el rendimiento al manejar objetos grandes asegurándose de que:

- Cada puerta de enlace y cada nodo de almacenamiento tiene suficiente ancho de banda de red para el rendimiento requerido. Por ejemplo, configure redes de cliente y de cuadrícula independientes en interfaces Ethernet de 10 Gbps.
- Se ponen en marcha suficientes nodos de pasarela y almacenamiento para el rendimiento requerido.
- Cada nodo de almacenamiento tiene suficiente rendimiento de I/o de disco para el rendimiento requerido.

**¿Qué son las marcas de agua del volumen de almacenamiento?**

StorageGRID usa tres marcas de agua de volúmenes de almacenamiento para garantizar que los nodos de almacenamiento pasan de forma segura a un estado de solo lectura antes de que se ejecuten con un espacio mínimo y para permitir que los nodos de almacenamiento que se hayan migrado al estado de solo lectura se vuelvan a escribir.



Las marcas de agua del volumen de almacenamiento solo se aplican al espacio utilizado para los datos de objetos replicados y codificados por borrado. Para obtener más información acerca del espacio reservado para los metadatos de objetos en el volumen 0, vaya a.Gestione el almacenamiento de metadatos de objetos.

#### ¿Qué es la Marca de agua blanda de sólo lectura?

**Marca de agua de sólo lectura suave del volumen de almacenamiento** es la primera Marca de agua que indica que el espacio utilizable de un nodo de almacenamiento para los datos del objeto se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que la Marca de agua de solo lectura suave de ese volumen, el nodo de almacenamiento pasará al *modo de solo lectura*. El modo de solo lectura significa que el nodo de almacenamiento anuncia servicios de solo lectura al resto del sistema StorageGRID, pero completa todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una Marca de agua blanda de solo lectura de 10 GB. En cuanto cada volumen tiene menos de 10 GB de espacio libre, el nodo de almacenamiento pasa al modo de solo lectura suave.

#### ¿Qué es la Marca de agua dura de sólo lectura?

- Marca de agua de sólo lectura dura de volumen de almacenamiento* es la siguiente Marca de agua para indicar que el espacio utilizable de un nodo para los datos de objeto se está llenando.

Si el espacio libre en un volumen es menor que la Marca de agua de sólo lectura de ese volumen, las escrituras en el volumen fallarán. Sin embargo, las escrituras en otros volúmenes pueden continuar hasta que el espacio libre en esos volúmenes sea menor que sus marcas de agua de sólo lectura.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una Marca de agua de solo lectura rígida de 5 GB. En cuanto cada volumen tenga menos de 5 GB de espacio libre, el nodo de almacenamiento ya no aceptará ninguna solicitud de escritura.

La Marca de agua dura de sólo lectura es siempre inferior a la Marca de agua blanda de sólo lectura.

#### ¿Qué es la Marca de agua de lectura y escritura?

**Marca de agua de lectura y escritura de volumen de almacenamiento** sólo se aplica a los nodos de almacenamiento que hayan pasado al modo de sólo lectura. Determina cuándo el nodo puede volver a ser de lectura y escritura. Cuando el espacio libre de un volumen de almacenamiento en un nodo de almacenamiento es mayor que la Marca de agua de lectura y escritura de ese volumen, el nodo cambia automáticamente al estado de lectura y escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Supongamos también que cada volumen tiene una Marca de agua de lectura y escritura de 30 GB. En cuanto el espacio libre de cualquier volumen aumente a 30 GB, el nodo volverá a ser de lectura y escritura.

La Marca de agua de lectura y escritura es siempre mayor que la Marca de agua de sólo lectura suave y la Marca de agua de sólo lectura dura.

#### Ver marcas de agua de volumen de almacenamiento

Puede ver los ajustes de Marca de agua actuales y los valores optimizados para el sistema. Si no se utilizan marcas de agua optimizadas, puede determinar si puede o debe ajustar los ajustes.

**Lo que necesitará**

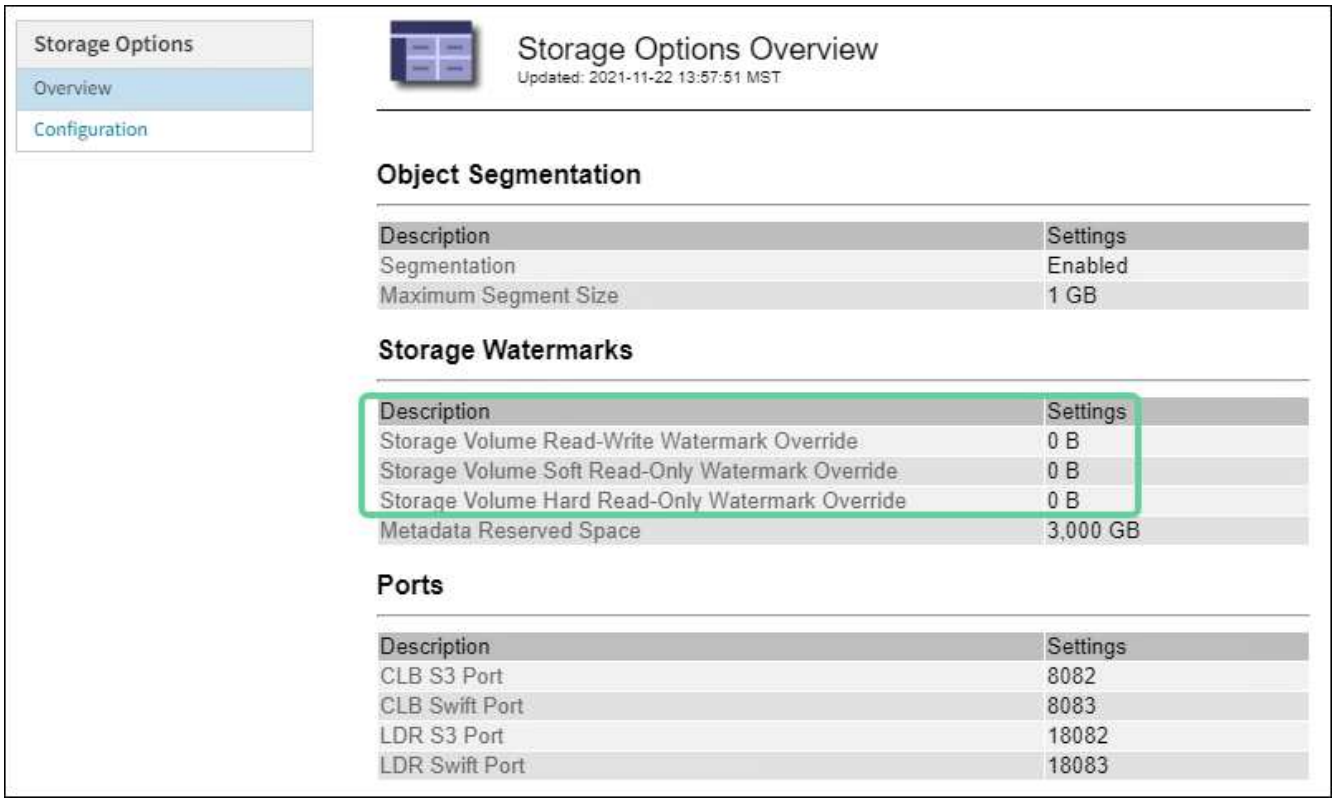
- Ha completado la actualización a StorageGRID 11.6.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

### Ver la configuración actual de la Marca de agua

Puede ver la configuración actual de la Marca de agua de almacenamiento en el Administrador de grid.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. En la sección Marcas de agua de almacenamiento, observe los ajustes para las tres anulaciones de la Marca de agua de volumen de almacenamiento.




   - Si las anulaciones de la Marca de agua son **0**, las tres marcas de agua están optimizadas para cada volumen de almacenamiento en cada nodo de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

     Esta es la configuración predeterminada y recomendada. No debe actualizar estos valores. Según sea necesario, puede opcionalmente Vea las marcas de agua de almacenamiento optimizadas.

   - Si las anulaciones de la Marca de agua son valores distintos de 0, se utilizan marcas de agua personalizadas (no optimizadas). No se recomienda utilizar la configuración de Marca de agua personalizada. Utilice las instrucciones para Solución de problemas de alertas de anulación de Marca de agua de sólo lectura baja para determinar si puede o debe ajustar la configuración.

### Vea las marcas de agua de almacenamiento optimizadas

StorageGRID utiliza dos métricas Prometheus para mostrar los valores optimizados que ha calculado para la Marca de agua * de sólo lectura suave de volumen de almacenamiento*. Puede ver los valores mínimos y

máximos optimizados para cada nodo de almacenamiento en la cuadrícula.

1. Seleccione **SUPPORT** > **Tools** > **Metrics**.
2. En la sección Prometheus, seleccione el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor optimizado mínimo de la Marca de agua de solo lectura suave para todos los volúmenes de almacenamiento de cada nodo de almacenamiento. Si este valor es mayor que el valor personalizado para **Marca de agua blanda de sólo lectura de volumen de almacenamiento**, se activa la alerta **anulación de Marca de agua de sólo lectura baja** para el nodo de almacenamiento.

4. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor optimizado máximo de la Marca de agua de solo lectura suave para todos los volúmenes de almacenamiento de cada nodo de almacenamiento.

## Gestione el almacenamiento de metadatos de objetos

La capacidad de metadatos de objetos de un sistema StorageGRID controla la cantidad máxima de objetos que se pueden almacenar en ese sistema. Para garantizar que el sistema StorageGRID tenga espacio suficiente para almacenar objetos nuevos, debe comprender dónde y cómo StorageGRID almacena los metadatos de objetos.

### ¿Qué son los metadatos de objetos?

Los metadatos de objetos son cualquier información que describa un objeto. StorageGRID utiliza metadatos de objetos para realizar un seguimiento de las ubicaciones de todos los objetos en el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

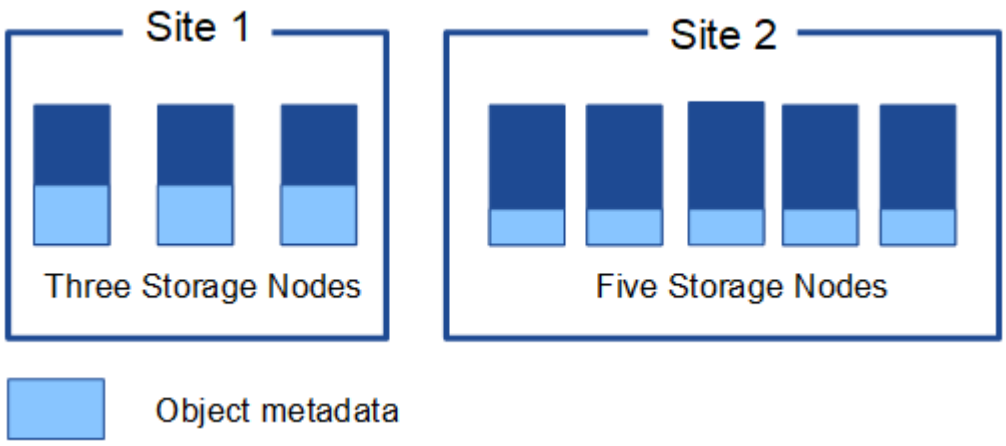
Para un objeto en StorageGRID, los metadatos de objeto incluyen los siguientes tipos de información:

- Metadatos del sistema, incluidos un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bloque de S3 o el contenedor Swift, el nombre o el ID de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y hora en que se modificó por última vez el objeto.
- Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
- Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
- Para objetos segmentados y objetos multipartes, identificadores de segmentos y tamaños de datos.

### ¿Cómo se almacenan los metadatos de objetos?

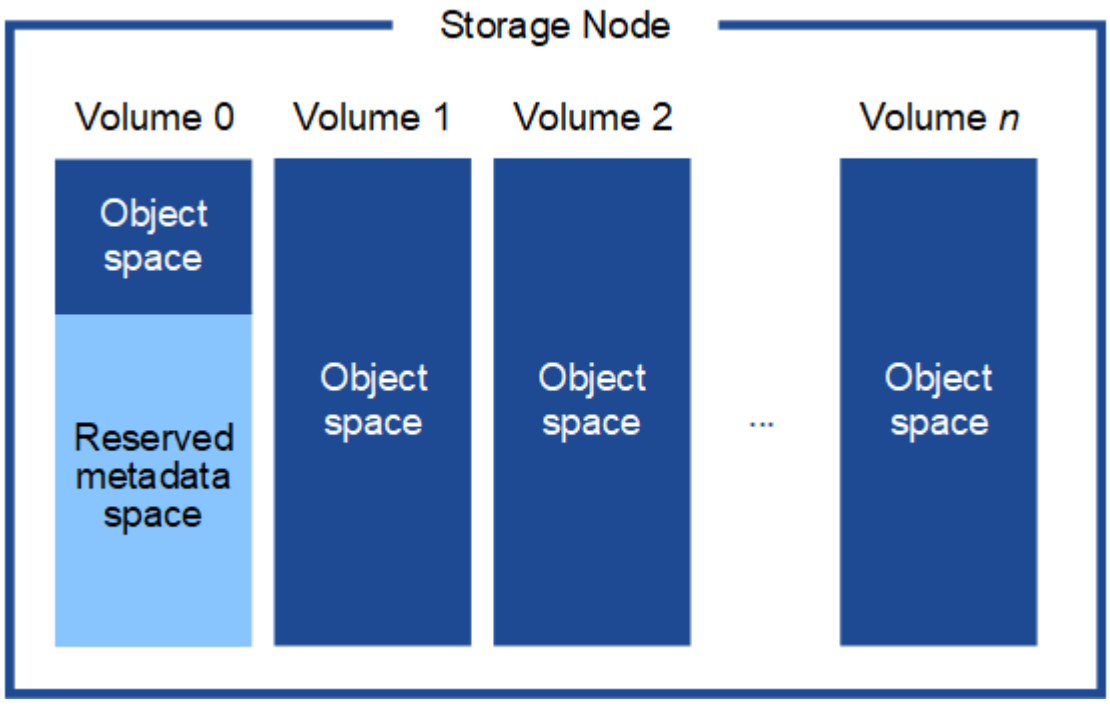
StorageGRID mantiene los metadatos de objetos en una base de datos de Cassandra, que se almacena independientemente de los datos de objetos. Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio.

Esta figura representa los nodos de almacenamiento de dos sitios. Cada sitio tiene la misma cantidad de metadatos de objetos, que está igualmente distribuido entre los nodos de almacenamiento de ese sitio.




### ¿Dónde se almacenan los metadatos de objetos?

En esta figura, se representan los volúmenes de almacenamiento para un único nodo de almacenamiento.




Como se muestra en la figura, StorageGRID reserva espacio para los metadatos del objeto en el volumen de almacenamiento 0 de cada nodo de almacenamiento. Utiliza el espacio reservado para almacenar metadatos de objetos y realizar operaciones esenciales de la base de datos. Cualquier espacio restante en el volumen de almacenamiento 0 y todos los demás volúmenes de almacenamiento del nodo de almacenamiento se utilizan

exclusivamente para los datos de objetos (copias replicadas y fragmentos codificados de borrado).

La cantidad de espacio que se reserva para metadatos de objetos en un nodo de almacenamiento determinado depende de varios factores, que se describen a continuación.

### Configuración de espacio reservado de metadatos

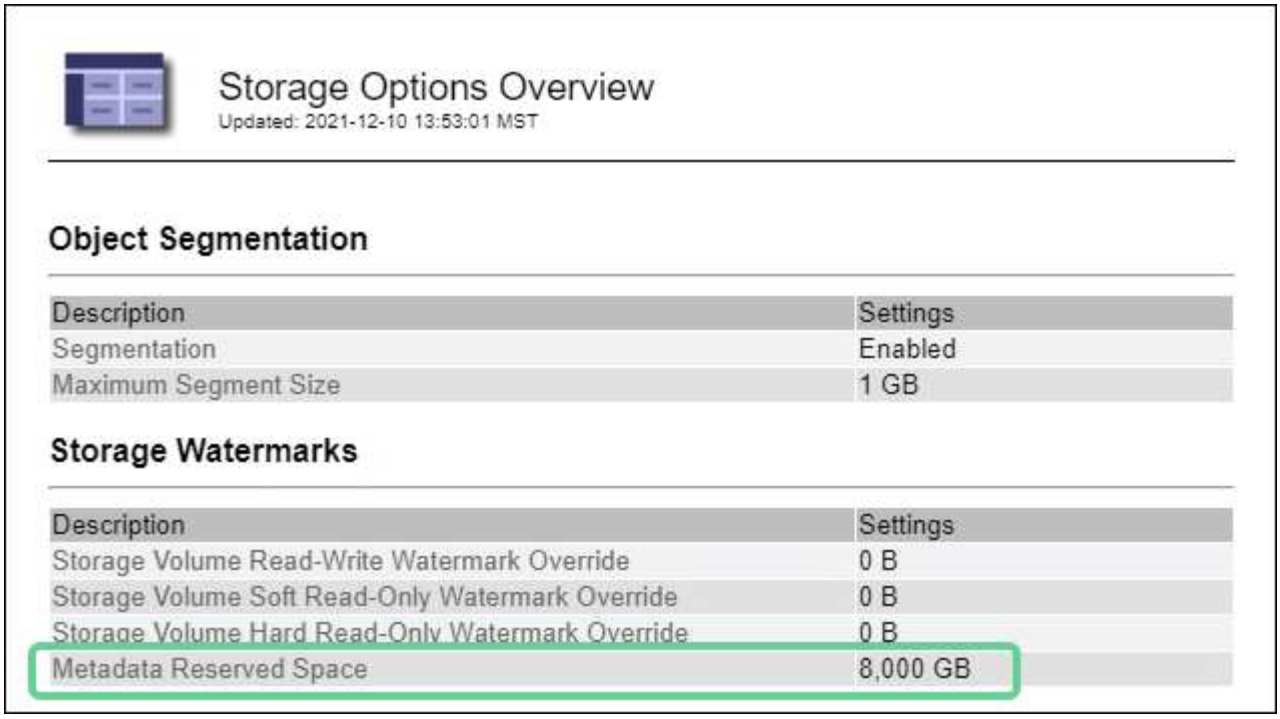
El *Metadata Reserved Space* es una configuración para todo el sistema que representa la cantidad de espacio que se reservará para metadatos en el volumen 0 de cada nodo de almacenamiento. Tal como se muestra en la tabla, el valor predeterminado de esta configuración para StorageGRID 11.6 se basa en lo siguiente:

- La versión de software que estaba utilizando cuando instaló inicialmente StorageGRID.
- La cantidad de RAM en cada nodo de almacenamiento.

| Versión utilizada para la instalación inicial de StorageGRID | Cantidad de RAM en los nodos de almacenamiento | Configuración de espacio reservado de metadatos predeterminado para StorageGRID 11.6 |
|---|---|---|
| 11.5/11.6 | 128 GB o más en cada nodo de almacenamiento del grid | 8 TB (8,000 GB) |
| | Debe haber menos de 128 GB en cualquier nodo de almacenamiento del grid | 3 TB (3,000 GB) |
| 11.1 a 11.4 | 128 GB o más en cada nodo de almacenamiento en un sitio | 4 TB (4,000 GB) |
| | Menos de 128 GB en cualquier nodo de almacenamiento de cada sitio | 3 TB (3,000 GB) |
| 11.0 o anterior | Cualquier cantidad | 2 TB (2,000 GB) |

Para ver la configuración del espacio reservado de metadatos para el sistema StorageGRID:

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. En la tabla Marcas de agua de almacenamiento, busque **espacio reservado de metadatos**.




En la captura de pantalla, el valor **espacio reservado de metadatos** es 8,000 GB (8 TB). Esta es la configuración predeterminada para una nueva instalación de StorageGRID 11.6 en la que cada nodo de almacenamiento tiene 128 GB o más de RAM.

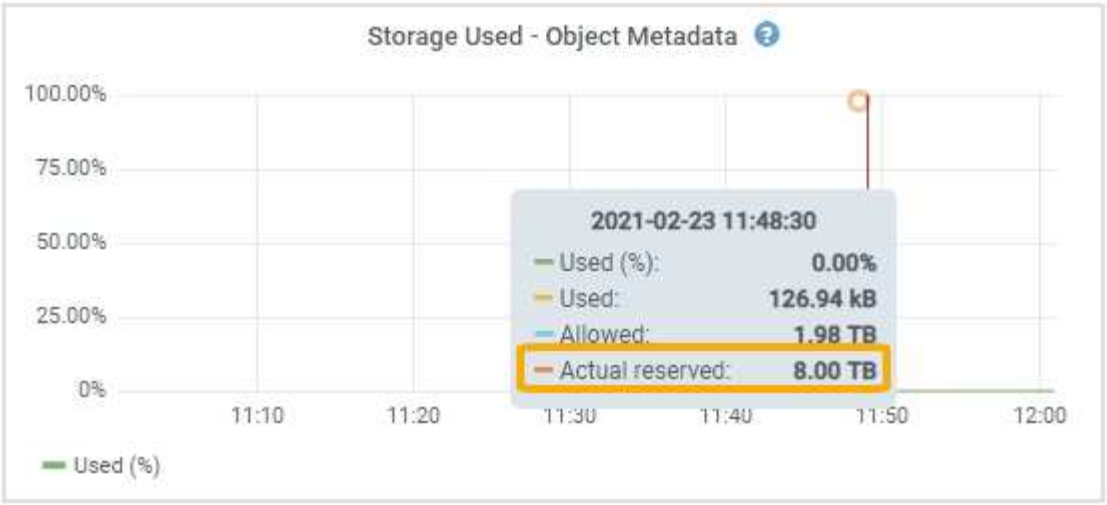
### Espacio reservado real para los metadatos

A diferencia de la configuración espacio reservado de metadatos para todo el sistema, se determina el *espacio reservado real* para los metadatos del objeto para cada nodo de almacenamiento. Para un nodo de almacenamiento determinado, el espacio reservado real para los metadatos depende del tamaño del volumen 0 para el nodo y de la configuración del espacio reservado de metadatos* para todo el sistema.

| El tamaño del volumen 0 para el nodo | Espacio reservado real para los metadatos |
|---|---|
| Menos de 500 GB (no uso en producción) | 10% del volumen 0 |
| 500 GB o más | El menor de estos valores:<br>• Volumen 0<br>• Configuración de espacio reservado de metadatos |

Para ver el espacio reservado real para los metadatos en un nodo de almacenamiento determinado:

1. En Grid Manager, seleccione **NODES** > ***Storage Node***.
2. Seleccione la ficha **almacenamiento**.
3. Pase el cursor sobre el gráfico almacenamiento utilizado — metadatos de objeto y localice el valor **reservado real**.




En la captura de pantalla, el valor **Real reservado** es 8 TB. Esta captura de pantalla es para un nodo de almacenamiento grande en una nueva instalación de StorageGRID 11.6. Debido a que la configuración de espacio reservado de metadatos para todo el sistema es menor que el volumen 0 para este nodo de almacenamiento, el espacio reservado real para este nodo es igual a la configuración de espacio reservado de metadatos.

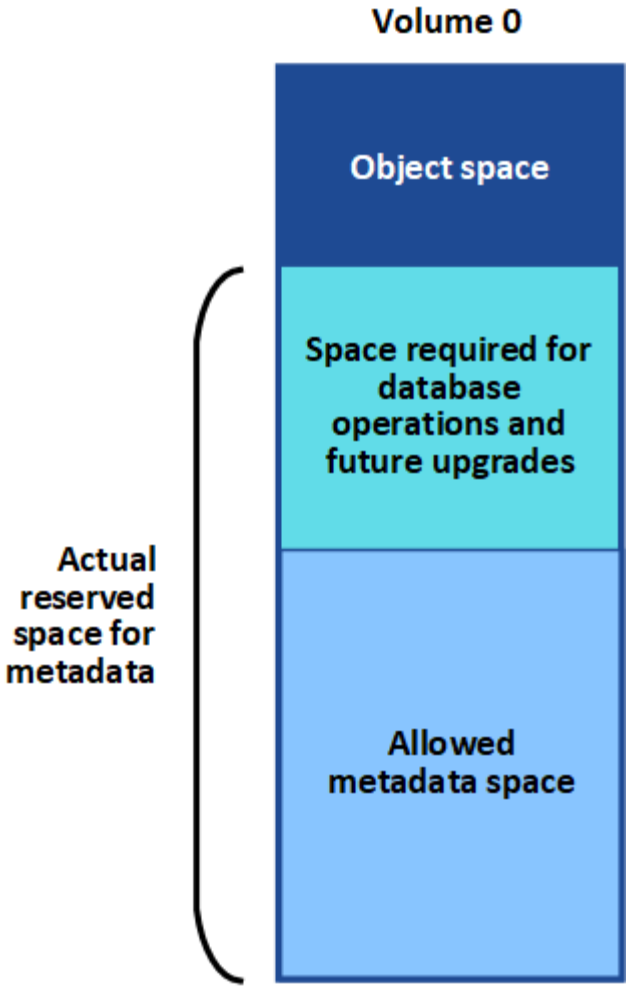
### Ejemplo de espacio de metadatos reservado real

Suponga que instala un nuevo sistema StorageGRID mediante la versión 11.6. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado de metadatos* para todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11.6 si cada nodo de almacenamiento tiene más de 128 GB de RAM.)
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (El volumen completo se reserva porque el volumen 0 es menor que la configuración **espacio reservado de metadatos**).

### Espacio de metadatos permitido

El espacio reservado real de cada nodo de almacenamiento para metadatos se subdivide en el espacio disponible para los metadatos del objeto (el *espacio de metadatos permitido*) y el espacio necesario para las operaciones esenciales de la base de datos (como compactación y reparación) y las futuras actualizaciones de hardware y software. El espacio de metadatos permitido rige la capacidad general del objeto.



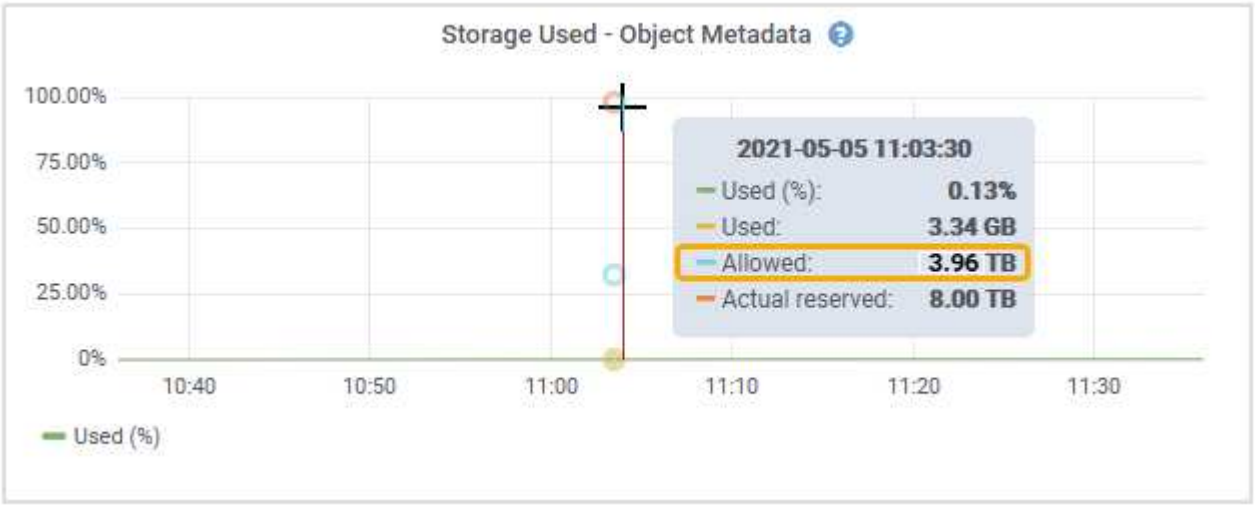

En la tabla siguiente se muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes nodos de almacenamiento, en función de la cantidad de memoria del nodo y del espacio reservado real para los metadatos.

| | | **Cantidad de memoria en el nodo de almacenamiento** | |
|---|---|---|---|
| | ≪ 128 GB | >= 128 GB | **Espacio reservado real para metadatos** |
| ≪= 4 TB | 60 % del espacio reservado real para metadatos, hasta un máximo de 1.32 TB | 60 % del espacio reservado real para metadatos, hasta un máximo de 1.98 TB | > 4 TB |

Para ver el espacio de metadatos permitido para un nodo de almacenamiento:

1. En Grid Manager, seleccione **NODES**.
2. Seleccione el nodo de almacenamiento.

3. Seleccione la ficha **almacenamiento**.
4. Coloque el cursor sobre el gráfico almacenamiento usado — metadatos de objeto y busque el valor **permitido**.




En la captura de pantalla, el valor **permitido** es 3.96 TB, que es el valor máximo para un nodo de almacenamiento cuyo espacio reservado real para metadatos es superior a 4 TB.

El valor **permitido** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

#### Ejemplo de espacio de metadatos permitido

Supongamos que instala un sistema StorageGRID mediante la versión 11.6. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado de metadatos* para todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para StorageGRID 11.6 cuando cada nodo de almacenamiento tiene más de 128 GB de RAM.)
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (El volumen completo se reserva porque el volumen 0 es menor que la configuración **espacio reservado de metadatos**).
- El espacio permitido para los metadatos en SN1 es de 3 TB, según el cálculo mostrado en la tabla para el espacio permitido para los metadatos: (Espacio reservado real para metadatos − 1 TB) × 60%, hasta un máximo de 3.96 TB.

#### Cómo afectan los nodos de almacenamiento de diferentes tamaños a la capacidad de objetos

Como se ha descrito anteriormente, StorageGRID distribuye uniformemente los metadatos de objetos de los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

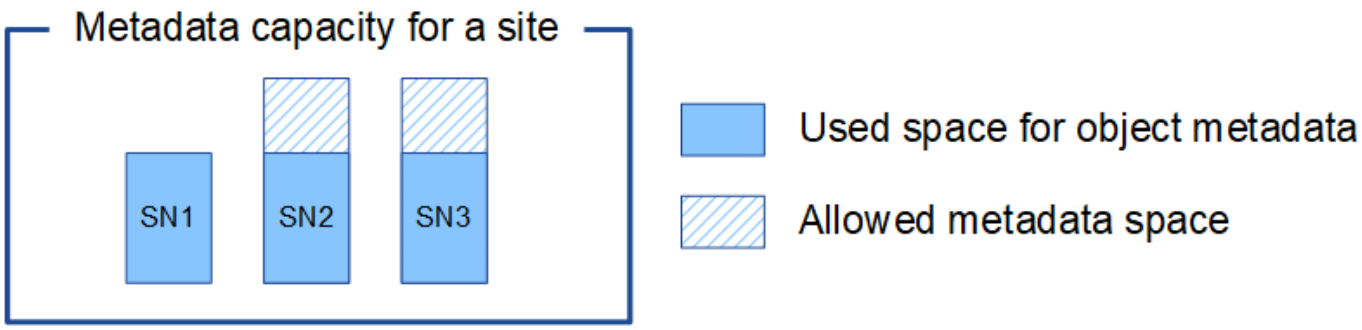
Observe el siguiente ejemplo:

- Hay una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de distintos tamaños.

- El ajuste **espacio reservado de metadatos** es de 4 TB.
- Los nodos de almacenamiento tienen los siguientes valores para el espacio de metadatos reservado real y el espacio de metadatos permitido.

| Nodo de almacenamiento | Tamaño del volumen 0 | Espacio real de metadatos reservado | Espacio de metadatos permitido |
|---|---|---|---|
| SN1 | 2.2 TB | 2.2 TB | 1.32 TB |
| SN2 | 5 TB | 4 TB | 1.98 TB |
| SN3 | 6 TB | 4 TB | 1.98 TB |

Como los metadatos de objetos se distribuyen uniformemente por los nodos de almacenamiento de un sitio, cada nodo de este ejemplo solo puede contener 1.32 TB de metadatos. No se pueden utilizar los 0.66 TB adicionales de espacio de metadatos permitidos para SN2 y SN3.




De igual modo, como StorageGRID mantiene todos los metadatos de objetos para un sistema StorageGRID en cada sitio, la capacidad general de metadatos de un sistema StorageGRID viene determinada por la capacidad de metadatos de objetos del sitio más pequeño.

Además, dado que la capacidad de metadatos de los objetos controla el recuento máximo de objetos, cuando un nodo se queda sin capacidad de metadatos, el grid está lleno de eficacia.

**Información relacionada**

- Para saber cómo supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento, vaya a. Supervisión y solución de problemas.
- Para aumentar la capacidad de metadatos de los objetos del sistema, añada nuevos nodos de almacenamiento. Vaya a. Amplíe su grid.

## Configurar la configuración global de los objetos almacenados

### Configurar la compresión de objetos almacenados

Puede utilizar la opción de cuadrícula comprimir objetos almacenados para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que los objetos consuman menos espacio de almacenamiento.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

La opción de cuadrícula Compress Stored Objects está desactivada de forma predeterminada. Si habilita esta opción, StorageGRID intenta comprimir cada objeto al guardarlo utilizando una compresión sin pérdidas.

> Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

Antes de habilitar esta opción, tenga en cuenta lo siguiente:

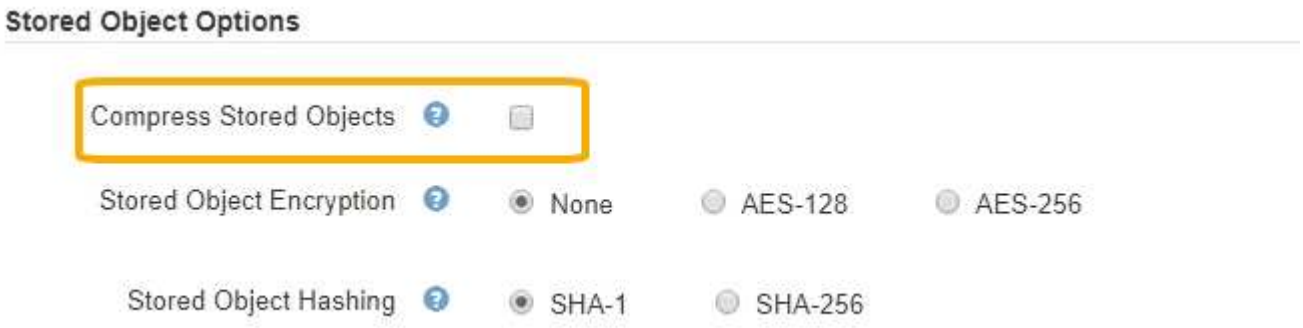
- No debe activar la compresión a menos que sepa que los datos almacenados son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimir objetos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, la activación de comprimir objetos almacenados no reducirá aún más el tamaño de un objeto.
- No active la compresión si utiliza FabricPool de NetApp con StorageGRID.
- Si la opción de cuadrícula Compress Stored Objects está habilitada, las aplicaciones cliente S3 y Swift deberían evitar realizar operaciones GET Object que especifiquen un intervalo de bytes que se devolverán. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos para acceder a los bytes solicitados. LAS operaciones GET Object que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

  Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

  > Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado , active la casilla de verificación **comprimir objetos almacenados** .




3. Seleccione **Guardar**.

### Configurar el cifrado de objetos almacenados

Puede cifrar objetos almacenados si desea garantizar que los datos no se puedan recuperar de forma legible si un almacén de objetos está comprometido. De forma predeterminada, los objetos no se cifran.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

#### Acerca de esta tarea

El cifrado de objetos almacenados permite el cifrado de todos los datos de objetos cuando se ingieren mediante S3 o Swift. Cuando se activa la configuración, todos los objetos recién ingeridos se cifran pero no se realiza ningún cambio en los objetos almacenados existentes. Si deshabilita el cifrado, los objetos cifrados actualmente permanecen cifrados pero los objetos recién ingeridos no se cifran.

> Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

Los objetos almacenados se pueden cifrar utilizando el algoritmo de cifrado AES-128 o AES-256.

La configuración de cifrado de objetos almacenados se aplica solo a objetos S3 que no se hayan cifrado mediante cifrado a nivel de bloque u objeto.

#### Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado, cambie el cifrado de objetos almacenados a **Ninguno** (predeterminado), **AES-128** o **AES-256**.

3. Seleccione **Guardar**.

### Configurar los hash de objetos almacenados

La opción de hash de objetos almacenados especifica el algoritmo de hash utilizado para verificar la integridad del objeto.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

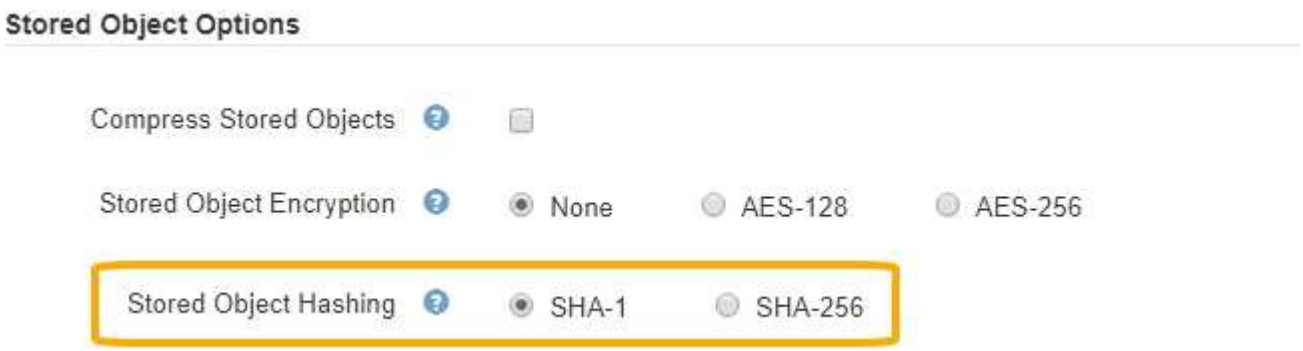
**Acerca de esta tarea**

De forma predeterminada, los datos de objeto se procesan mediante el algoritmo SHA-1. El algoritmo SHA-256 requiere recursos de CPU adicionales y generalmente no se recomienda para la verificación de integridad.

> Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado, cambie el hash de objetos almacenados a **SHA-1** (predeterminado) o **SHA-256**.




3. Seleccione **Guardar**.

## Opciones de configuración del nodo de almacenamiento

Cada nodo de almacenamiento utiliza una serie de opciones de configuración y contadores. Puede que necesite ver los ajustes actuales o restablecer contadores para borrar alarmas (sistema heredado).

> Excepto cuando se le indique específicamente en la documentación, debe consultar con el soporte técnico antes de modificar los ajustes de configuración de nodos de almacenamiento. Según sea necesario, puede restablecer los contadores de eventos para borrar las alarmas heredadas.

Para acceder a las opciones de configuración y los contadores de un nodo de almacenamiento:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node***.
3. Expanda el nodo de almacenamiento y seleccione el servicio o el componente.
4. Seleccione la ficha **Configuración**.

Las siguientes tablas resumen los ajustes de configuración de nodos de almacenamiento.

**LDR**

| Nombre de atributo | Codificación | Descripción |
| --- | --- | --- |
| Estado HTTP | HSTE | El estado actual del protocolo HTTP para S3, Swift y otro tráfico interno de StorageGRID:<br>• Sin conexión: No se permiten operaciones y cualquier aplicación cliente que intente abrir una sesión HTTP al servicio LDR recibe un mensaje de error. Las sesiones activas se cierran correctamente.<br>• En línea: El funcionamiento continúa con normalidad |
| HTTP de inicio automático | HTA | • Si se selecciona, el estado del sistema al reiniciar depende del estado del componente **LDR** > **almacenamiento**. Si el componente **LDR** > **almacenamiento** es de sólo lectura al reiniciar, la interfaz HTTP también es de sólo lectura. Si el componente **LDR** > **almacenamiento** está en línea, HTTP también está en línea. De lo contrario, la interfaz HTTP permanece en estado sin conexión.<br>• Si no se selecciona, la interfaz HTTP permanece sin conexión hasta que se habilita explícitamente. |

**LDR > almacén de datos**

| Nombre de atributo | Codificación | Descripción |
| --- | --- | --- |
| Restablecer recuento de objetos perdidos | RCOR | Restablezca el contador del número de objetos perdidos en este servicio. |

**LDR > almacenamiento**

| Nombre de atributo | Codificación | Descripción |
| --- | --- | --- |
| Estado de almacenamiento — deseado | SSD | Una configuración que puede configurar el usuario para el estado deseado del componente de almacenamiento. El servicio LDR lee este valor e intenta hacer coincidir el estado indicado por este atributo. El valor se mantiene de un reinicio a otro.<br><br>Por ejemplo, puede usar esta configuración para forzar a que el almacenamiento pase a ser de solo lectura, incluso si hay un gran espacio de almacenamiento disponible. Esto puede ser útil para la solución de problemas.<br><br>El atributo puede tomar uno de los siguientes valores:<br><br>• Sin conexión: Cuando el estado deseado es sin conexión, el servicio LDR desconecta el componente **LDR** > **almacenamiento**.<br>• Solo lectura: Cuando el estado deseado es de solo lectura, el servicio LDR mueve el estado de almacenamiento a sólo lectura y deja de aceptar contenido nuevo. Tenga en cuenta que el contenido puede seguir guardado en el nodo de almacenamiento durante un breve periodo hasta que se cierran las sesiones abiertas.<br>• En línea: Deje el valor en línea durante el funcionamiento normal del sistema. Estado del almacenamiento: El servicio establecerá de forma dinámica la corriente del componente de almacenamiento en función del estado del servicio LDR, como la cantidad de espacio de almacenamiento de objetos disponible. Si el espacio es bajo, el componente se convierte en de solo lectura. |
| Tiempo de espera de comprobación del estado | HCT | El límite de tiempo en segundos en el que debe completarse una prueba de comprobación del estado para que un volumen de almacenamiento se considere correcto. Cambie este valor solo cuando lo indique el equipo de soporte de. |

**LDR > verificación**

| Nombre de atributo | Codificación | Descripción |
| --- | --- | --- |
| Restablecer recuento de objetos que faltan | VCMI | Restablece el recuento de objetos que faltan detectados (OMIS). Utilice sólo una vez completada la comprobación de la existencia del objeto. El sistema StorageGRID restaura automáticamente los datos de objetos replicados que faltan. |

| Nombre de atributo | Codificación | Descripción |
|---|---|---|
| Tasa de verificación | VPRI | Establecer la velocidad a la que se realiza la verificación en segundo plano. Consulte la información sobre cómo configurar la tasa de verificación en segundo plano. |
| Restablecer recuento de objetos dañados | VCCR | Restablece el contador para los datos de objetos replicados dañados que se han encontrado durante la verificación en segundo plano. Esta opción se puede utilizar para borrar la condición de alarma objetos dañados detectados (OCOR). Para obtener más detalles, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID. |
| Eliminar objetos en cuarentena | OQRT | Eliminar objetos dañados del directorio de cuarentena, restablecer el recuento de objetos en cuarentena a cero y borrar la alarma objetos en cuarentena detectados (OQRT). Esta opción se utiliza después de que el sistema StorageGRID restaura automáticamente los objetos dañados.<br><br>Si se activa una alarma objetos perdidos, es posible que el soporte técnico desee acceder a los objetos en cuarentena. En algunos casos, los objetos en cuarentena podrían ser útiles para la recuperación de datos o para depurar los problemas subyacentes que causaron las copias de objetos dañadas. |

**LDR > codificación de borrado**

| Nombre de atributo | Codificación | Descripción |
|---|---|---|
| Restablecer el número de errores de escritura | RSWF | Restablezca el contador para obtener errores de escritura de los datos de objetos codificados con borrado al nodo de almacenamiento. |
| Recuento de errores de restablecimiento de lecturas | RSRF | Restablezca el contador para ver los errores de lectura de los datos de objetos codificados con borrado desde el nodo de almacenamiento. |
| Restablecer recuento de errores de eliminación | RSDF | Restablezca el contador para eliminar errores de datos de objetos codificados con borrado desde el nodo de almacenamiento. |
| Restablecer el número de copias dañadas detectadas | RSCC | Restablezca el contador del número de copias dañadas de datos de objetos codificados con borrado en el nodo de almacenamiento. |

| Nombre de atributo | Codificación | Descripción |
|---|---|---|
| Restablecer recuento de fragmentos dañados detectados | RSCD | Restablezca el contador para fragmentos dañados de datos de objetos codificados con borrado en el nodo de almacenamiento. |
| Restablecer recuento de fragmentos perdidos detectados | RSMD | Restablezca el contador para ver los fragmentos faltantes de datos de objetos codificados con borrado en el nodo de almacenamiento. Utilice sólo una vez completada la comprobación de la existencia del objeto. |

**LDR > replicación**

| Nombre de atributo | Codificación | Descripción |
|---|---|---|
| Restablecer recuento de fallos de replicación entrante | RICR | Restablezca el contador de fallos de replicación de entrada. Esto se puede utilizar para borrar la alarma RIRF (replicación entrante — fallida). |
| Restablecer recuento de fallos de replicación de salida | RCR | Restablezca el contador para fallos de replicación saliente. Esto se puede utilizar para borrar la alarma RORF (réplicas de salida — fallida). |
| Desactivar la replicación entrante | DSIR | Seleccione esta opción para desactivar la replicación entrante como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal.<br><br>Cuando la replicación entrante está deshabilitada, los objetos se pueden recuperar del nodo de almacenamiento para copiar en otras ubicaciones del sistema StorageGRID, pero los objetos no se pueden copiar en este nodo de almacenamiento desde otras ubicaciones: El servicio LDR es de sólo lectura. |
| Desactive la replicación saliente | DSOR | Seleccione esta opción para deshabilitar la replicación saliente (incluidas las solicitudes de contenido para las recuperaciones HTTP) como parte de un procedimiento de mantenimiento o de prueba. Deje sin marcar durante el funcionamiento normal.<br><br>Cuando la replicación saliente está deshabilitada, los objetos se pueden copiar a este nodo de almacenamiento, pero no es posible recuperar objetos del nodo de almacenamiento que se van a copiar en otras ubicaciones del sistema StorageGRID. El servicio LDR es de sólo escritura. |

**Información relacionada**

Supervisión y solución de problemas

## Gestione nodos de almacenamiento completos

A medida que los nodos de almacenamiento alcancen la capacidad, debe ampliar el sistema StorageGRID añadiendo almacenamiento nuevo. Hay tres opciones disponibles: Añadir volúmenes de almacenamiento, añadir bandejas de ampliación de almacenamiento y añadir nodos de almacenamiento.

### Añadir volúmenes de almacenamiento

Cada nodo de almacenamiento es compatible con un número máximo de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento contiene menos de la cantidad máxima de volúmenes de almacenamiento, es posible añadir volúmenes para aumentar su capacidad. Consulte las instrucciones para Expandir un sistema StorageGRID.

### Añada bandejas de ampliación del almacenamiento

Algunos nodos de almacenamiento de dispositivos StorageGRID, como el SG6060, pueden admitir bandejas de almacenamiento adicionales. Si tiene dispositivos StorageGRID con funcionalidades de expansión que todavía no se han expandido hasta la máxima capacidad, se pueden añadir bandejas de almacenamiento para aumentar la capacidad. Consulte las instrucciones para Expandir un sistema StorageGRID.

### Añada nodos de almacenamiento

Puede aumentar la capacidad de almacenamiento con la adición de nodos de almacenamiento. Al añadir almacenamiento, deben tenerse en cuenta las reglas de ILM activas y los requisitos de capacidad. Consulte las instrucciones para Expandir un sistema StorageGRID.

# Gestione los nodos de administrador

## Qué es un nodo de administrador

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Cada grid debe tener un nodo de administrador primario y puede tener cualquier cantidad de nodos de administrador no primarios por motivos de redundancia.

Cuando inicia sesión en el administrador de grid o en el administrador de inquilinos, se conecta a un nodo de administración. Puede conectarse a cualquier nodo de administrador y cada nodo de administrador muestra una vista similar del sistema StorageGRID. Sin embargo, se deben realizar los procedimientos de mantenimiento usando el nodo de administración principal.

Los nodos de administración también se pueden usar para equilibrar la carga del tráfico de clientes S3 y Swift.

Los nodos de administración alojan los siguientes servicios:

- Servicio AMS
- Servicio CMN
- Servicio NMS
- Servicio Prometheus
- Equilibrador de carga y servicios de alta disponibilidad (para admitir el tráfico de cliente S3 y Swift)

Los nodos de administración también admiten la interfaz de programa de aplicaciones de gestión (API de gestión) para procesar las solicitudes desde la API de gestión de grid y la API de gestión de inquilinos. Consulte Utilice la API de gestión de grid.

#### Qué es el servicio AMS

El servicio sistema de gestión de auditorías (AMS) realiza un seguimiento de la actividad y los eventos del sistema.

#### En qué consiste el servicio CMN

El servicio nodo de gestión de configuración (CMN) administra las configuraciones de todo el sistema de las características de conectividad y protocolo necesarias para todos los servicios. Además, el servicio CMN se utiliza para ejecutar y supervisar tareas de cuadrícula. Solo hay un servicio CMN por instalación de StorageGRID. El nodo de administración que aloja el servicio CMN se conoce como nodo de administración principal.

#### Qué es el servicio NMS

El servicio sistema de administración de red (NMS) activa las opciones de supervisión, generación de informes y configuración que se muestran a través de Grid Manager, la interfaz basada en explorador del sistema StorageGRID.

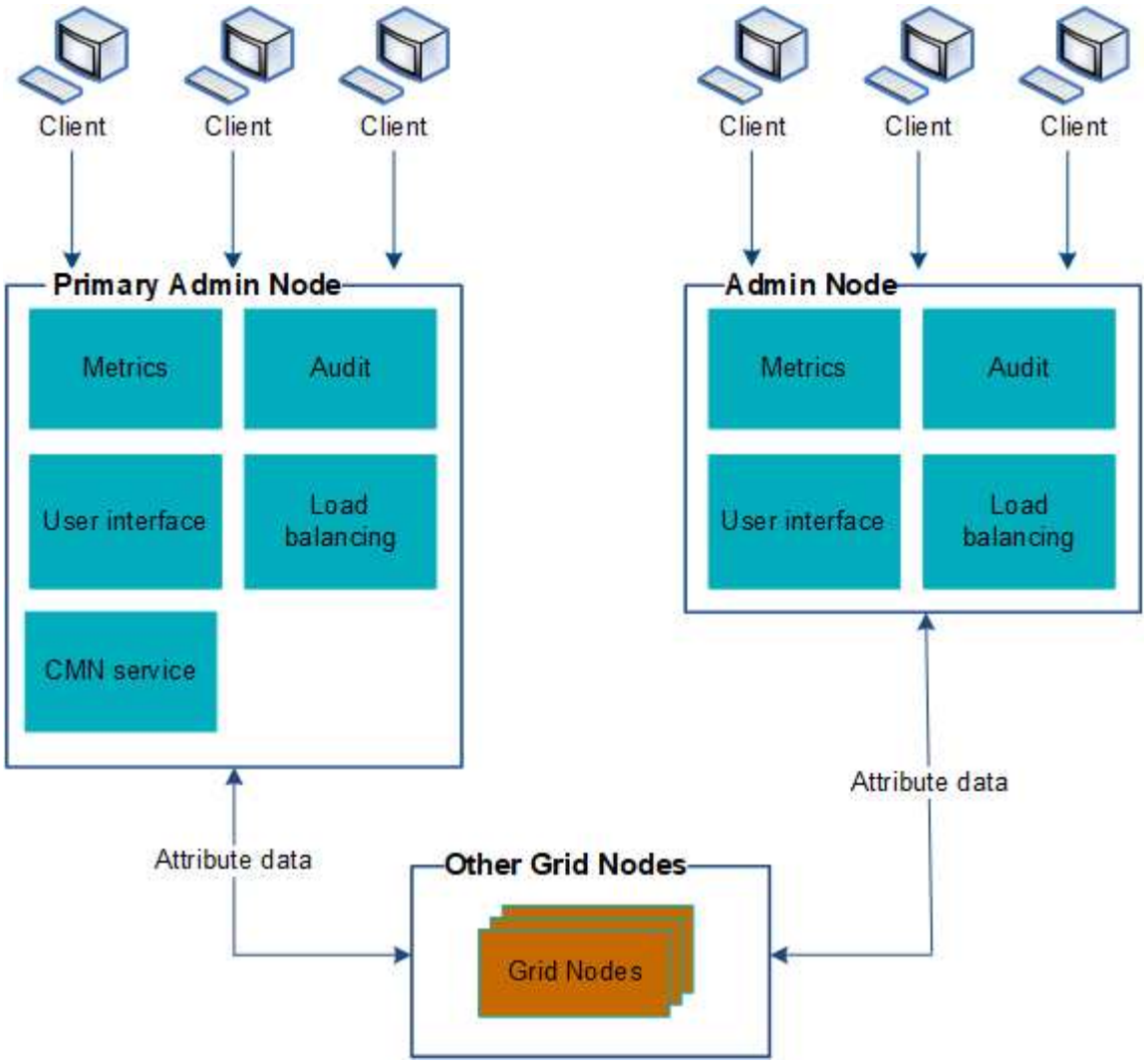
#### Qué es el servicio Prometheus

El servicio Prometheus recopila métricas de series temporales de los servicios de todos los nodos.

## Use varios nodos de administrador

Un sistema StorageGRID puede incluir varios nodos de administrador para permitir supervisar y configurar continuamente el sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, las alertas y alarmas (sistema heredado) aún se activan y las notificaciones por correo electrónico y los mensajes de AutoSupport siguen enviados. Sin embargo, disponer de varios nodos de administrador no proporciona protección contra conmutación al nodo de respaldo, excepto notificaciones y mensajes de AutoSupport. En particular, las confirmaciones de alarma realizadas desde un nodo de administración no se copian a otros nodos de administración.




Si falla un nodo de administración, existen dos opciones para ver y configurar el sistema StorageGRID:

- Los clientes web pueden volver a conectarse a cualquier otro nodo de administrador disponible.
- Si un administrador del sistema ha configurado un grupo de nodos de administración de alta disponibilidad, los clientes web pueden seguir accediendo a Grid Manager o al Gestor de inquilinos mediante la dirección IP virtual del grupo de alta disponibilidad. Consulte Gestión de grupos de alta disponibilidad.

> Cuando se utiliza un grupo de alta disponibilidad, se interrumpe el acceso si falla el nodo de administración maestro. Los usuarios deben volver a iniciar sesión después de que la dirección IP virtual del grupo ha conmute a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo se pueden realizar con el nodo de administrador principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar completamente.

## Identifique el nodo de administración principal

El nodo de administración principal aloja el servicio CMN. Algunos procedimientos de mantenimiento solo se pueden realizar mediante el nodo de administrador principal.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > **Admin Node** y, a continuación, seleccione ➕ Para expandir el árbol de topología y mostrar los servicios alojados en este nodo de administración.

   El nodo de administración principal aloja el servicio CMN.

3. Si este nodo de administrador no aloja el servicio CMN, compruebe los demás nodos de administración.

## Seleccione un remitente preferido

Si la implementación de StorageGRID incluye varios nodos de administrador, puede seleccionar qué nodo de administrador debe ser el remitente preferido de notificaciones. De forma predeterminada, se selecciona el nodo de administración principal, pero cualquier nodo de administración puede ser el remitente preferido.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

La página **CONFIGURATION** > **System** > **Opciones de visualización** muestra qué nodo de administración está seleccionado actualmente para ser el emisor preferido. El nodo de administrador principal está seleccionado de forma predeterminada.

En operaciones normales del sistema, solo el remitente preferido envía las siguientes notificaciones:

- Mensajes de AutoSupport
- Notificaciones SNMP
- Mensajes de correo electrónico de alerta
- Correos electrónicos de alarma (sistema heredado)

Sin embargo, todos los demás nodos de administración (remitentes en espera) supervisan al remitente preferido. Si se detecta un problema, un remitente en espera también puede enviar estas notificaciones.

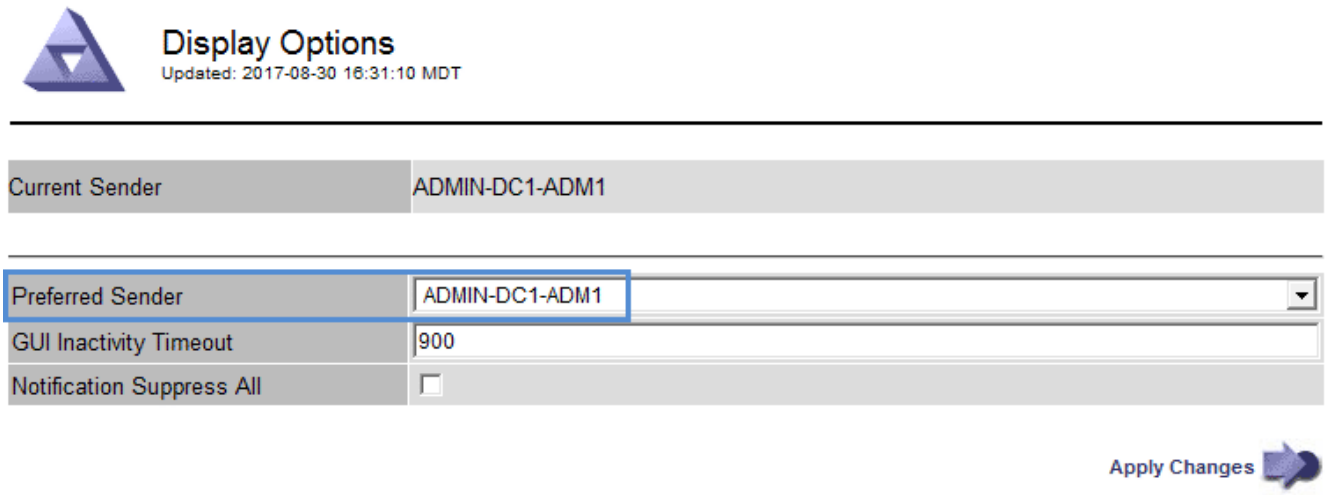
Tanto el remitente preferido como el remitente en espera pueden enviar notificaciones en los siguientes casos:

- Si los nodos de administración se convierten en "'desembarcados'" entre sí, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones, y pueden recibirse varias copias de las notificaciones.
- Después de que un remitente en espera detecta problemas con el remitente preferido y comienza a enviar notificaciones, es posible que el remitente preferido recupere su capacidad de enviar notificaciones. Si esto ocurre, es posible que se envíen notificaciones duplicadas. El remitente en espera dejará de enviar notificaciones cuando ya no detecte errores en el remitente preferido.

Cuando prueba notificaciones de alarma y mensajes de AutoSupport, todos los nodos administrador envían el correo electrónico de prueba. Cuando prueba las notificaciones de alerta, debe iniciar sesión en cada nodo de administrador para verificar la conectividad.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. En el menú Opciones de pantalla, seleccione **Opciones**.
3. Seleccione el nodo de administración que desea establecer como remitente preferido de la lista desplegable.



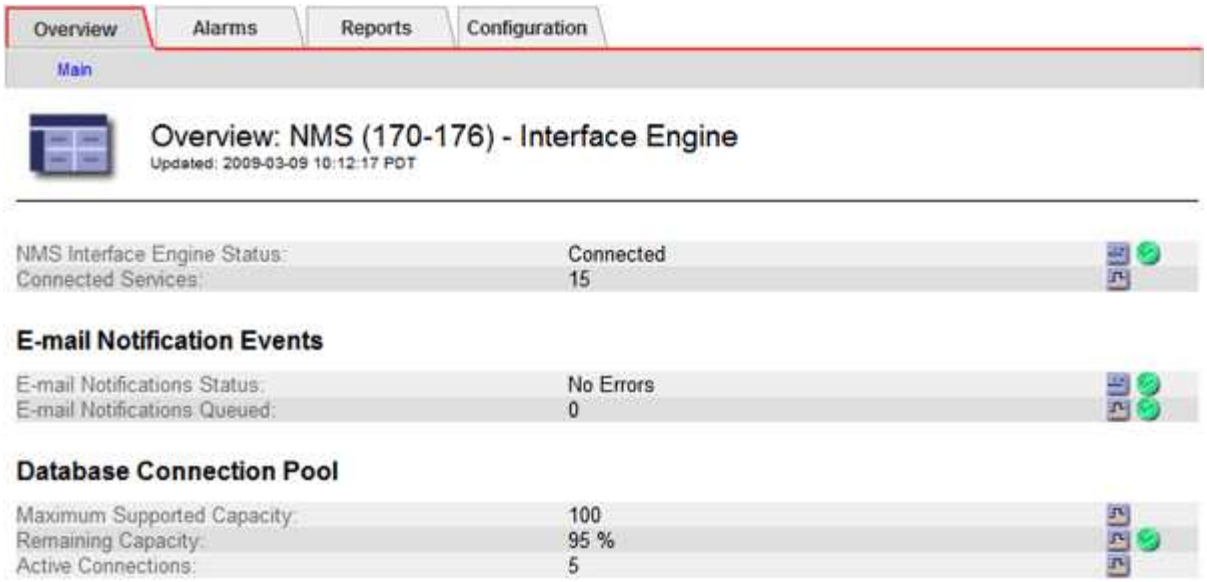

4. Seleccione **aplicar cambios**.

   El nodo de administrador se establece como el remitente preferido de notificaciones.

## Ver el estado de notificación y las colas

El servicio del sistema de administración de redes (NMS) en los nodos de administración envía notificaciones al servidor de correo. Puede ver el estado actual del servicio NMS y el tamaño de su cola de notificaciones en la página Motor de interfaz.

Para acceder a la página Motor de interfaz, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. Por último, seleccione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.

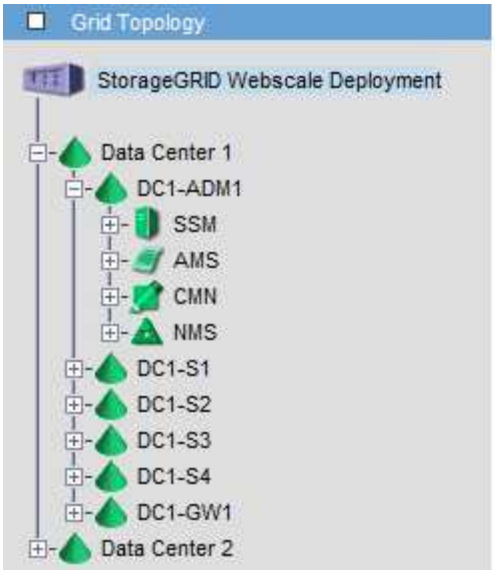


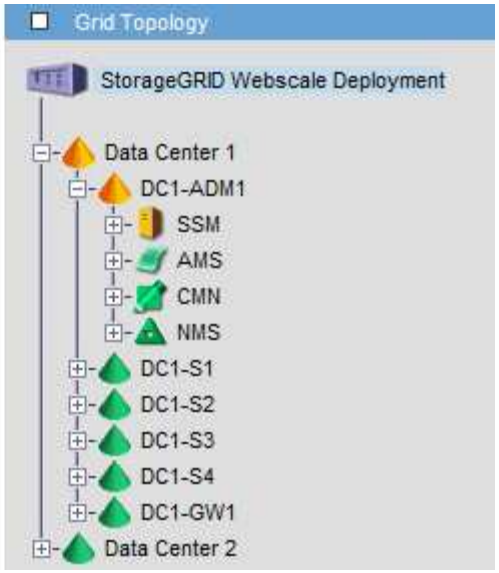

Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la notificación, un intento de mayor esfuerzo de reenviar la notificación al servidor de correo continúa durante un período de 60 segundos. Si la notificación no se envía al servidor de correo después de 60 segundos, la notificación se descarta de la cola de notificaciones y se realiza un intento de enviar la siguiente notificación de la cola. Puesto que las notificaciones se pueden borrar de la cola de notificaciones sin enviarse, es posible que se active una alarma sin que se envíe una notificación. En el caso de que una notificación se descarta de la cola sin enviarse, se activa la alarma Minor DE MINUTOS (Estado de notificación por correo electrónico).

## Cómo muestran los nodos de administración alarmas confirmadas (sistema heredado)

Cuando reconoce una alarma en un nodo de administración, la alarma confirmada no se copia en ningún otro nodo de administración. Debido a que las confirmaciones no se copian en otros nodos de administración, es posible que el árbol de topología de cuadrícula no tenga el mismo aspecto para cada nodo de administración.

Esta diferencia puede ser útil al conectar clientes Web. Los clientes web pueden tener diferentes vistas del sistema StorageGRID de acuerdo con las necesidades del administrador.




Tenga en cuenta que las notificaciones se envían desde el nodo de administración donde se produce la confirmación.

## Configure el acceso de los clientes de auditoría

El nodo Admin, a través del servicio sistema de administración de auditorías (AMS), registra todos los eventos del sistema auditados en un archivo de registro disponible a través del recurso compartido de auditoría, que se agrega a cada nodo Admin en la instalación. Para facilitar el acceso a los registros de auditoría, puede configurar el acceso de los clientes a recursos compartidos de auditoría de CIFS y NFS.

El sistema StorageGRID utiliza un reconocimiento positivo para evitar la pérdida de mensajes de auditoría antes de que se escriban en el archivo de registro. Un mensaje permanece en cola en un servicio hasta que el servicio AMS o un servicio intermedio de retransmisión de auditoría ha reconocido el control de él.

Para obtener más información, consulte Revisar los registros de auditoría.

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID. Si dispone de la opción de utilizar CIFS o NFS, elija NFS.

### Configurar clientes de auditoría para CIFS

El procedimiento utilizado para configurar un cliente de auditoría depende del método de autenticación: Windows Workgroup o Windows Active Directory (AD). Cuando se añade, el recurso compartido de auditoría se habilita automáticamente como un recurso compartido de solo lectura.

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

#### Configurar clientes de auditoría para Workgroup

Realice este procedimiento para cada nodo de administrador en una implementación de

StorageGRID desde la que desea recuperar mensajes de auditoría.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

**Acerca de esta tarea**

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

**Pasos**

1. 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 `#`.

2. Confirme que todos los servicios tienen el estado en ejecución o verificado: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Establezca la autenticación para el grupo de trabajo de Windows:

   Si ya se ha establecido la autenticación, aparece un mensaje de aviso. Si ya se ha configurado la autenticación, vaya al paso siguiente.

   a. Introduzca: `set-authentication`
   b. Cuando se le solicite la instalación de Windows Workgroup o Active Directory, introduzca: `workgroup`

c. Cuando se le solicite, escriba un nombre del grupo de trabajo: *workgroup_name*

d. Cuando se le solicite, cree un nombre NetBIOS significativo: *netbios_name*

o.

Pulse **Intro** para utilizar el nombre de host del nodo de administración como nombre NetBIOS.

La secuencia de comandos reinicia el servidor Samba y se aplican los cambios. Esto debería tardar menos de un minuto. Después de establecer la autenticación, agregue un cliente de auditoría.

a. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

6. Agregar un cliente de auditoría:

a. Introduzca: `add-audit-share`

El recurso compartido se añade automáticamente como de solo lectura.

b. Cuando se le solicite, agregue un usuario o grupo: *user*

c. Cuando se le solicite, introduzca el nombre de usuario de auditoría: *audit_user_name*

d. Cuando se le solicite, escriba una contraseña para el usuario de auditoría: *password*

e. Cuando se le solicite, vuelva a introducir la misma contraseña para confirmarla: *password*

f. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

No es necesario introducir un directorio. El nombre del directorio de auditoría está predefinido.

7. Si se permite que más de un usuario o grupo acceda al recurso compartido de auditoría, agregue los usuarios adicionales:

a. Introduzca: `add-user-to-share`

Se muestra una lista numerada de los recursos compartidos habilitados.

b. Cuando se le solicite, escriba el número del recurso compartido auditoría-exportación: *share_number*

c. Cuando se le solicite, agregue un usuario o grupo: `user`

1. `group`

d. Cuando se le solicite, introduzca el nombre del usuario o grupo de auditoría: *audit_user or audit_group*

e. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

f. Repita estos subpasos para cada usuario o grupo adicional que tenga acceso al recurso compartido de auditoría.

8. Si lo desea, compruebe la configuración: `validate-config`

   Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

   ```
   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
   (16384)
   ```

   a. Cuando se le solicite, pulse **Intro**.

      Se muestra la configuración del cliente de auditoría.

   b. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

9. Cierre la utilidad de configuración CIFS: `exit`
10. Inicie el servicio Samba: `service smbd start`
11. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    o.

    De manera opcional, si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite este recurso compartido de auditoría según sea necesario:

    a. Inicie sesión de forma remota en el nodo de administración de un sitio:
       i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
       ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
       iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
       iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    b. Repita los pasos para configurar el recurso compartido de auditoría de cada nodo de administración adicional.
    c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`
12. Cierre la sesión del shell de comandos: `exit`

#### Configurar clientes de auditoría para Active Directory

## Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).

- Tiene el nombre de usuario y la contraseña de CIFS Active Directory.
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

**Pasos**

1. 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 `#`.

2. Confirme que todos los servicios tienen el estado en ejecución o verificado: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Establezca la autenticación de Active Directory: `set-authentication`

   En la mayoría de las implementaciones, debe establecer la autenticación antes de agregar el cliente de auditoría. Si ya se ha establecido la autenticación, aparece un mensaje de aviso. Si ya se ha configurado la autenticación, vaya al paso siguiente.

   a. Cuando se le solicite la instalación de Workgroup o Active Directory: `ad`
   b. Cuando se le solicite, escriba el nombre del dominio de AD (nombre de dominio corto).
   c. Cuando se le solicite, introduzca la dirección IP o el nombre de host DNS del controlador de dominio.
   d. Cuando se le solicite, escriba el nombre completo del dominio.

Utilice letras mayúsculas.

e. Cuando se le solicite que habilite el soporte winbind, escriba **y**.

Winbind se utiliza para resolver la información de usuarios y grupos desde los servidores AD.

f. Cuando se le solicite, introduzca el nombre NetBIOS.

g. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

6. Únase al dominio:

a. Si no se ha iniciado todavía, inicie la utilidad de configuración de CIFS: `config_cifs.rb`

b. Únase al dominio: `join-domain`

c. Se le solicitará que pruebe si el nodo de administración es actualmente un miembro válido del dominio. Si este nodo de administrador no se ha Unido previamente al dominio, introduzca: `no`

d. Cuando se le solicite, indique el nombre de usuario del administrador: *`administrator_username`*

donde *`administrator_username`* Es el nombre de usuario de CIFS Active Directory, no el de StorageGRID.

e. Cuando se le solicite, proporcione la contraseña del administrador: *`administrator_password`*

lo eran *`administrator_password`* Es el nombre de usuario de CIFS Active Directory, no la contraseña de StorageGRID.

f. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

7. Compruebe que se ha Unido correctamente al dominio:

a. Únase al dominio: `join-domain`

b. Cuando se le solicite que compruebe si el servidor es actualmente un miembro válido del dominio, especifique: `y`

Si recibe el mensaje "'Join is OK,'" se ha Unido correctamente al dominio. Si no obtiene esta respuesta, intente configurar la autenticación y unirse al dominio de nuevo.

c. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

8. Agregar un cliente de auditoría: `add-audit-share`

a. Cuando se le solicite agregar un usuario o grupo, escriba: `user`

b. Cuando se le solicite que introduzca el nombre de usuario de auditoría, introduzca el nombre de usuario de auditoría.

c. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de CIFS.

9. Si se permite que más de un usuario o grupo acceda al recurso compartido de auditoría, agregue usuarios adicionales: `add-user-to-share`

   Se muestra una lista numerada de los recursos compartidos habilitados.

   a. Introduzca el número del recurso compartido auditoría-exportación.
   b. Cuando se le solicite agregar un usuario o grupo, escriba: `group`

      Se le solicitará el nombre del grupo de auditoría.

   c. Cuando se le solicite el nombre del grupo de auditoría, introduzca el nombre del grupo de usuarios de auditoría.
   d. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

   e. Repita este paso con cada usuario o grupo adicional que tenga acceso al recurso compartido de auditoría.

10. Si lo desea, compruebe la configuración: `validate-config`

    Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-interfaces.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-filesystem.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-interfaces.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-custom-config.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-shares.inc`
    - Rlimit_max: Aumentando rlimit_max (1024) al límite mínimo de Windows (16384)

      > No combine la configuración 'Security=ADS' con el parámetro 'Password Server'. (Por defecto Samba descubrirá el DC correcto para contactar automáticamente).

      i. Cuando se le solicite, pulse **Intro** para mostrar la configuración del cliente de auditoría.
      ii. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

11. Cierre la utilidad de configuración CIFS: `exit`
12. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    o.

    De manera opcional, si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite estos recursos compartidos de auditoría según sea necesario:

    a. Inicie sesión de forma remota en el nodo de administración de un sitio:
       i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`

iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración.

c. Cierre el inicio de sesión seguro remoto en Admin Node: `exit`

13. Cierre la sesión del shell de comandos: `exit`

#### Añada un usuario o un grupo a un recurso compartido de auditoría CIFS

## Es posible añadir un usuario o un grupo a un recurso compartido de auditoría CIFS que esté integrado con la autenticación de AD.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

**Acerca de esta tarea**

El siguiente procedimiento es para un recurso compartido de auditoría integrado con la autenticación AD.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

**Pasos**

1. 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 `#`.

2. Confirme que todos los servicios tienen el estado en ejecución o verificado. Introduzca: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
-------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------------
```

5. Comenzar a agregar un usuario o grupo: `add-user-to-share`

   Se muestra una lista numerada de los recursos compartidos de auditoría configurados.

6. Cuando se le solicite, introduzca el número del recurso compartido de auditoría (auditoría-exportación): *`audit_share_number`*

   Se le preguntará si desea proporcionar a un usuario o grupo acceso a este recurso compartido de auditoría.

7. Cuando se le solicite, agregue un usuario o grupo: `user` o. `group`
8. Cuando se le solicite el nombre de usuario o grupo para este recurso compartido de auditoría de AD, escriba el nombre.

   El usuario o grupo se agrega como de solo lectura para el recurso compartido de auditoría tanto en el sistema operativo del servidor como en el servicio CIFS. La configuración de Samba se vuelve a cargar para permitir al usuario o grupo acceder al recurso compartido del cliente de auditoría.

9. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

10. Repita estos pasos para cada usuario o grupo que tenga acceso al recurso compartido de auditoría.
11. Si lo desea, compruebe la configuración: `validate-config`

    Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

    - No se puede encontrar el archivo /etc/samba/includes/cifs-interfaces.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-filesystem.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-custom-config.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-shares.inc.
      i. Cuando se le solicite, pulse **Intro** para mostrar la configuración del cliente de auditoría.
      ii. Cuando se le solicite, pulse **Intro**.

12. Cierre la utilidad de configuración CIFS: `exit`

13. Determine si necesita habilitar recursos compartidos de auditoría adicionales, de la siguiente forma:
    - Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.
    - Si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite estos recursos compartidos de auditoría según sea necesario:
        i. Inicie sesión de forma remota en el nodo de administración de un sitio:
            A. Introduzca el siguiente comando: `ssh admin@grid_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.
        ii. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración.
        iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`
14. Cierre la sesión del shell de comandos: `exit`

#### Quitar un usuario o un grupo de un recurso compartido de auditoría CIFS

## No se puede eliminar el último usuario o grupo permitido para acceder al recurso compartido de auditoría.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con las contraseñas de la cuenta raíz (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

**Acerca de esta tarea**

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

**Pasos**

1. 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 `#`.

2. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
-------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
-------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
-------------------------------------------------------------------
```

3. Comience a eliminar un usuario o grupo: `remove-user-from-share`

   Se muestra una lista numerada de los recursos compartidos de auditoría disponibles para el nodo de administración. El recurso compartido de auditoría se etiqueta audit-export.

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite que elimine un usuario o un grupo: `user` o. `group`

   Se muestra una lista numerada de usuarios o grupos para el recurso compartido de auditoría.

6. Introduzca el número correspondiente al usuario o grupo que desea eliminar: *`number`*

   Se actualiza el recurso compartido de auditoría y el usuario o grupo ya no tiene permiso de acceso al recurso compartido de auditoría. Por ejemplo:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Cierre la utilidad de configuración CIFS: `exit`
8. Si la implementación de StorageGRID incluye nodos de administración en otros sitios, deshabilite el recurso compartido de auditoría en cada sitio según sea necesario.
9. Cierre la sesión de cada shell de comando cuando la configuración se haya completado: `exit`

#### Cambiar un nombre de usuario o de grupo de recurso compartido de auditoría CIFS

Es posible cambiar el nombre de un usuario o de un grupo de un recurso compartido de auditoría de CIFS. Para ello, añada un nuevo usuario o grupo y, a continuación, elimine el anterior.

**Acerca de esta tarea**

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

**Pasos**

1. Agregue un nuevo usuario o grupo con el nombre actualizado al recurso compartido de auditoría.
2. Elimine el nombre de usuario o grupo anterior.

**Información relacionada**

- Añada un usuario o un grupo a un recurso compartido de auditoría CIFS
- Quitar un usuario o un grupo de un recurso compartido de auditoría CIFS

#### Compruebe la integración de la auditoría de CIFS

El recurso compartido de auditoría es de solo lectura. Los archivos de registro están diseñados para que los lean las aplicaciones del equipo y la verificación no incluye abrir un archivo. Se considera suficiente verificación de que los archivos de registro de auditoría aparecen en una ventana del Explorador de Windows. Tras la verificación de la conexión, cierre todas las ventanas.

### Configurar el cliente de auditoría para NFS

El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con la contraseña root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

**Acerca de esta tarea**

Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

**Pasos**

1. 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 `#`.

2. Confirme que todos los servicios tienen el estado en ejecución o verificado. Introduzca: `storagegrid-status`

   Si alguno de los servicios no aparece como en ejecución o verificado, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos. Pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración NFS. Introduzca: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Agregue el cliente de auditoría: `add-audit-share`
   a. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: `client_IP_address`
   b. Cuando se le solicite, pulse **Intro**.
6. Si se permite que más de un cliente de auditoría acceda al recurso compartido de auditoría, agregue la dirección IP del usuario adicional: `add-ip-to-share`
   a. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
   b. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*
   c. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

   d. Repita estos mismos pasos para cada cliente de auditoría adicional que tenga acceso al recurso compartido de auditoría.
7. De manera opcional, compruebe su configuración.
   a. Introduzca lo siguiente: `validate-config`

      Los servicios se comprueban y visualizan.

   b. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

   c. Cierre la utilidad de configuración NFS: `exit`
8. Determine si debe habilitar los recursos compartidos de auditoría en otros sitios.

- Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.
- Si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite estos recursos compartidos de auditoría según sea necesario:
  i. Inicie sesión de forma remota en el nodo de administración del sitio:
    A. Introduzca el siguiente comando: `ssh admin@grid_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.
  ii. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.
  iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota. Introduzca: `exit`

9. Cierre la sesión del shell de comandos: `exit`

   A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido o elimine un cliente de auditoría existente eliminando su dirección IP.

#### Agregar un cliente de auditoría NFS a un recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido de auditoría.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

**Pasos**

1. 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 `#`.

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Introduzca: `add-ip-to-share`

   Se muestra una lista de los recursos compartidos de auditoría de NFS habilitados en el nodo de administración. El recurso compartido de auditoría aparece como: `/var/local/audit/export`

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*

   El cliente de auditoría se agrega al recurso compartido de auditoría.

6. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

7. Repita los pasos para cada cliente de auditoría que se debe agregar al recurso compartido de auditoría.
8. Si lo desea, compruebe la configuración: `validate-config`

   Los servicios se comprueban y visualizan.

   a. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

9. Cierre la utilidad de configuración NFS: `exit`
10. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    De lo contrario, si la implementación de StorageGRID incluye nodos de administración en otros sitios, opcionalmente podrá habilitar estos recursos compartidos de auditoría según sea necesario:

    a. Inicie sesión de forma remota en el nodo de administración de un sitio:
       i. Introduzca el siguiente comando: `ssh admin@`*`grid_node_IP`*
       ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
       iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
       iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración.

c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`

11. Cierre la sesión del shell de comandos: `exit`

#### Comprobar la integración de auditoría de NFS

Después de configurar un recurso compartido de auditoría y agregar un cliente de auditoría NFS, puede montar el recurso compartido del cliente de auditoría y comprobar que los archivos estén disponibles en el recurso compartido de auditoría.

**Pasos**

1. Verifique la conectividad (o variante para el sistema cliente) usando la dirección IP del cliente del nodo de administración que aloja el servicio AMS. Introduzca: `ping IP_address`

   Verifique que el servidor responde, indicando conectividad.

2. Monte el recurso compartido de sólo lectura de auditoría usando un comando apropiado para el sistema operativo cliente. Un comando de Linux de ejemplo es (introduzca en una línea):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Utilice la dirección IP del nodo de administración que aloja el servicio AMS y el nombre de recurso compartido predefinido para el sistema de auditoría. El punto de montaje puede ser cualquier nombre seleccionado por el cliente (por ejemplo, *`myAudit`* en el comando anterior).

3. Verifique que los archivos estén disponibles en el recurso compartido de auditoría. Introduzca: `ls myAudit /*`

   donde *`myAudit`* es el punto de montaje del recurso compartido de auditoría. Debe haber al menos un archivo de registro en la lista.

#### Eliminar un cliente de auditoría NFS del recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Puede eliminar un cliente de auditoría existente eliminando su dirección IP.

**Lo que necesitará**

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

**Acerca de esta tarea**

No se puede eliminar la última dirección IP permitida para acceder al recurso compartido de auditoría.

**Pasos**

1. 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 `#`.

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Elimine la dirección IP del recurso compartido de auditoría: `remove-ip-from-share`

Se muestra una lista numerada de recursos compartidos de auditoría configurados en el servidor. El recurso compartido de auditoría aparece como: `/var/local/audit/export`

4. Introduzca el número correspondiente al recurso compartido de auditoría: *`audit_share_number`*

Se muestra una lista numerada de direcciones IP permitidas para acceder al recurso compartido de auditoría.

5. Introduzca el número correspondiente a la dirección IP que desea eliminar.

El recurso compartido de auditoría se actualiza y ya no se permite el acceso desde ningún cliente de auditoría con esta dirección IP.

6. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de NFS.

7. Cierre la utilidad de configuración NFS: `exit`
8. Si la implementación de StorageGRID es una puesta en marcha de varios sitios de centro de datos con nodos de administración adicionales en otros sitios, deshabilite estos recursos compartidos de auditoría según sea necesario:
   a. Inicie sesión de forma remota en el nodo de administración de cada sitio:
      i. Introduzca el siguiente comando: `ssh admin@`*`grid_node_IP`*
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.

c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`

9. Cierre la sesión del shell de comandos: `exit`

#### Cambiar la dirección IP de un cliente de auditoría de NFS

Complete estos pasos si necesita cambiar la dirección IP de un cliente de auditoría de NFS.

**Pasos**

1. Agregue una nueva dirección IP a un recurso compartido de auditoría NFS existente.
2. Elimine la dirección IP original.

**Información relacionada**

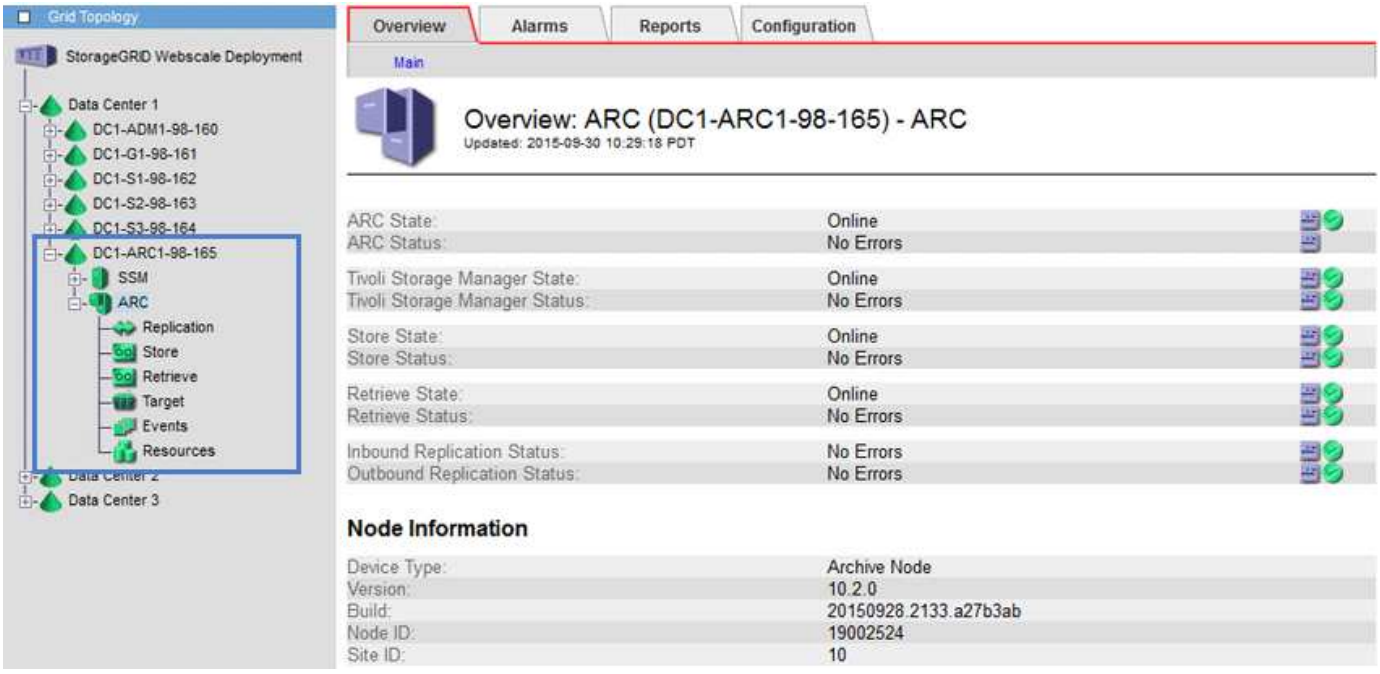
- Agregar un cliente de auditoría NFS a un recurso compartido de auditoría
- Eliminar un cliente de auditoría NFS del recurso compartido de auditoría

# Gestione los nodos de archivado

## Qué es un nodo de archivado

Opcionalmente, cada sitio del centro de datos StorageGRID se puede poner en marcha con un nodo de archivado, que permite conectarse a un sistema de almacenamiento de archivado externo específico, como Tivoli Storage Manager (TSM).

El nodo de archivado proporciona una interfaz a través de la cual se puede dirigir un sistema de almacenamiento de archivado externo para el almacenamiento a largo plazo de datos de objetos. El nodo de archivado también supervisa esta conexión y la transferencia de datos de objeto entre el sistema StorageGRID y el sistema de almacenamiento de archivado externo objetivo.




Después de configurar las conexiones con el destino externo, puede configurar el nodo de archivado para

optimizar el rendimiento de TSM, desconectar un nodo de archivado cuando un servidor TSM se acerca a la capacidad o no está disponible y configurar la configuración de replicación y recuperación. También puede establecer alarmas personalizadas para el nodo de archivado.

Los datos de objetos que no se pueden eliminar, pero a los que no se tiene acceso regularmente, se pueden trasladar en cualquier momento fuera de los discos giratorios de un nodo de almacenamiento y a un almacenamiento de archivado externo, como el cloud o la cinta. Este archivado de los datos de objetos se realiza mediante la configuración del nodo de archivado del sitio del centro de datos y, a continuación, con la configuración de las reglas de ILM donde este nodo de archivado se selecciona como el "destino" para obtener instrucciones de colocación de contenido. El nodo de archivado no gestiona los propios datos de objetos archivados, lo consigue el dispositivo de archivado externo.

Los metadatos de objetos no se archivan, pero siguen en los nodos de almacenamiento.

#### Qué es el servicio ARC

El servicio de archivado (ARC) en nodos de archivado ofrece la interfaz de gestión que se puede utilizar para configurar conexiones a almacenamiento de archivado externo, como la cinta, a través de middleware TSM.

Se trata del servicio de ARC que interactúa con un sistema de almacenamiento de archivado externo, por lo que envía datos de objetos para almacenamiento near-line y realiza recuperaciones cuando una aplicación cliente solicita un objeto archivado. Cuando una aplicación cliente solicita un objeto archivado, un nodo de almacenamiento solicita los datos del objeto del servicio ARC. El servicio ARC realiza una solicitud al sistema de almacenamiento de archivos externo, que recupera los datos de objeto solicitados y los envía al servicio ARC. El servicio ARC verifica los datos del objeto y los reenvía al nodo de almacenamiento, que a su vez devuelve el objeto a la aplicación cliente solicitante.

Las solicitudes de datos de objetos archivados a cinta mediante TSM Middleware se gestionan por la eficiencia de las recuperaciones. Las solicitudes se pueden solicitar para que los objetos almacenados en orden secuencial en la cinta se soliciten en el mismo orden secuencial. A continuación, las solicitudes se colocan en la cola de espera para su envío al dispositivo de almacenamiento. En función del dispositivo de archivado, se pueden procesar simultáneamente varias solicitudes de objetos en diferentes volúmenes.

## Archivado en el cloud mediante la API de S3

Puede configurar un nodo de archivado para conectarse directamente a Amazon Web Services (AWS) o a cualquier otro sistema que pueda conectarse al sistema StorageGRID a través de la API de S3.

El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades. La opción **Cloud Tiering - simple Storage Service (S3)** sigue siendo compatible, pero puede que prefiera implementar Cloud Storage Pools en su lugar.

Si actualmente utiliza un nodo de archivado con la opción **Cloud Tiering - simple Storage Service (S3)**, considere la posibilidad de migrar los objetos a un grupo de almacenamiento en cloud. Consulte las instrucciones para Gestión de objetos con ILM.

#### Configure los ajustes de conexión para la API de S3

Si se conecta a un nodo de archivado con la interfaz de S3, debe configurar los ajustes

de conexión para la API de S3. Hasta que se hayan configurado estos ajustes, el servicio ARC permanecerá en un estado de alarma principal, ya que no puede comunicarse con el sistema de almacenamiento de archivos externo.

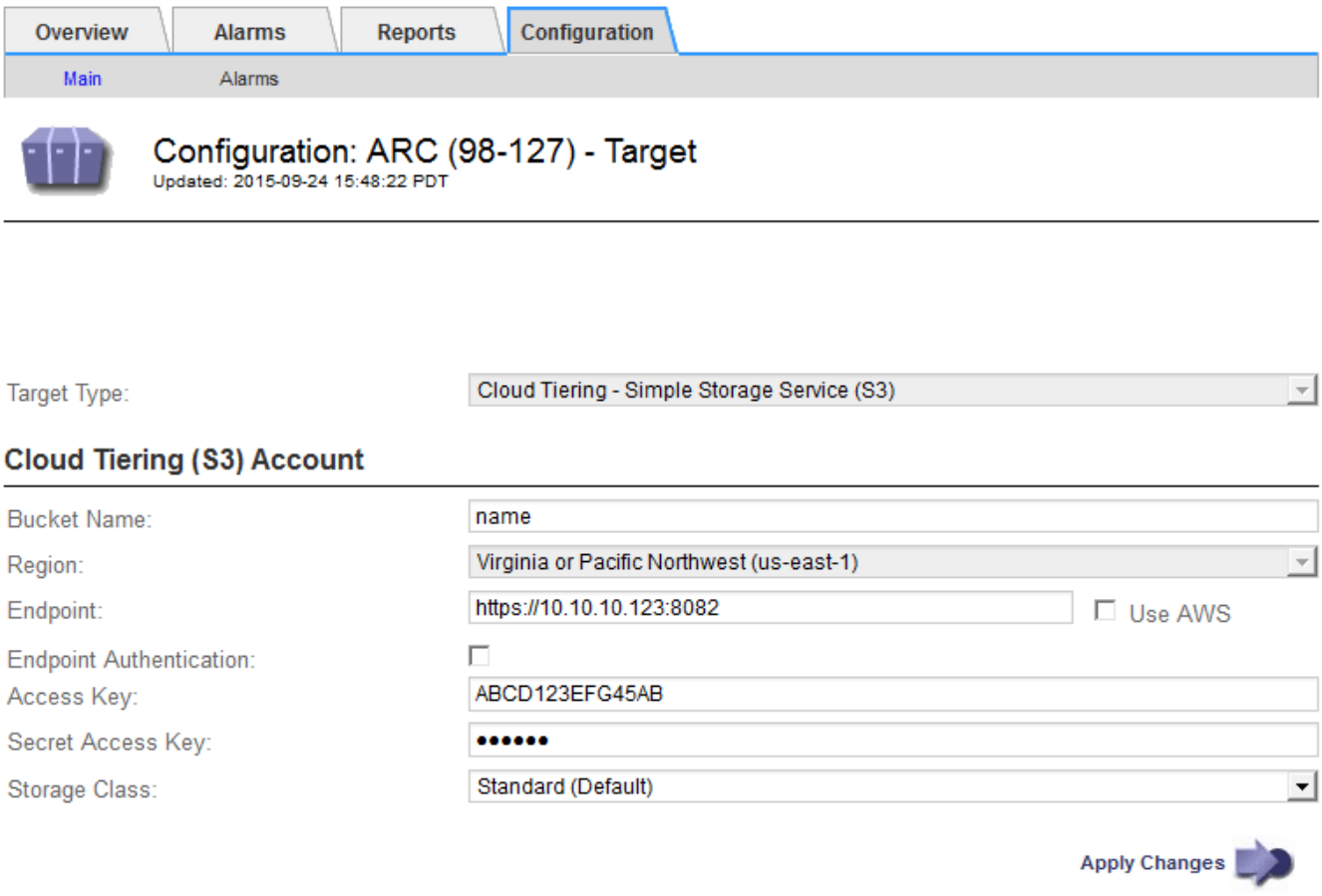
> El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades. La opción **Cloud Tiering - simple Storage Service (S3)** sigue siendo compatible, pero puede que prefiera implementar Cloud Storage Pools en su lugar.
>
> Si actualmente utiliza un nodo de archivado con la opción **Cloud Tiering - simple Storage Service (S3)**, considere la posibilidad de migrar los objetos a un grupo de almacenamiento en cloud. Consulte Gestión de objetos con ILM.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha creado un bucket en el sistema de almacenamiento de archivado de destino:
  - El bloque está dedicado a un único nodo de archivado. No puede utilizarlo otros nodos de archivado ni otras aplicaciones.
  - El cucharón tiene la región adecuada seleccionada para su ubicación.
  - El bloque debe configurarse con el control de versiones suspendido.
- La segmentación de objetos está activada y el tamaño máximo de segmento es menor o igual a 4.5 GIB (4,831,838,208 bytes). Las solicitudes de API S3 que superen este valor fallarán si se usa S3 como sistema de almacenamiento de archivado externo.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **objetivo**.
3. Seleccione **Configuración** > **Principal**.




4. Seleccione **Cloud Tiering - simple Storage Service (S3)** en la lista desplegable Target Type.

> Los ajustes de configuración no estarán disponibles hasta que seleccione un tipo de destino.

5. Configure la cuenta de organización en niveles de cloud (S3) a través de la cual el nodo de archivado se conectará al sistema de almacenamiento de archivado externo compatible con S3 de destino.

   La mayoría de los campos en esta página son claros y explicativos. A continuación, se describen los campos que podrían presentar dificultades.

   - **Región**: Sólo está disponible si se selecciona **usar AWS**. La región que seleccione debe coincidir con la región del bloque.
   - **Endpoint** y **Use AWS**: Para Amazon Web Services (AWS), seleccione **usar AWS**. **Endpoint** se rellena automáticamente con una dirección URL de extremo basada en los atributos Nombre de bloque y Región. Por ejemplo:

     `https://bucket.region.amazonaws.com`

     En el caso de un destino que no sea AWS, introduzca la URL del sistema que aloja el bloque, incluido el número de puerto. Por ejemplo:

`https://system.com:1080`

   - **Autenticación de punto final**: Activada de forma predeterminada. Si la red al sistema de almacenamiento de archivado externo es de confianza, puede anular la selección de la casilla de verificación para deshabilitar la verificación de nombre de host y certificado SSL de punto final para el

sistema de almacenamiento de archivado externo de destino. Si otra instancia de un sistema StorageGRID es el dispositivo de almacenamiento de archivado de destino y el sistema está configurado con certificados firmados públicamente, puede mantener seleccionada la casilla de verificación.

- **Clase de almacenamiento**: Seleccione **Estándar (predeterminado)** para almacenamiento normal. Seleccione **redundancia reducida** sólo para objetos que se puedan volver a crear fácilmente. **Redundancia reducida** proporciona almacenamiento de menor costo con menos confiabilidad. Si el sistema de almacenamiento de archivado objetivo es otra instancia del sistema StorageGRID, **clase de almacenamiento** controla cuántas copias provisionales del objeto se realizan durante el procesamiento en el sistema de destino, si se utiliza el COMMIT doble cuando se ingieren objetos allí.

6. Seleccione **aplicar cambios**.

   Los ajustes de configuración especificados se validan y se aplican al sistema StorageGRID. Una vez que se configura, el destino no se puede cambiar.

### Modifique la configuración de conexión para la API de S3

Una vez que se configura el nodo de archivado para conectarse a un sistema de almacenamiento de archivado externo a través de la API S3, puede modificar algunos ajustes si cambia la conexión.

#### Lo que necesitará

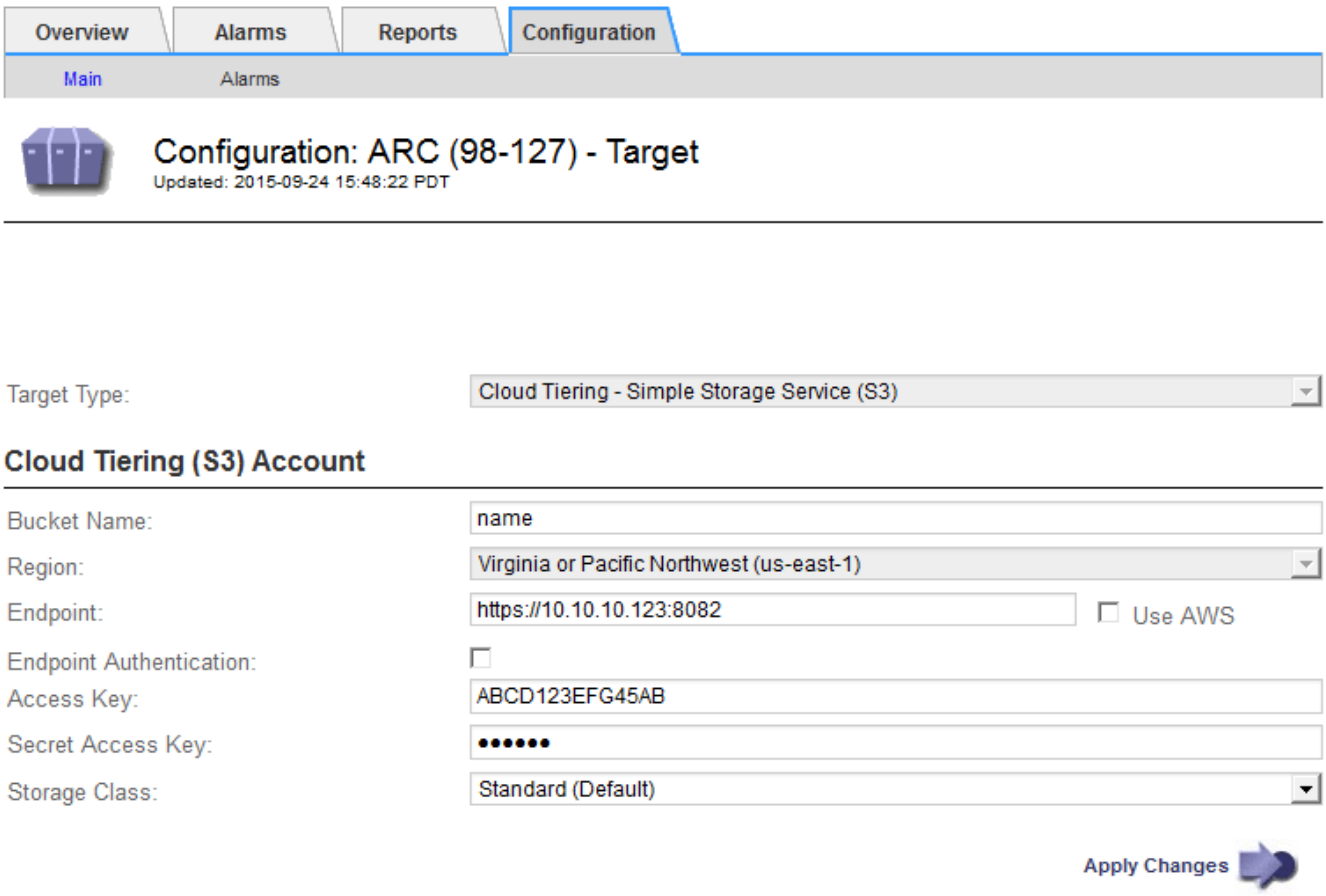
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

#### Acerca de esta tarea

Si cambia la cuenta de Cloud Tiering (S3), debe asegurarse de que las credenciales de acceso del usuario tengan acceso de lectura/escritura al bloque, incluidos todos los objetos que el nodo de archivado había ingerido previamente en el bloque.

#### Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.




4. Modifique la información de la cuenta, según sea necesario.

   Si cambia la clase de almacenamiento, se almacenan datos de objeto nuevos con la nueva clase de almacenamiento. El objeto existente continúa almacenado en la clase de almacenamiento definida cuando se procesa.

   Nombre de bloque, región y extremo, utilice los valores de AWS y no se puede cambiar.

5. Seleccione **aplicar cambios**.

### Modifique el estado del servicio de organización en niveles del cloud

Puede controlar la capacidad de lectura y escritura del nodo de archivado en el sistema de almacenamiento de archivado externo objetivo que se conecta a través de la API de S3 cambiando el estado del servicio de organización en niveles de cloud.

#### Lo que necesitará

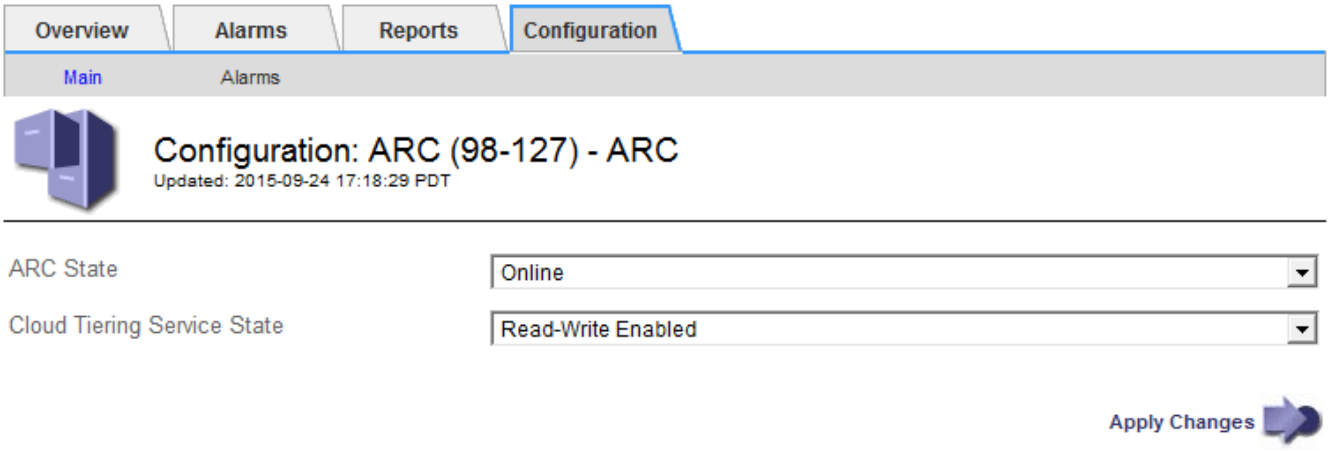
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- Debe configurarse el nodo de archivado.

#### Acerca de esta tarea

Puede desconectar el nodo de archivado de forma efectiva cambiando el estado del servicio de organización en niveles en la nube a **Read-Write Disabled**.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC**.
3. Seleccione **Configuración** > **Principal**.




4. Seleccione un **Estado del servicio de organización en niveles de la nube**.
5. Seleccione **aplicar cambios**.

### Restablezca el número de errores de almacén para la conexión API de S3

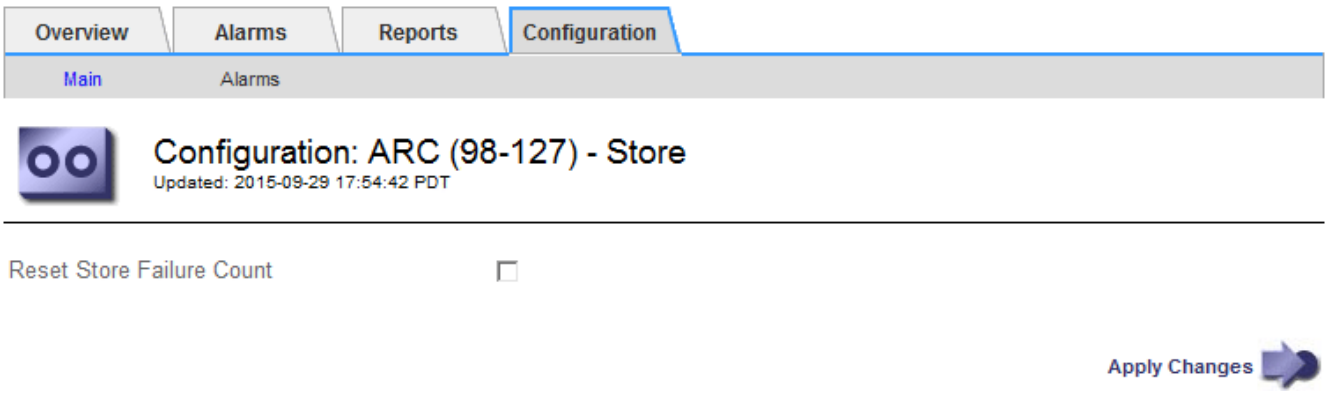
Si el nodo de archivado se conecta a un sistema de almacenamiento de archivado a través de la API de S3, puede restablecer el recuento de fallos de almacenamiento, que se puede utilizar para borrar la alarma de ARVF (fallos de almacenamiento).

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.




4. Seleccione **Restablecer recuento de fallos de tienda**.

5. Seleccione **aplicar cambios**.

   El atributo fallos de almacén se restablece a cero.

### Migrar objetos desde organización en niveles en el cloud: S3 a un pool de almacenamiento en el cloud

Si actualmente utiliza la función **Cloud Tiering - simple Storage Service (S3)** para organizar los datos de objetos en niveles en un bloque de S3, considere la posibilidad de migrar sus objetos a un Cloud Storage Pool en su lugar. Los pools de almacenamiento en cloud proporcionan un método escalable que aprovecha todos los nodos de almacenamiento del sistema StorageGRID.

#### Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ya ha almacenado objetos en el bloque de S3 configurado para la organización en niveles del cloud.

> Antes de migrar datos de objetos, póngase en contacto con su representante de cuenta de NetApp para comprender y gestionar cualquier coste asociado.

#### Acerca de esta tarea

Desde el punto de vista de la gestión del ciclo de vida de la información, un pool de almacenamiento en cloud es similar al de un pool de almacenamiento. Sin embargo, si bien los pools de almacenamiento constan de nodos de almacenamiento o nodos de archivado dentro del sistema StorageGRID, un pool de almacenamiento en cloud consta de un bloque S3 externo.

Antes de migrar objetos desde Cloud Tiering: S3 a un pool de almacenamiento en cloud, primero debe crear un bucket de S3 y, a continuación, crear el Cloud Storage Pool en StorageGRID. A continuación, se puede crear una nueva política de ILM y reemplazar la regla de ILM utilizada para almacenar objetos en el bloque de niveles de cloud con una regla de ILM clonada que almacena los mismos objetos en el Cloud Storage Pool.

> Cuando los objetos se almacenan en un pool de almacenamiento en cloud, las copias de dichos objetos no se pueden almacenar también en StorageGRID. Si la regla de ILM que está usando actualmente para la organización en niveles del cloud está configurada para almacenar objetos en varias ubicaciones a la vez, considere si desea realizar esta migración opcional porque perderá esa funcionalidad. Si continúa con esta migración, debe crear nuevas reglas en lugar de clonar las existentes.

#### Pasos

1. Cree un pool de almacenamiento en el cloud.

   Utilice un nuevo bloque de S3 para el Cloud Storage Pool a fin de garantizar que solo contenga los datos gestionados por el Cloud Storage Pool.

2. Ubique cualquier regla de ILM en la política activa de ILM que provoque que los objetos se almacenen en el bloque de niveles del cloud.
3. Clonar cada una de estas reglas.
4. En las reglas clonadas, cambie la ubicación de ubicación a la nueva agrupación de almacenamiento en cloud.

5. Guarde las reglas clonadas.
6. Cree una nueva directiva que utilice las nuevas reglas.
7. Simular y activar la nueva directiva.

   Cuando se activa la nueva política y se realiza la evaluación de ILM, los objetos se mueven desde el bloque de S3 configurado para Cloud Tiering al bloque de S3 configurado para Cloud Storage Pool. El espacio utilizable de la cuadrícula no se ve afectado. Una vez que los objetos se mueven al Cloud Storage Pool, se eliminan del bloque de almacenamiento en niveles del cloud.

**Información relacionada**

Gestión de objetos con ILM

## Archivado en cinta mediante TSM Middleware

Puede configurar un nodo de archivado para que se destine a un servidor de Tivoli Storage Manager (TSM) que proporcione una interfaz lógica para almacenar y recuperar datos de objetos en dispositivos de almacenamiento de acceso aleatorio o secuencial, incluidas bibliotecas de cintas.

El servicio ARC del nodo de archivado actúa como cliente al servidor TSM, usando Tivoli Storage Manager como middleware para comunicarse con el sistema de almacenamiento de archivado.

### Clases de gestión de TSM

Las clases de gestión definidas por el middleware TSM describen cómo funcionan las operaciones de copia de seguridad y archivado de TSM's y se pueden utilizar para especificar reglas para el contenido que aplica el servidor TSM. Estas reglas funcionan de manera independiente con la política de ILM del sistema StorageGRID, y deben ser coherentes con la necesidad del sistema StorageGRID de que los objetos se almacenen de forma permanente y que siempre estén disponibles para su recuperación en el nodo de archivado. Una vez que el nodo de archivado envía los datos de objeto a un servidor TSM, se aplican las reglas de ciclo de vida y retención de TSM mientras los datos del objeto se almacenan en cinta gestionada por el servidor TSM.

El servidor TSM utiliza la clase de gestión TSM para aplicar reglas para la ubicación de los datos o la retención después de que el nodo de archivado envía los objetos al servidor TSM. Por ejemplo, los objetos identificados como backups de base de datos (contenido temporal que puede sobrescribirse con datos más nuevos) se pueden tratar de forma diferente a los datos de la aplicación (contenido fijo que debe conservarse indefinidamente).

### Configurar conexiones al middleware TSM

Antes de que el nodo de archivado pueda comunicarse con el middleware Tivoli Storage Manager (TSM), debe configurar una serie de opciones.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

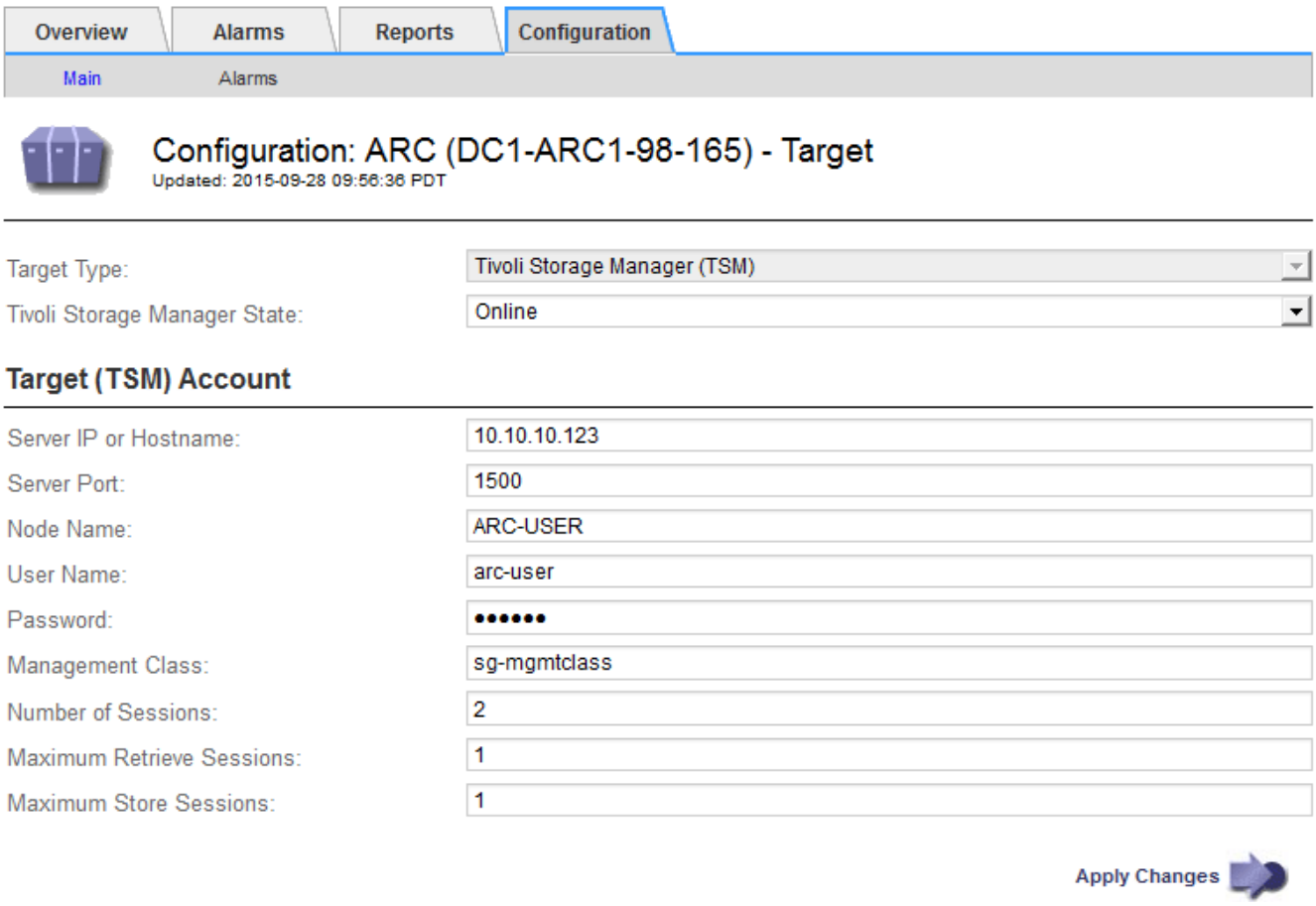
**Acerca de esta tarea**

Hasta que se hayan configurado estos ajustes, el servicio ARC permanecerá en un estado de alarma

principal, ya que no puede comunicarse con Tivoli Storage Manager.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.




4. En la lista desplegable **Tipo de destino**, seleccione **Tivoli Storage Manager (TSM)**.
5. En **Tivoli Storage Manager State**, seleccione **Offline** para evitar las recuperaciones desde el servidor de middleware TSM.

   De forma predeterminada, el estado de Tivoli Storage Manager se establece en línea, lo que significa que el nodo de archivado puede recuperar datos de objeto del servidor de middleware TSM.

6. Complete la siguiente información:

   - **IP del servidor o nombre de host**: Especifique la dirección IP o el nombre de dominio completo del servidor de middleware TSM utilizado por el servicio ARC. La dirección IP predeterminada es 127.0.0.1.
   - **Puerto del servidor**: Especifique el número de puerto en el servidor de middleware TSM al que se conectará el servicio ARC. El valor predeterminado es 1500.
   - **Nombre de nodo**: Especifique el nombre del nodo de archivado. Debe introducir el nombre (Arc-user) que ha registrado en el servidor de middleware TSM.
   - **Nombre de usuario**: Especifique el nombre de usuario que el servicio ARC utiliza para iniciar sesión en el servidor TSM. Introduzca el nombre de usuario predeterminado (Arc-user) o el usuario

administrativo que ha especificado para el nodo de archivado.

- **Contraseña**: Especifique la contraseña utilizada por el servicio ARC para iniciar sesión en el servidor TSM.
- **Clase de administración**: Especifique la clase de administración predeterminada que se va a utilizar si no se especifica una clase de administración cuando el objeto se está guardando en el sistema StorageGRID, o la clase de administración especificada no está definida en el servidor de middleware TSM.
- **Número de sesiones**: Especifique el número de unidades de cinta en el servidor de middleware TSM dedicadas al nodo de archivado. El nodo de archivado crea simultáneamente un máximo de una sesión por punto de montaje más un pequeño número de sesiones adicionales (menos de cinco).

  Debe cambiar este valor para que sea igual al valor establecido para MAXNUMMP (número máximo de puntos de montaje) cuando se registró o actualizó el nodo de archivado. (En el comando register, el valor predeterminado de MAXNUMMP utilizado es 1, si no se establece ningún valor.)

También debe cambiar el valor de MAXSESSIONS para el servidor TSM a un número que sea al menos tan grande como el número de sesiones establecido para el servicio ARC. El valor predeterminado de MAXSESSIONS en el servidor TSM es 25.

- **Sesiones de recuperación máximas**: Especifique el número máximo de sesiones que el servicio ARC puede abrir al servidor de middleware TSM para las operaciones de recuperación. En la mayoría de los casos, el valor apropiado es el número de sesiones menos el número máximo de sesiones de almacén. Si necesita compartir una unidad de cinta para su almacenamiento y recuperación, especifique un valor igual al número de sesiones.
- **Sesiones de almacenamiento máximas**: Especifique el número máximo de sesiones simultáneas que el servicio ARC puede abrir al servidor de middleware TSM para operaciones de archivado.

  Este valor se debería establecer en uno excepto cuando el sistema de almacenamiento de archivado destino está lleno y solo se pueden llevar a cabo recuperaciones. Establezca este valor en cero para utilizar todas las sesiones para las recuperaciones.

7. Seleccione **aplicar cambios**.

### Optimice un nodo de archivado para sesiones de middleware de TSM

Puede optimizar el rendimiento de un nodo de archivado que se conecta a Tivoli Server Manager (TSM) configurando las sesiones del nodo de archivado.

#### Lo que necesitará

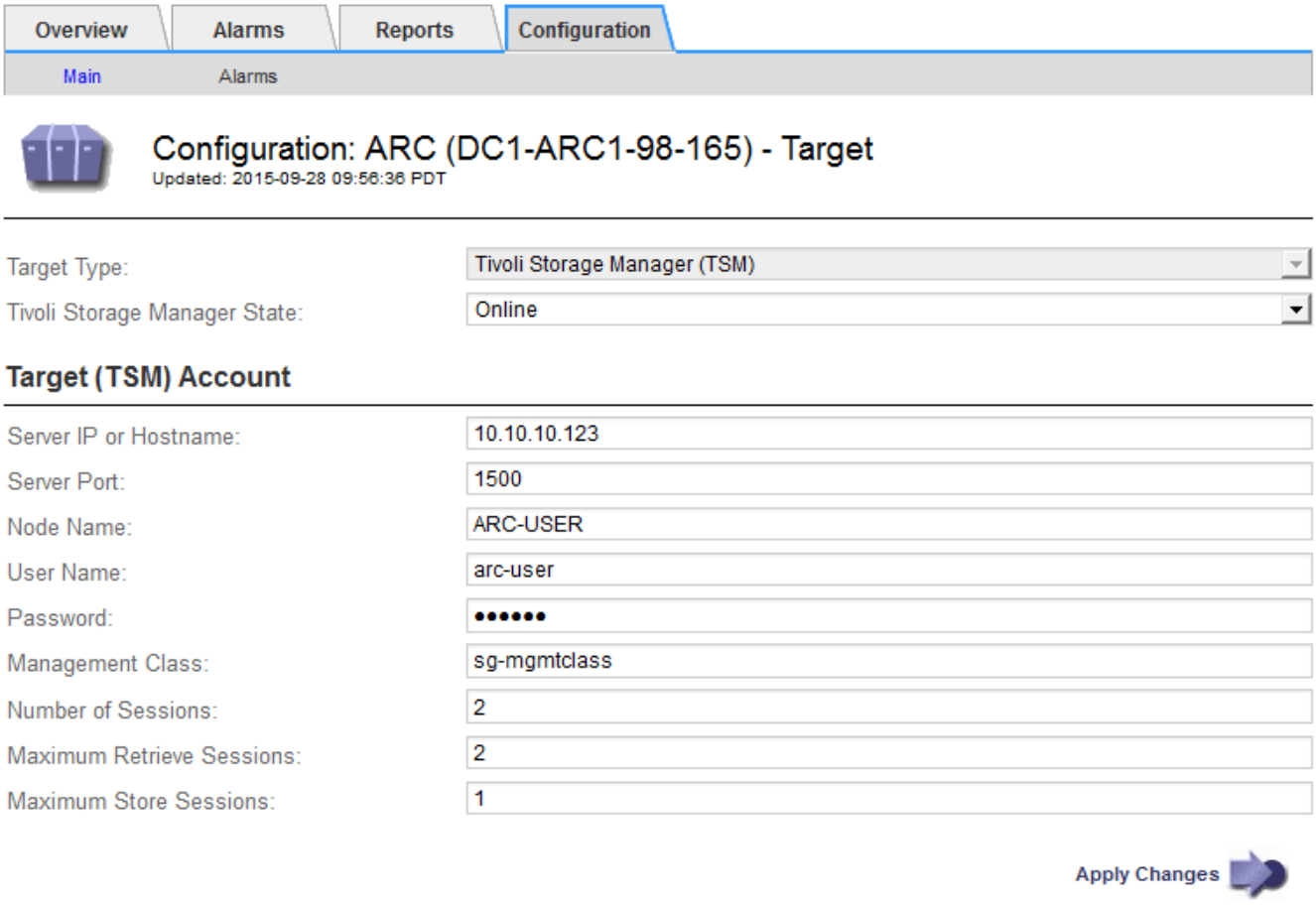
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

#### Acerca de esta tarea

Normalmente, el número de sesiones simultáneas que el nodo de archivado ha abierto al servidor de middleware TSM se establece en el número de unidades de cinta que el servidor TSM ha dedicado al nodo de archivado. Se asigna una unidad de cinta para el almacenamiento mientras el resto se asigna para la recuperación. Sin embargo, en situaciones en las que un nodo de almacenamiento se está reconstruyendo desde copias de nodo de archivado o el nodo de archivado está funcionando en modo de sólo lectura, puede optimizar el rendimiento del servidor TSM estableciendo el número máximo de sesiones de recuperación para que sea el mismo que el número de sesiones simultáneas. El resultado es que todas las unidades pueden utilizarse al mismo tiempo para la recuperación; como máximo, una de estas unidades también puede utilizarse para el almacenamiento, si corresponde.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.
4. Cambiar **máximo de sesiones de recuperación** para que sea igual que **número de sesiones**.




5. Seleccione **aplicar cambios**.

### Configure el estado del archivo y los contadores para TSM

Si el nodo de archivado se conecta a un servidor de middleware TSM, puede configurar el estado del almacén de archivos de un nodo de archivado en línea o sin conexión. También puede desactivar el almacén de archivos cuando se inicie el nodo de archivado por primera vez o restablecer el recuento de fallos que se va a realizar el seguimiento de la alarma asociada.

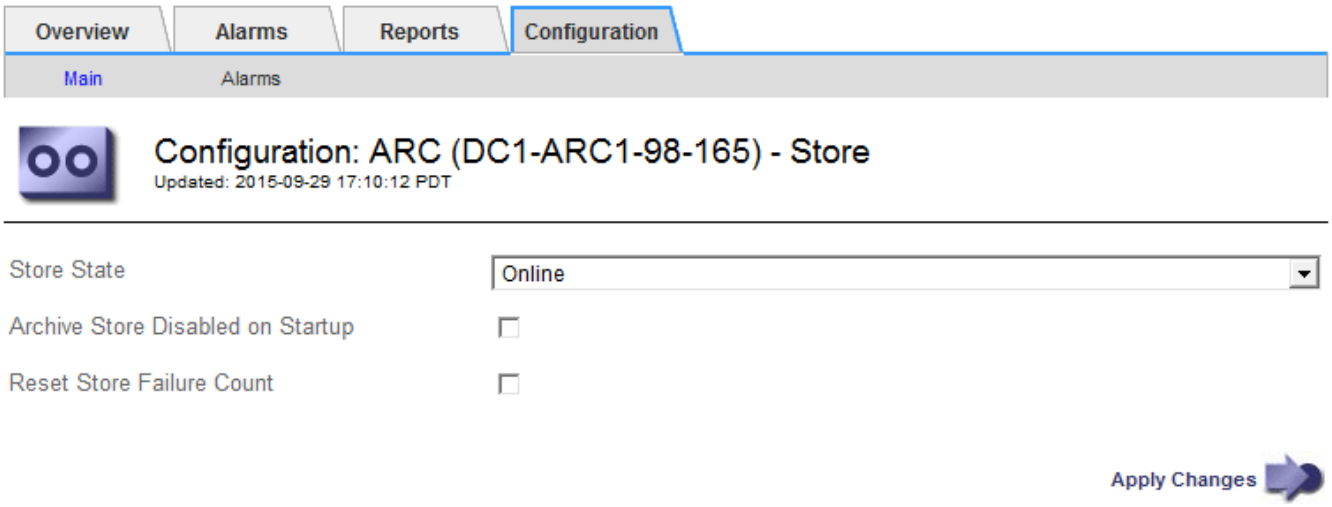
**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.

3. Seleccione **Configuración** > **Principal**.




4. Modifique los siguientes ajustes, según sea necesario:
   - Estado del almacén: Establezca el estado del componente en:
     - Online: El nodo de archivado está disponible para procesar datos de objetos para el almacenamiento del sistema de almacenamiento de archivado.
     - Offline: El nodo de archivado no está disponible para procesar datos de objetos para el almacenamiento del sistema de almacenamiento de archivado.
   - Almacén de archivos desactivado al inicio: Cuando se selecciona, el componente almacén de archivos permanece en el estado de sólo lectura cuando se reinicia. Se usa para deshabilitar de forma persistente el almacenamiento en el sistema de almacenamiento de archivado dirigido. Útil cuando el sistema de almacenamiento de archivado dirigido no puede aceptar contenido.
   - Restablecer recuento de fallos de almacén: Restablezca el contador para fallos de almacén. Se puede utilizar para borrar la alarma ARVF (fallo de almacén).
5. Seleccione **aplicar cambios**.

**Información relacionada**

Gestione un nodo de archivado cuando el servidor TSM alcance la capacidad

### Gestione un nodo de archivado cuando el servidor TSM alcance la capacidad

El servidor TSM no tiene forma de notificar al nodo de archivado cuando la base de datos TSM o el almacenamiento multimedia de archivado gestionado por el servidor TSM está cerca de su capacidad. Esta situación se puede evitar gracias a la supervisión proactiva del servidor TSM.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Acerca de esta tarea**

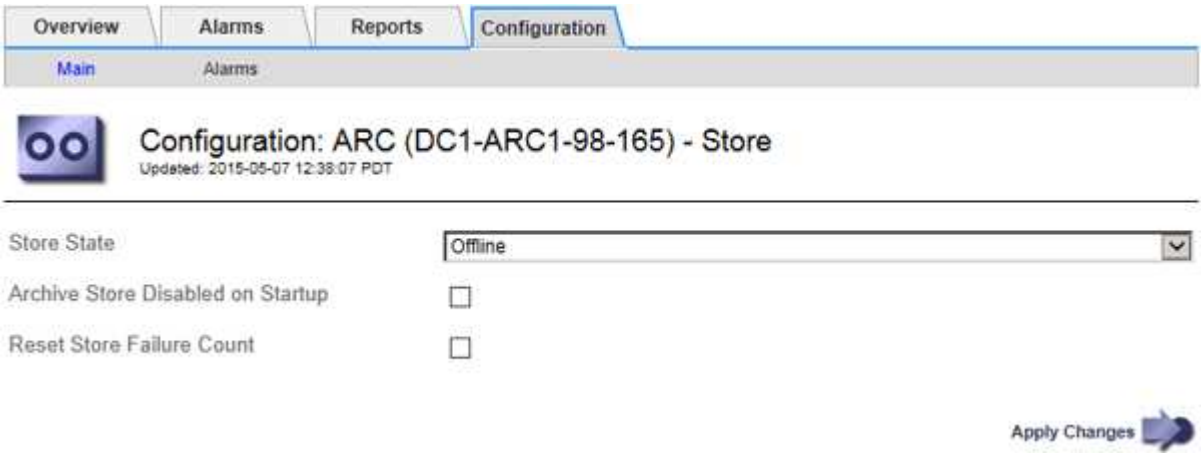
El nodo de archivado continúa aceptando datos de objetos para su transferencia al servidor TSM una vez que el servidor TSM deja de aceptar contenido nuevo. Este contenido no se puede escribir en medios gestionados por el servidor TSM. Si esto ocurre, se activa una alarma.

#### Impedir que el servicio ARC envíe contenido al servidor TSM

Para evitar que el servicio ARC envíe más contenido al servidor TSM, puede desconectar el nodo de archivado si desconecta el componente **ARC** > **Store**. Este procedimiento también puede ser útil para evitar alarmas cuando el servidor TSM no está disponible para tareas de mantenimiento.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.




4. Cambiar **Estado de tienda** a `Offline`.
5. Seleccione **almacén de archivos desactivado al inicio**.
6. Seleccione **aplicar cambios**.

#### Configure el nodo de archivado como de solo lectura si el middleware TSM alcanza la capacidad

Si el servidor de middleware TSM objetivo alcanza la capacidad, el nodo de archivado se puede optimizar para realizar únicamente recuperaciones.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.
4. Cambie el número máximo de sesiones de recuperación para que sea el mismo que el número de sesiones simultáneas enumeradas en el número de sesiones.
5. Cambie el número máximo de sesiones de almacenamiento a 0.

> No es necesario cambiar el número máximo de sesiones de almacén a 0 si el nodo de archivado es de sólo lectura. No se crearán sesiones de almacenamiento.

6. Seleccione **aplicar cambios**.

## Configure los ajustes de recuperación del nodo de archivado

Puede configurar los ajustes de recuperación de un nodo de archivado para establecer el

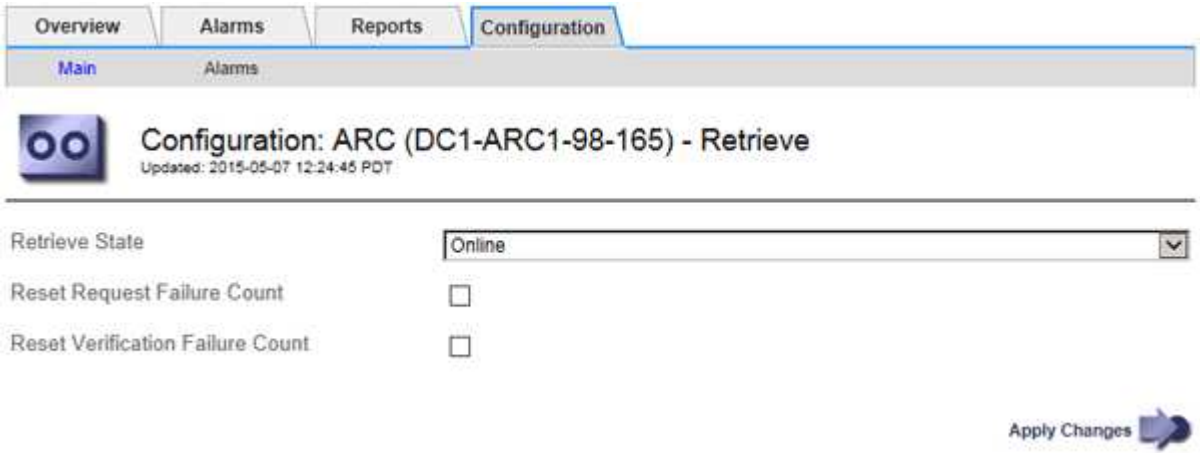
estado en línea o sin conexión, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **recuperar**.
3. Seleccione **Configuración** > **Principal**.




4. Modifique los siguientes ajustes, según sea necesario:
   - **Estado de recuperación**: Establezca el estado del componente en:
     - En línea: El nodo de cuadrícula está disponible para recuperar datos de objeto del dispositivo multimedia de archivado.
     - Offline: El nodo de grid no está disponible para recuperar los datos del objeto.
   - Restablecer recuento de fallos de solicitud: Seleccione la casilla de verificación para restablecer el contador en caso de fallos de solicitud. Esto se puede utilizar para borrar la alarma ARRF (fallos de solicitud).
   - Restablecer recuento de fallos de verificación: Seleccione la casilla de verificación para restablecer el contador en busca de fallos de verificación en los datos del objeto recuperado. Esto se puede utilizar para borrar la alarma ARRV (fallos de verificación).
5. Seleccione **aplicar cambios**.

## Configure la replicación del nodo de archivado

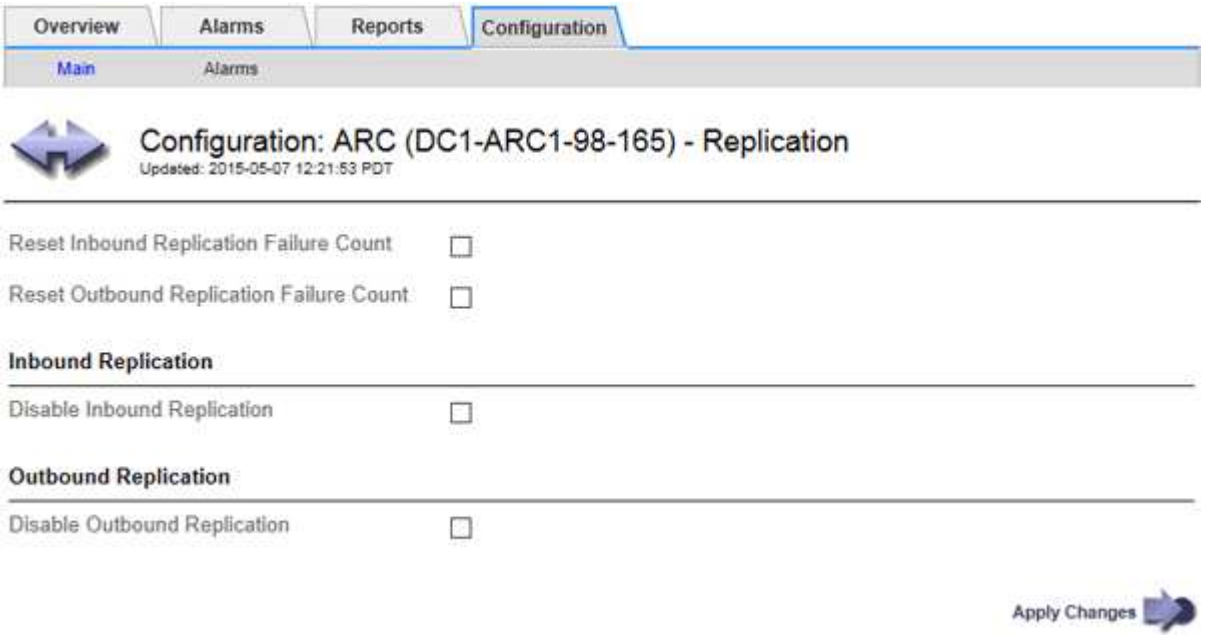
Puede configurar la configuración de replicación para un nodo de archivado y desactivar la replicación entrante y saliente, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

**Lo que necesitará**

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

**Pasos**

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Replication**.
3. Seleccione **Configuración** > **Principal**.




4. Modifique los siguientes ajustes, según sea necesario:
   - **Restablecer recuento de fallos de replicación entrante**: Seleccione para restablecer el contador en caso de fallos de replicación entrante. Esto se puede utilizar para borrar la alarma RIRF (replicaciones entrantes — fallidas).
   - **Reset Outbound Replication Failure Count**: Seleccione para restablecer el contador de fallos de replicación saliente. Esto se puede utilizar para borrar la alarma RORF (réplicas de salida — fallida).
   - **Desactivar replicación entrante**: Seleccione esta opción para desactivar la replicación entrante como parte de un procedimiento de mantenimiento o prueba. Dejar borrado durante el funcionamiento normal.

     Cuando la replicación entrante está deshabilitada, los datos de objeto se pueden recuperar desde el servicio ARC para su replicación a otras ubicaciones del sistema StorageGRID, pero los objetos no se pueden replicar en este servicio ARC desde otras ubicaciones del sistema. El servicio ARC es de sólo lectura-.

   - **Desactivar la replicación saliente**: Active la casilla de verificación para desactivar la replicación saliente (incluidas las solicitudes de contenido para las recuperaciones HTTP) como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal.

     Cuando la replicación saliente está deshabilitada, los datos de objeto se pueden copiar en este servicio ARC para cumplir con las reglas de ILM, pero los datos de objeto no se pueden recuperar del servicio ARC para copiarlos en otras ubicaciones del sistema StorageGRID. El servicio ARC es de sólo escritura-.

5. Seleccione **aplicar cambios**.

## Establezca alarmas personalizadas para el nodo de archivado

Debe establecer alarmas personalizadas para los atributos ARQL y ARRL que se utilizan para supervisar la velocidad y la eficacia de la recuperación de datos de objetos del sistema de almacenamiento de archivado por parte del nodo de archivado.

- ARQL: Longitud media de la cola. El tiempo medio, en microsegundos, que los datos de objetos se encuentran en cola para la recuperación del sistema de almacenamiento de archivado.
- ARRL: Promedio de latencia de solicitud. El tiempo medio, en microsegundos, que necesita el nodo de archivado para recuperar los datos de objetos del sistema de almacenamiento de archivado.

Los valores aceptables para estos atributos dependen de la configuración y el uso del sistema de almacenamiento de ficheros. (Vaya a **ARC** > **Retrieve** > **Overview** > **Main**.) Los valores establecidos para los tiempos de espera de las solicitudes y el número de sesiones disponibles para las solicitudes de recuperación tienen una influencia especial.

Una vez finalizada la integración, supervise las recuperaciones de datos de objetos del nodo de archivado para establecer valores para los tiempos de recuperación y las longitudes de cola normales. A continuación, cree alarmas personalizadas para ARQL y ARRL que se activarán si surge una condición de funcionamiento anormal. Consulte Supervisión y solución de problemas.

## Integrar Tivoli Storage Manager

### Configuración y funcionamiento del nodo de archivado

Su sistema StorageGRID gestiona el nodo de archivado como una ubicación en la que los objetos se almacenan de forma indefinida y siempre son accesibles.

Cuando se procesa un objeto, se crean copias en todas las ubicaciones necesarias, incluidos los nodos de archivado, según las reglas de gestión del ciclo de vida de la información (ILM) definidas para el sistema StorageGRID. El nodo de archivado actúa como cliente de un servidor TSM y las bibliotecas del cliente TSM se instalan en el nodo de archivado mediante el proceso de instalación del software StorageGRID. Los datos de objeto dirigidos al nodo de archivado para el almacenamiento se guardan directamente en el servidor TSM a medida que se reciben. El nodo de archivado no guarda los datos de objetos antes de guardarlos en el servidor TSM ni realiza la agregación de objetos. Sin embargo, el nodo de archivado puede enviar varias copias al servidor TSM en una única transacción cuando las tasas de datos lo garantizan.

Una vez que el nodo de archivado guarda los datos de objeto en el servidor TSM, el servidor TSM administra los datos de objeto con sus políticas de ciclo de vida/retención. Estas políticas de retención deben definirse para que sean compatibles con la operación del nodo de archivado. Es decir, los datos de objeto guardados por el nodo de archivado deben almacenarse indefinidamente y siempre deben ser accesibles desde el nodo de archivado, a menos que el nodo de archivado los elimine.

No hay conexión entre las reglas de ILM del sistema StorageGRID y las políticas de retención/ciclo de vida del servidor TSM. Cada uno de ellos funciona de forma independiente; sin embargo, a medida que se ingiere cada objeto en el sistema StorageGRID, puede asignarle una clase de gestión de TSM. Esta clase de gestión se pasa al servidor TSM junto con los datos de objetos. La asignación de diferentes clases de gestión a diferentes tipos de objetos permite configurar el servidor TSM para colocar los datos de objetos en distintos pools de almacenamiento o aplicar distintas políticas de migración o retención según sea necesario. Por ejemplo, los objetos identificados como backups de base de datos (contenido temporal que puede sobrescribirse con datos más nuevos) pueden tratarse de forma diferente a los datos de la aplicación (contenido fijo que debe conservarse indefinidamente).

El nodo de archivado se puede integrar con un servidor TSM nuevo o existente; no requiere un servidor TSM dedicado. Los servidores TSM se pueden compartir con otros clientes, siempre que el tamaño del servidor TSM se ajusta de forma adecuada a la carga máxima esperada. TSM debe instalarse en un servidor o máquina virtual independiente del nodo de archivado.

Es posible configurar más de un nodo de archivado para escribir en el mismo servidor TSM; sin embargo, esta configuración sólo se recomienda si los nodos de archivado escriben diferentes conjuntos de datos en el servidor TSM. No se recomienda configurar más de un nodo de archivado para escribir en el mismo servidor TSM cuando cada nodo de archivado escribe copias de los mismos datos de objeto en el archivo. En este último caso, ambas copias están sujetas a un único punto de error (el servidor TSM) para las copias redundantes de datos de objetos.

Los nodos de archivado no utilizan el componente de administración de almacenamiento jerárquico (HSM) de TSM.

**Prácticas recomendadas de configuración**

Cuando esté dimensionando y configurando su servidor TSM, debería aplicar las prácticas recomendadas para optimizar su funcionamiento con el nodo de archivado.

Al cambiar el tamaño y configurar el servidor TSM, debe tener en cuenta los siguientes factores:

- Como el nodo de archivado no agrega objetos antes de guardarlos en el servidor TSM, se debe ajustar el tamaño de la base de datos TSM para que contenga referencias a todos los objetos que se escribirán en el nodo de archivado.
- El software Archive Node no puede tolerar la latencia que implica la escritura de objetos directamente en la cinta u otro medio extraíble. Por lo tanto, el servidor TSM debe configurarse con un pool de almacenamiento en disco para el almacenamiento inicial de datos guardados por el nodo de archivado siempre que se utilice un medio extraíble.
- Debe configurar las políticas de retención de TSM para utilizar la retención basada en eventos-. El nodo de archivado no admite las políticas de retención de TSM basadas en la creación. Utilice los siguientes valores recomendados de retmin=0 y retver=0 en la directiva de retención (que indica que la retención comienza cuando el nodo de archivado activa un evento de retención y se conserva durante 0 días después de ese). Sin embargo, estos valores para retmin y retver son opcionales.

El pool de discos debe estar configurado para migrar datos al pool de cintas (es decir, el pool de cintas debe ser NXTSTGPOOL del pool de discos). El pool de cintas no debe configurarse como un pool de copias del pool de discos con escritura simultánea en ambos pools (es decir, el pool de cintas no puede ser un COPYSTGPOOL para el pool de discos). Para crear copias sin conexión de las cintas que contienen datos del nodo de archivado, configure el servidor TSM con un segundo grupo de cintas que sea un grupo de copias del grupo de cintas utilizado para los datos del nodo de archivado.

**Complete la configuración del nodo de archivado**

El nodo de archivado no funciona después de completar el proceso de instalación. Antes de que el sistema StorageGRID pueda guardar objetos en el nodo de archivado de TSM, debe completar la instalación y configuración del servidor TSM y configurar el nodo de archivado para que se comunique con el servidor TSM.

Consulte la siguiente documentación de IBM, según sea necesario, cuando prepare el servidor TSM para la integración con el nodo de archivado en un sistema StorageGRID:

- "Guía del usuario e instalación de los controladores de dispositivos de cinta de IBM"
- "Referencia de programación de controladores de dispositivo de cinta IBM"

#### Instale un nuevo servidor TSM

Puede integrar el nodo de archivado con un servidor TSM nuevo o existente. Si va a instalar un nuevo servidor TSM, siga las instrucciones de la documentación de TSM para completar la instalación.

Un nodo de archivado no se puede alojar conjuntamente con un servidor TSM.

#### Configure el servidor TSM

Esta sección incluye instrucciones de ejemplo para preparar un servidor TSM siguiendo las prácticas recomendadas de TSM.

Las siguientes instrucciones le guían en el proceso de:

- Definición de un pool de almacenamiento en disco y un pool de almacenamiento en cinta (si es necesario) en el servidor TSM
- Definición de una directiva de dominio que utiliza la clase de administración TSM para los datos guardados desde el nodo de archivado y registro de un nodo para utilizar esta directiva de dominio

Estas instrucciones se proporcionan sólo para su guía; no están diseñadas para sustituir la documentación de TSM ni para proporcionar instrucciones completas y completas adecuadas para todas las configuraciones. Un administrador de TSM debe proporcionar instrucciones específicas para la implementación que esté familiarizado con sus requisitos detallados y con el conjunto completo de documentación de TSM Server.

#### Definir los pools de almacenamiento en disco y cinta de TSM

El nodo de archivado escribe en un pool de almacenamiento en disco. Para archivar el contenido en cinta, debe configurar el grupo de almacenamiento en disco para mover el contenido a un grupo de almacenamiento en cinta.

##### Acerca de esta tarea

Para un servidor TSM, debe definir un pool de almacenamiento en cinta y un pool de almacenamiento en disco en Tivoli Storage Manager. Después de definir el pool de discos, cree un volumen de discos y asígnelo al pool de discos. -pool de cintas no es necesario si el servidor TSM utiliza únicamente el almacenamiento en disco.

Debe completar una serie de pasos en el servidor TSM para poder crear un grupo de almacenamiento de cinta. (Cree una biblioteca de cintas y al menos una unidad en la biblioteca de cintas. Defina una ruta de acceso desde el servidor a la biblioteca y desde el servidor a las unidades y, a continuación, defina una clase de dispositivo para las unidades.) Los detalles de estos pasos pueden variar en función de la configuración de hardware y los requisitos de almacenamiento del sitio. Para obtener más información, consulte la documentación de TSM.

El siguiente conjunto de instrucciones ilustra el proceso. Debe tener en cuenta que los requisitos de su sitio pueden variar en función de los requisitos de la implementación. Para obtener detalles de configuración e instrucciones, consulte la documentación de TSM.

Debe iniciar sesión en el servidor con privilegios administrativos y utilizar la herramienta dsmadmc para ejecutar los siguientes comandos.

**Pasos**

1. Cree una biblioteca de cintas.

   ```
   define library tapelibrary libtype=scsi
   ```

   Donde *tapelibrary* es un nombre arbitrario elegido para la biblioteca de cintas y el valor de `libtype` pueden variar en función del tipo de biblioteca de cintas.

2. Defina una ruta de acceso desde el servidor a la biblioteca de cintas.

   ```
   define path servername tapelibrary srctype=server desttype=library device=lib-devicename
   ```

   - *servername* Es el nombre del servidor TSM
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido
   - *lib-devicename* es el nombre del dispositivo de la biblioteca de cintas

3. Defina una unidad para la biblioteca.

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* es el nombre que desea especificar para la unidad
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido

     Se recomienda configurar una unidad o unidades adicionales, según la configuración de hardware. (Por ejemplo, si el servidor TSM está conectado a un switch Fibre Channel que tiene dos entradas de una biblioteca de cintas, quizás desee definir una unidad para cada entrada).

4. Defina una ruta desde el servidor hasta la unidad definida.

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - *drive-dname* es el nombre del dispositivo de la unidad
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido

     Repita el procedimiento para cada unidad que haya definido para la biblioteca de cintas, utilizando una unidad aparte *drivename* y.. *drive-dname* para cada unidad.

5. Defina una clase de dispositivo para las unidades.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - *DeviceClassName* es el nombre de la clase de dispositivo
   - *lto* es el tipo de unidad conectada al servidor
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido

- *tapetype* es el tipo de cinta; por ejemplo, triunter3

6. Agregue volúmenes de cinta al inventario de la biblioteca.

   `checkin libvolume` *tapelibrary*

   *tapelibrary* es el nombre de la biblioteca de cintas que ha definido.

7. Cree la agrupación de almacenamiento de cinta principal.

   `define stgpool` *SGWSTapePool DeviceClassName* `description=`*description collocate=filespace* `maxscratch=`*XX*

   - *SGWSTapePool* Es el nombre del pool de almacenamiento de cinta del nodo de archivado. Puede seleccionar cualquier nombre para la agrupación de almacenamiento de cinta (siempre que el nombre utilice las convenciones de sintaxis esperadas por el servidor TSM).
   - *DeviceClassName* es el nombre de la clase de dispositivo para la biblioteca de cintas.
   - *description* Es una descripción del grupo de almacenamiento que se puede mostrar en el servidor TSM mediante `query stgpool` comando. Por ejemplo: «'bloque de almacenamiento en cinta para el nodo de archivado».
   - *collocate=filespace* Especifica que el servidor TSM debe escribir objetos del mismo espacio en una única cinta.
   - `XX` es uno de los siguientes:
     - El número de cintas vacías de la biblioteca de cintas (en el caso de que el nodo de archivado sea la única aplicación que utiliza la biblioteca).
     - El número de cintas asignadas para su uso por el sistema StorageGRID (en aquellos casos en los que se comparte la biblioteca de cintas).

8. En un servidor TSM, cree un pool de almacenamiento en disco. En la consola administrativa del servidor TSM, introduzca

   `define stgpool` *SGWSDiskPool* `disk description=`*description* `maxsize=`*maximum_file_size nextstgpool=SGWSTapePool* `highmig=`*percent_high* `lowmig=`*percent_low*

   - *SGWSDiskPool* Es el nombre del pool de discos del nodo de archivado. Es posible seleccionar cualquier nombre para el pool de almacenamiento de discos (siempre que el nombre utilice las convenciones de sintaxis que espera el TSM).
   - *description* Es una descripción del grupo de almacenamiento que se puede mostrar en el servidor TSM mediante `query stgpool` comando. Por ejemplo, «depósito de almacenamiento de disco para el nodo de archivado».
   - *maximum_file_size* fuerza a que los objetos de mayor tamaño se escriban directamente en la cinta, en lugar de en la caché del pool de discos. Se recomienda establecer *maximum_file_size* A 10 GB.
   - *nextstgpool=SGWSTapePool* Hace referencia al pool de almacenamiento de disco al pool de almacenamiento de cinta definido para el nodo de archivado.
   - *percent_high* establece el valor en el que el pool de discos comienza a migrar su contenido al grupo de cintas. Se recomienda establecer *percent_high* 0 para que la migración de datos comience inmediatamente

- *percent_low* establece el valor en el que se detiene la migración al pool de cintas. Se recomienda establecer *percent_low* 0 para borrar el pool de discos.

9. En un servidor TSM, cree un volumen de disco (o volúmenes) y asígnelo al pool de discos.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* es el nombre del pool de discos.
   - *volume_name* es la ruta completa a la ubicación del volumen (por ejemplo, `/var/local/arc/stage6.dsm`) En el servidor TSM en el que escribe el contenido del pool de discos como preparación para la transferencia a cinta.
   - *size* Es el tamaño, en MB, del volumen de disco.

     Por ejemplo, para crear un único volumen de disco de forma que el contenido de un pool de discos llene una única cinta, configure el valor del tamaño en 200000 cuando el volumen de cinta tenga una capacidad de 200 GB.

     Sin embargo, es posible que sea conveniente crear varios volúmenes de disco de un tamaño menor, ya que el servidor TSM puede escribir en cada volumen del pool de discos. Por ejemplo, si el tamaño de la cinta es 250 GB, cree 25 volúmenes de disco con un tamaño de 10 GB (10000) cada uno.

   El servidor TSM preasigna espacio en el directorio para el volumen de disco. Esto puede tardar algún tiempo en completarse (más de tres horas para un volumen de disco de 200 GB).

#### Defina una directiva de dominio y registre un nodo

Debe definir una directiva de dominio que utilice la clase de administración TSM para los datos guardados desde el nodo de archivado y, a continuación, registrar un nodo para utilizar esta directiva de dominio.

> Los procesos de nodo de archivado pueden perder memoria si caduca la contraseña de cliente para el nodo de archivado en Tivoli Storage Manager (TSM). Asegúrese de que el servidor TSM esté configurado para que el nombre de usuario/contraseña del cliente para el nodo de archivado no caduque nunca.

Al registrar un nodo en el servidor TSM para el uso del nodo de archivado (o actualizar un nodo existente), debe especificar el número de puntos de montaje que el nodo puede utilizar para las operaciones de escritura especificando el parámetro MAXNUMMP en el comando REGISTER NODE. La cantidad de puntos de montaje suele ser equivalente al número de cabezales de unidad de cinta asignados al nodo de archivado. El número especificado para MAXNUMMP en el servidor TSM debe ser al menos tan grande como el valor establecido para **ARC** > **Target** > **Configuration** > **Main** > **Maximum Store Sessions** para el nodo de archivado, Que se establece en un valor de 0 o 1, ya que el nodo de archivado no admite sesiones de almacenamiento simultáneas.

El valor de MAXSESSIONS establecido para el servidor TSM controla el número máximo de sesiones que todas las aplicaciones cliente pueden abrir al servidor TSM. El valor de MAXSESSIONS especificado en el TSM debe ser al menos tan grande como el valor especificado para **ARC** > **Target** > **Configuration** > **Main** > **Number of Sessions** en el Grid Manager para el nodo de archivado. El nodo de archivado crea simultáneamente al menos una sesión por punto de montaje más un pequeño número (< 5) de sesiones adicionales.

El nodo TSM asignado al nodo de archivado utiliza una directiva de dominio personalizada `tsm-domain`. La

`tsm-domain` La política de dominios es una versión modificada de la política de dominio "tandard", configurada para escribir en cinta y con el destino de archivado configurado como base de almacenamiento del sistema StorageGRID (*`SGWSDiskPool`*).

> Debe iniciar sesión en el servidor TSM con privilegios administrativos y utilizar la herramienta dsmadmc para crear y activar la directiva de dominio.

**Crear y activar la directiva de dominio**

Debe crear una directiva de dominio y, a continuación, activarla para configurar el servidor TSM a fin de guardar los datos enviados desde el nodo de archivado.

**Pasos**

1. Crear una política de dominio.

   ```
   copy domain standard tsm-domain
   ```

2. Si no está utilizando una clase de administración existente, introduzca una de las siguientes opciones:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   *`default`* es la clase de administración predeterminada para la implementación.

3. Cree un copygroup en el pool de almacenamiento apropiado. Introducir (en una línea):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   *`default`* Es la clase de administración predeterminada para el nodo de archivado. Los valores de `retinit`, `retmin`, y. `retver` Se han elegido para reflejar el comportamiento de retención utilizado actualmente por el nodo de archivado

   > No configurado `retinit` para `retinit=create`. Ajuste `retinit=create` Bloquea el nodo de archivado para que no elimine contenido ya que los eventos de retención se utilizan para eliminar contenido del servidor TSM.

4. Asigne la clase de administración para que sea la predeterminada.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Establezca el nuevo conjunto de directivas como activo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignore la advertencia «'no backup copy group'» que aparece cuando se introduce el comando Activate.

6. Registre un nodo para utilizar el nuevo conjunto de directivas en el servidor TSM. En el servidor TSM, introduzca (en una línea):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   ```

`MAXNUMMP=number-of-sessions`

Arc-user y Arc-password son el mismo nombre de nodo de cliente y contraseña que se define en Archive Node, y el valor de MAXNUMMP se establece en el número de unidades de cinta reservadas para las sesiones de almacén de nodo de archivado.

> De forma predeterminada, al registrar un nodo se crea un ID de usuario administrativo con la autoridad del propietario del cliente, con la contraseña definida para el nodo.

# Migrar datos a StorageGRID

Puede migrar grandes cantidades de datos al sistema StorageGRID a la vez que utiliza el sistema StorageGRID para realizar operaciones diarias.

La siguiente sección es una guía para comprender y planificar una migración de grandes cantidades de datos al sistema StorageGRID. No es una guía general sobre la migración de datos y no incluye pasos detallados para realizar una migración. Siga las directrices y las instrucciones de esta sección para asegurarse de que la migración de datos al sistema StorageGRID se realice de forma eficiente sin interferir en las operaciones del día a día y de que el sistema StorageGRID gestione los datos migrados de forma adecuada.

## Confirmar la capacidad del sistema StorageGRID

Antes de migrar grandes cantidades de datos al sistema StorageGRID, confirme que el sistema StorageGRID tiene la capacidad de disco necesaria para gestionar el volumen previsto.

Si el sistema StorageGRID incluye un nodo de archivado y se ha guardado una copia de los objetos migrados en almacenamiento near-line (como la cinta), asegúrese de que el almacenamiento del nodo de archivado dispone de suficiente capacidad para el volumen previsto de datos migrados.

Como parte de la evaluación de la capacidad, observe el perfil de datos de los objetos que tiene pensado migrar y calcule la cantidad de capacidad de disco necesaria. Para obtener información detallada sobre cómo supervisar la capacidad del disco del sistema StorageGRID, consulte Gestione nodos de almacenamiento y.. Supervisión y solución de problemas.

## Determine la política de ILM para los datos migrados

La política de ILM del sistema StorageGRID determina cuántas copias se realizan, las ubicaciones a las que se almacenan las copias y durante el tiempo que se conservan estas copias. Una política de ILM consta de un conjunto de reglas de ILM que describen cómo filtrar objetos y gestionar datos de objetos a lo largo del tiempo.

En función del uso que se haga de los datos migrados y de los requisitos relativos a los datos migrados, es posible que desee definir reglas de ILM únicas para los datos migrados que difieren de las reglas de ILM que se usan para las operaciones cotidianas. Por ejemplo, si hay requisitos normativos diferentes para la gestión diaria de los datos que para los datos que se incluyen en la migración, es posible que desee usar un número distinto de copias de los datos migrados en un grado de almacenamiento diferente.

Puede configurar reglas que se apliquen exclusivamente a los datos migrados si es posible distinguir de forma única entre los datos migrados y los datos de objetos guardados de las operaciones diarias.

Si puede distinguir de forma fiable entre los tipos de datos mediante uno de los criterios de metadatos, puede usar estos criterios para definir una regla de ILM que solo se aplica a los datos migrados.

Antes de iniciar la migración de datos, asegúrese de comprender la política de gestión del ciclo de vida de la información del sistema StorageGRID y cómo se aplicará a los datos migrados, y de haber realizado y probado cualquier cambio en la política de ILM. Consulte Gestión de objetos con ILM.

> Una política de ILM que se haya especificado incorrectamente puede provocar una pérdida de datos irrecuperable. Revise detenidamente todos los cambios realizados en una política de ILM antes de activarla para asegurarse de que la política funcione como se desee.

## Impacto de la migración en las operaciones

Un sistema StorageGRID está diseñado para proporcionar un funcionamiento eficiente para el almacenamiento y la recuperación de objetos, y proporcionar una protección excelente frente a la pérdida de datos mediante la creación sin problemas de copias redundantes de datos de objetos y metadatos.

Sin embargo, la migración de datos debe gestionarse con cuidado según las instrucciones de este capítulo para evitar que afecte a las operaciones diarias del sistema o, en casos extremos, colocarse datos en riesgo de pérdida en caso de fallo en el sistema StorageGRID.

Migración de grandes cantidades de datos coloca una carga adicional en el sistema. Cuando el sistema StorageGRID está cargado en gran medida, responde más lentamente a las solicitudes de almacenamiento y recuperación de objetos. Esto puede interferir con las solicitudes de almacenamiento y recuperación que son integrales a las operaciones diarias. La migración también puede ocasionar otros problemas operativos. Por ejemplo, cuando un nodo de almacenamiento se está agotando la capacidad, la carga intermitente pesada debido a la ingesta en lote puede provocar que el nodo de almacenamiento se cicle entre las notificaciones de solo lectura y de lectura y escritura.

Si la carga pesada persiste, se pueden desarrollar colas para diversas operaciones que el sistema StorageGRID debe realizar para garantizar la redundancia total de los datos de objetos y los metadatos.

La migración de datos debe gestionarse con cuidado según las directrices que se indican en este documento para garantizar el funcionamiento seguro y eficiente del sistema StorageGRID durante la migración. Al migrar datos, procese objetos en lotes o acelerador continuamente del procesamiento. A continuación, supervise de forma continua el sistema StorageGRID para garantizar que no se superen los distintos valores de atributo.

## Programe y supervise la migración de datos

La migración de datos debe programarse y supervisarse según sea necesario para garantizar que los datos se coloquen según la política de ILM en el plazo estipulado.

### Programar la migración de datos

Evite migrar datos durante las horas operativas del núcleo. Limite la migración de datos a noches, fines de semana y otras veces cuando el uso del sistema sea bajo.

De ser posible, no programe la migración de datos durante periodos de alta actividad. Sin embargo, si no es práctico evitar completamente el período de alta actividad, es seguro continuar siempre que usted supervise de cerca los atributos relevantes y tome medidas si exceden los valores aceptables.

### Supervisar la migración de datos

En esta tabla, se enumeran los atributos que debe supervisar durante la migración de datos y los problemas que representan.

Si utiliza directivas de clasificación de tráfico con límites de tasa para acelerar el procesamiento, puede supervisar la tasa observada junto con las estadísticas descritas en la siguiente tabla y reducir los límites si es necesario.

| Supervisar | Descripción |
|---|---|
| Número de objetos que están a la espera de la evaluación de ILM | 1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.<br>2. Seleccione ***deployment*** > **Descripción general** > **Principal**.<br>3. En la sección ILM Activity, supervise el número de objetos que se muestran para los siguientes atributos:<br>◦ **Esperando - todos (XQUZ)**: El número total de objetos que esperan la evaluación de ILM.<br>◦ **Esperando - Cliente (XCQZ)**: El número total de objetos que esperan la evaluación de ILM de las operaciones cliente (por ejemplo, ingesta).<br>4. Si el número de objetos mostrado para cualquiera de estos atributos supera 100,000, acelere la tasa de procesamiento de objetos para reducir la carga en el sistema StorageGRID. |
| Capacidad de almacenamiento específica del sistema de archivado | Si la normativa de gestión del ciclo de vida de la información guarda una copia de los datos migrados a un sistema de almacenamiento de archivado dirigido (cinta o cloud), supervise la capacidad del sistema de almacenamiento de archivado dirigido para garantizar que los datos migrados disponen de capacidad suficiente. |
| **Nodo de archivo** > **ARC** > **Tienda** | Si se activa una alarma para el atributo **fallos de almacenamiento (ARVF)**, es posible que el sistema de almacenamiento de archivado dirigido haya alcanzado la capacidad. Compruebe el sistema de almacenamiento de archivos de destino y resuelva cualquier problema que haya activado una alarma. |

## Información de copyright

Copyright © 2024 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.