Administre StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Administre StorageGRID

Aprenda a configurar el sistema StorageGRID.

- "Administración de un sistema StorageGRID"
- "Controlando el acceso del administrador a StorageGRID"
- "Configuración de servidores de gestión de claves"
- "Gestión de inquilinos"
- "Configurar las conexiones de clientes S3 y Swift"
- "Gestionar redes y conexiones StorageGRID"
- "Configurando AutoSupport"
- "Gestión de nodos de almacenamiento"
- "Gestión de los nodos de administrador"
- "Gestión de los nodos de archivado"
- "Migración de datos a StorageGRID"

Administración de un sistema StorageGRID

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

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.

> Se han movido las instrucciones de gestión de objetos con reglas y políticas de gestión de ciclo de vida de la información (ILM) a."Gestión de objetos con ILM".

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

Lo que necesitará

- 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.

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	87
Microsoft Edge	87

Navegador Web	Versión mínima admitida
Mozilla Firefox	84

Debe establecer la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Iniciando 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

- Debe tener sus credenciales de inicio de sesión.
- Debe tener la dirección URL de Grid Manager.
- Debe utilizar un navegador web compatible.
- Las cookies deben estar habilitadas en su navegador web.
- Debe tener 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 principal preferido del grupo, de manera que al acceder al Administrador de grid, tenga acceso al 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:

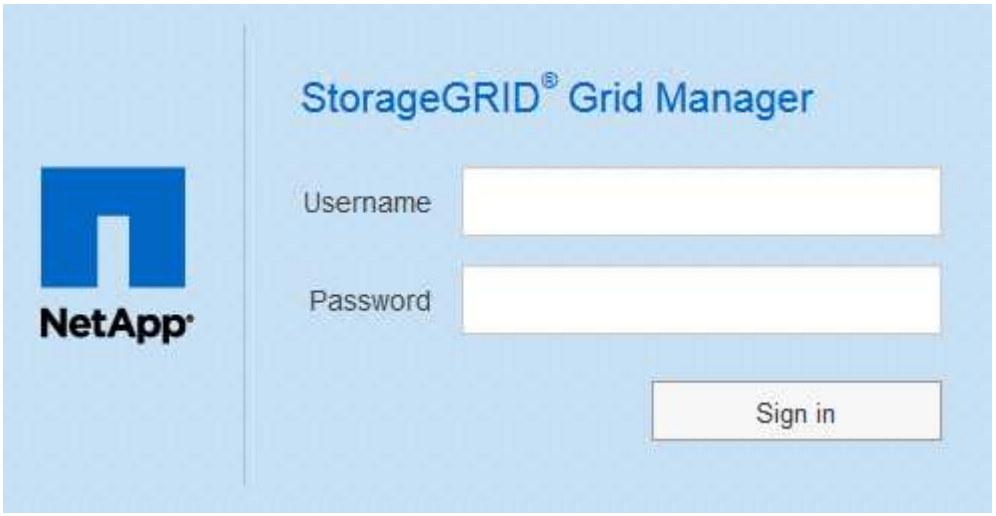
   `https://FQDN_or_Admin_Node_IP/`

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:

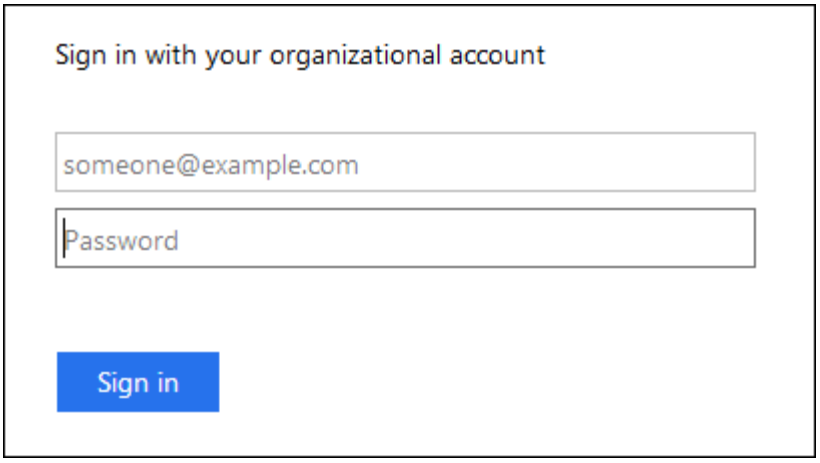
`https://FQDN_or_Admin_Node_IP:port/`

3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
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. Haga clic en **Iniciar sesión**.



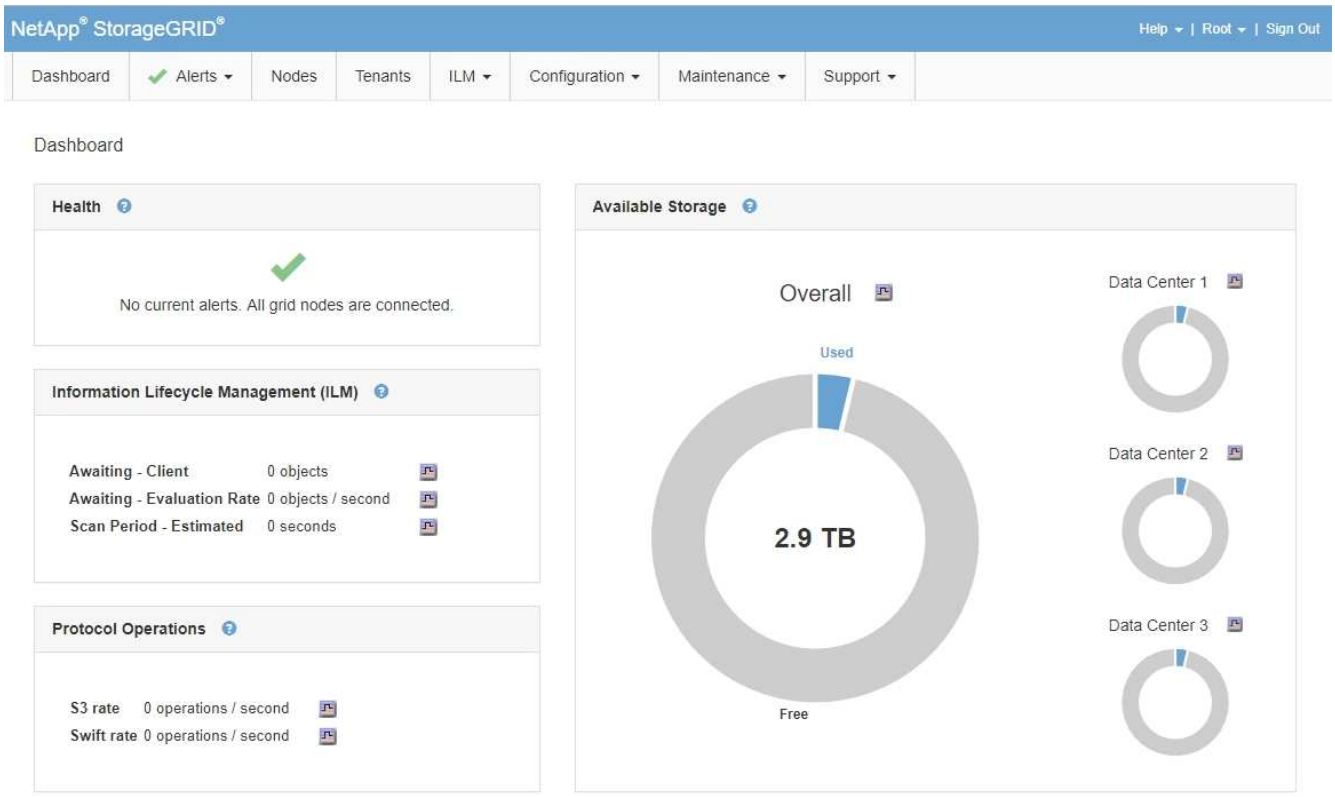
   - Si SSO está habilitado para el sistema StorageGRID y esta es la primera vez que accede a la URL en este navegador:
     i. Haga clic en **Iniciar sesión**. Puede dejar el campo ID de cuenta en blanco.

     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 haga clic en **Iniciar sesión**.
     - Seleccione **Grid Manager** si aparece en la lista de cuentas recientes y haga clic en **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 «'visualización del panel» en las instrucciones de supervisión y solución de problemas de StorageGRID.



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. b. Introduzca su nombre de usuario y contraseña para el administrador de grid. c. Haga clic en **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. 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. **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

"Requisitos del navegador web"

"Controlar el acceso mediante firewalls"

"Configuración de certificados de servidor"

"Configuración del inicio de sesión único"

"Gestión de los grupos de administración"

"Gestionar grupos de alta disponibilidad"

"Usar una cuenta de inquilino"

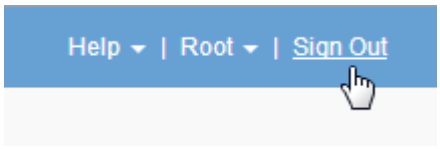
"Solución de problemas de monitor"

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



2. Haga clic en **Cerrar sesión**.

Opción	Descripción
SSO no en uso	Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión de Grid Manager. **Nota:** Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo.

Opción	Descripción
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. **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

"Configuración del inicio de sesión único"

"Usar una cuenta de inquilino"

Cambiando la contraseña

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

Lo que necesitará

Debe iniciar sesión en Grid Manager mediante un explorador 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. Haga clic en **Guardar**.

Cambiar la clave de acceso de 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. También se requiere la contraseña para descargar las copias de seguridad del paquete de recuperación que incluyen la información de topología de la cuadrícula y las claves de cifrado del sistema StorageGRID.

Lo que necesitará

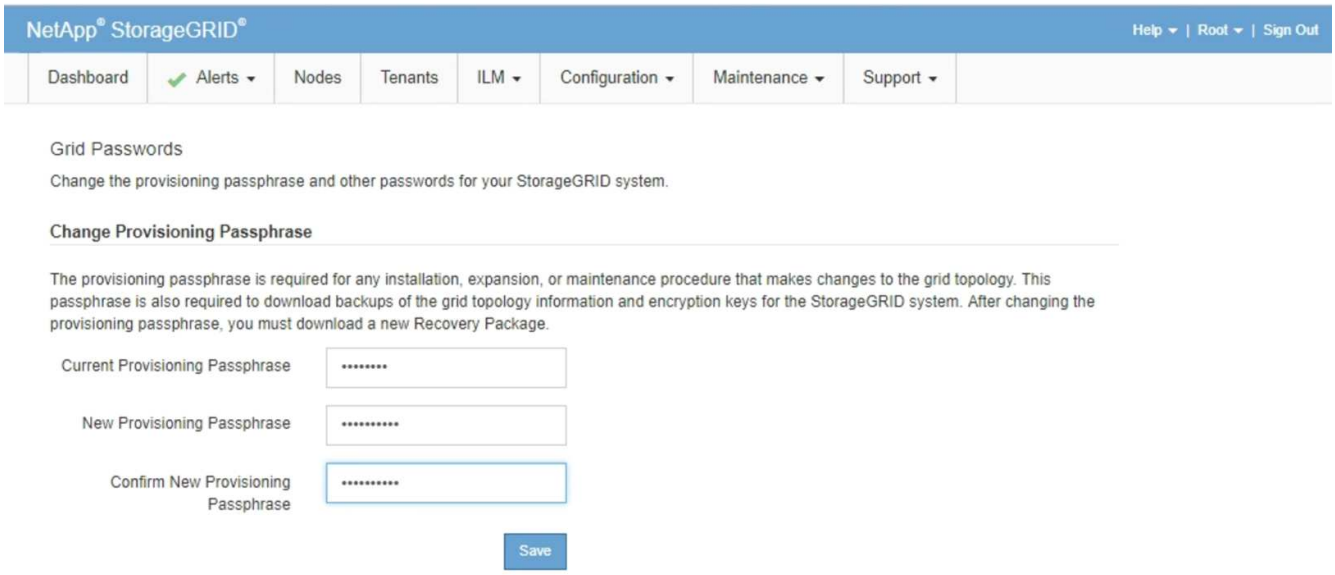
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento y para descargar el 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**.

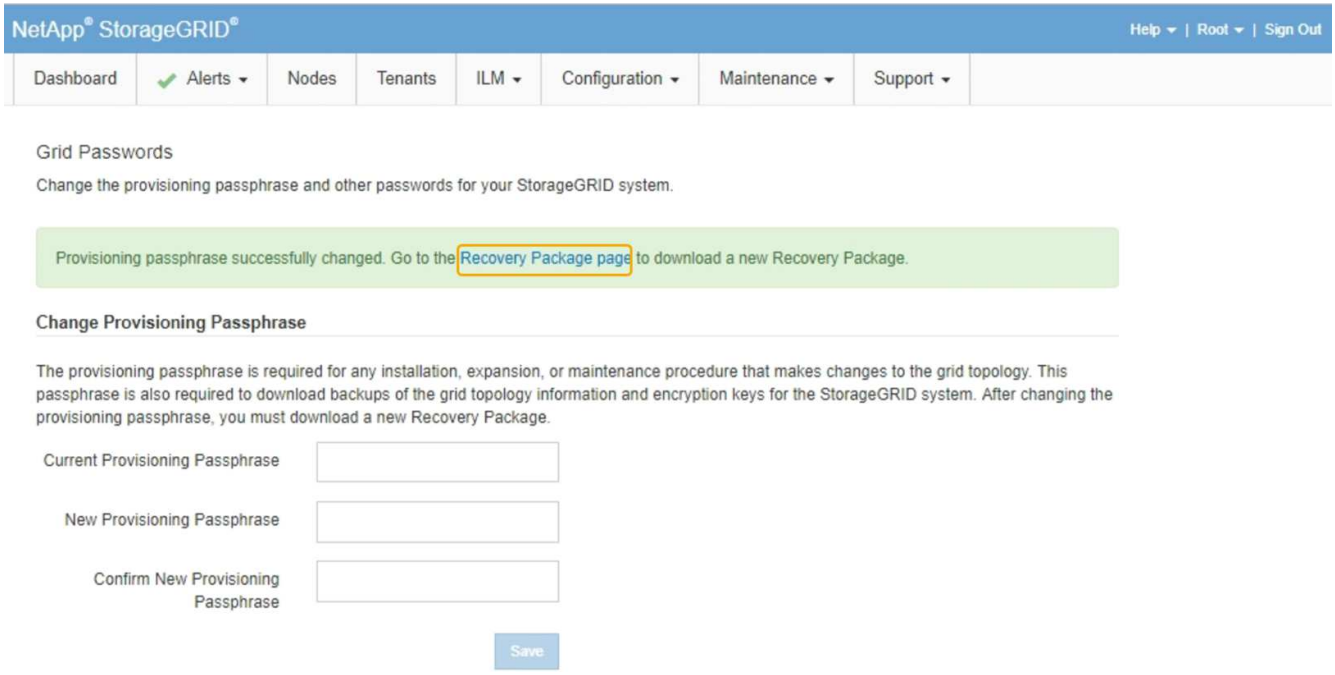


2. Introduzca la clave de acceso de aprovisionamiento actual.
3. Introduzca el nuevo pasepartido.la frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.

> Almacene la nueva clave de acceso de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.

4. Vuelva a introducir la nueva contraseña y haga clic en **Guardar**.

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



5. Seleccione el enlace **página del paquete de recuperación** que se encuentra dentro del banner de éxito.
6. Descargue el nuevo paquete de recuperación desde Grid Manager. Seleccione **Mantenimiento** > **paquete de recuperación** e introduzca la nueva contraseña de aprovisionamiento.

> 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.

Cambiar 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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 hiciera clic en **Cerrar sesión** manualmente. El usuario debe volver a introducir sus credenciales de SSO para volver a acceder a StorageGRID.

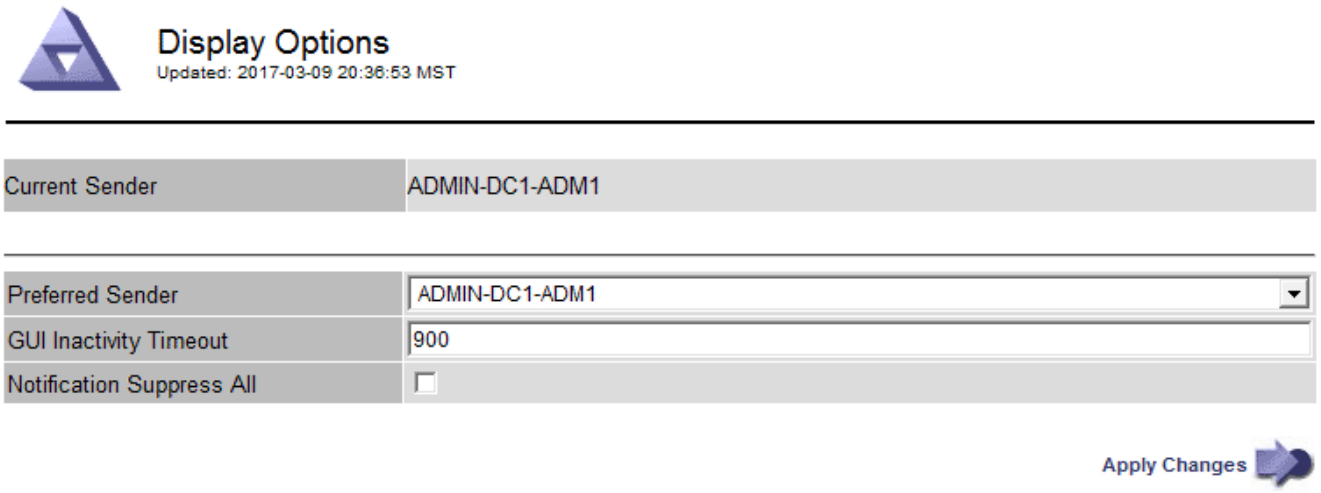
El tiempo de espera de la sesión de usuario también puede controlarse por lo siguiente:

- 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** > **Configuración del 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. Haga clic en **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.

Información relacionada

"Cómo funciona el inicio de sesión único"

"Usar una cuenta de inquilino"

Ver información de licencias 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

- Debe iniciar sesión en Grid Manager mediante un explorador 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, haga clic en el icono Estado de la licencia o en 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.

Actualizar 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

- Debe tener un nuevo archivo de licencia para aplicar al sistema StorageGRID.
- Debe tener permisos de acceso específicos.
- Debe tener 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. Haga clic en **examinar**.
4. En el cuadro de diálogo Abrir, busque y seleccione el nuevo archivo de licencia (`.txt`) Y haga clic en **Abrir**.

   El nuevo archivo de licencia se valida y muestra.

5. Haga clic en **Guardar**.

Uso de 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.

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.

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 detalles, consulte la información acerca del uso de cuentas de inquilino.
- `/private`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados. Estas API están pensadas para el uso interno únicamente y no se documentan públicamente. Estas API también están sujetas a cambios sin previo aviso.

Información relacionada

"Usar una cuenta de inquilino"

"Prometheus: Aspectos básicos de las consultas"

Operaciones de API de gestión de grid

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

- **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.

- **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.

Emitir solicitudes API

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

Lo que necesitará

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

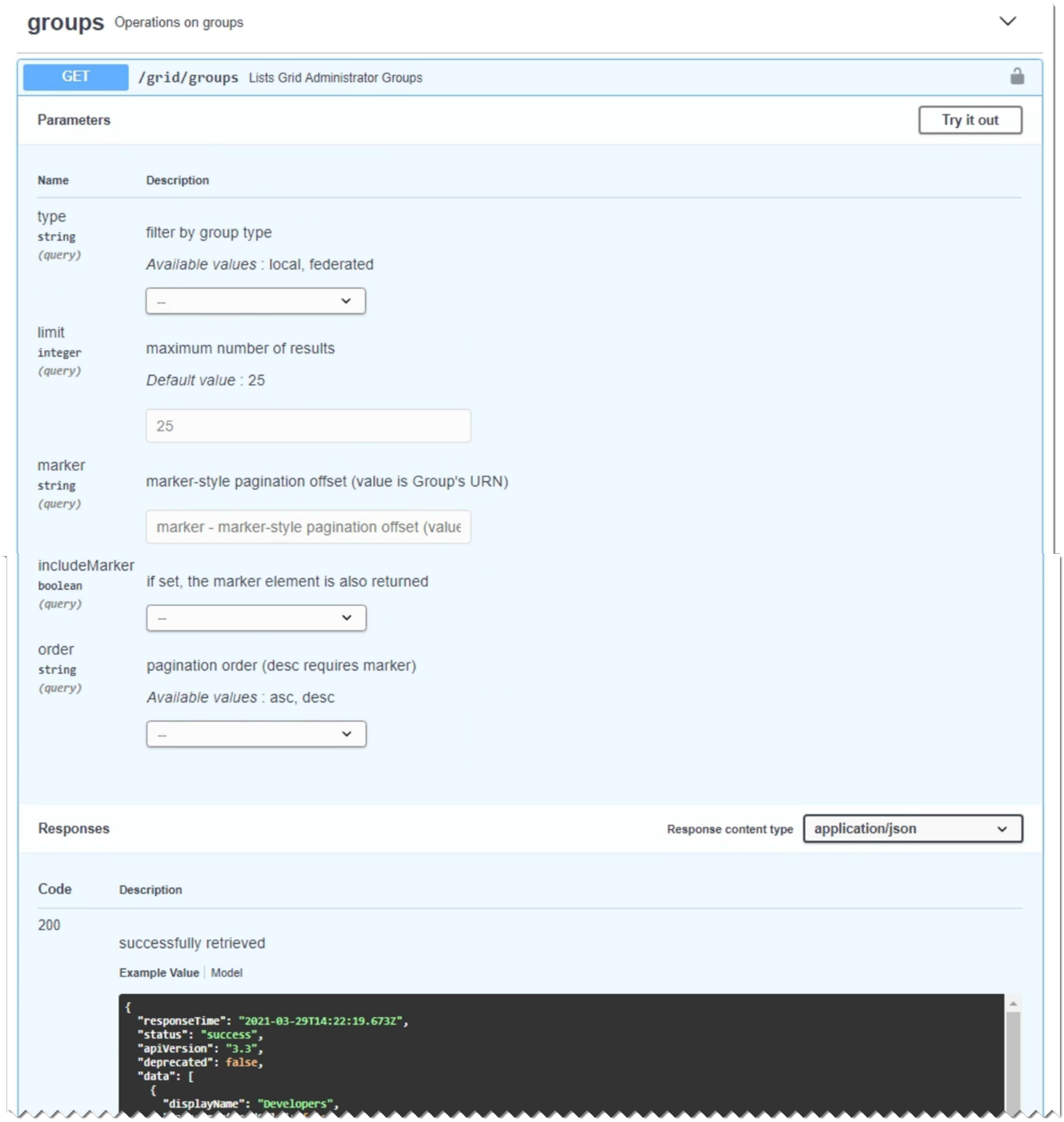
> Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. Seleccione **Ayuda** > **Documentación de API** en el encabezado de Grid Manager.
2. Seleccione la operación deseada.

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

3. 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.



4. 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.
5. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede hacer clic en **Modelo** para conocer los requisitos de cada campo.
6. Haga clic en **probar**.
7. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.

8. Haga clic en **Ejecutar**.
9. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

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"
```

Determinar 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
  ]
}
```

Especificar una versión de 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.

Usar la API si está activado el inicio de sesión único

Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, no puede utilizar las solicitudes estándar de la API de autenticación para iniciar sesión y cerrar sesión en la API de administración de grid o en la API de gestión de inquilinos.

Iniciar 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 obtener un token de autenticación de AD FS que sea válido para la API de gestión de grid o la API de gestión de inquilinos.

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: No se ha encontrado una confirmación de suscripción válida en esta respuesta.

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

Si tiene un problema de codificación URL, es posible que aparezca el error: Versión de SAML no compatible.

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 nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - Si desea acceder a la API de gestión de inquilinos, introduzca el ID de cuenta de inquilino.

   +

   ```
   python3 /tmp/storagegrid-ssoauth.py
   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=For
msAuthentication" --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.

Cerrar sesión en la API si se habilita el inicio de sesión único

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.

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=fZDNboMwEI
RfhZ...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
```

Usar certificados de seguridad StorageGRID

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).

Una entidad de certificación externa (CA) puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de su empresa. StorageGRID también incluye una entidad de certificación (CA) integrada que genera certificados de CA internos durante la instalación del sistema. Estos certificados de CA internos se utilizan, de forma predeterminada, para proteger el tráfico StorageGRID interno. Si bien se pueden utilizar los certificados de CA internos para un entorno que no sea de producción, la práctica recomendada para un entorno de producción es usar 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 las directrices de endurecimiento del sistema para los certificados de servidor.

  "Endurecimiento del sistema"

- 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.

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de cliente de administrador	Cliente	Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos. • Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID. • Permite una supervisión segura de StorageGRID mediante herramientas externas.	**Configuración** > **Control de acceso** > **certificados de cliente**	"Configurar certificados de cliente de administrador"
Certificado de federación de identidades	Servidor	Autentica la conexión entre StorageGRID y un Active Directory, OpenLDAP o Oracle Directory Server externo.used for Identity federation, que permite que los grupos y usuarios de administración sean administrados por un sistema externo.	**Configuración** > **Control de acceso** > **Federación de identidades**	"Mediante la federación de identidades"
Certificado de inicio de sesión único (SSO)	Servidor	Autentica la conexión entre Active Directory Federation Services (AD FS) y StorageGRID que se utiliza para solicitudes de inicio de sesión único (SSO).	**Configuración** > **Control de acceso** > **Inicio de sesión único**	"Configuración del inicio de sesión único"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de servidor de gestión de claves (KMS)	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** > **Configuración del sistema** > **servidor de administración de claves**	"Adición de un servidor de gestión de claves (KMS)"
Certificado de notificación de alertas por correo electrónico	Servidor y cliente	Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo SMTP requiere certificados de cliente para la autenticación.	**Alertas** > **Configuración de correo electrónico**	"Solución de problemas de monitor"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de punto final de equilibrador de carga	Servidor	Autentica la conexión entre clientes S3 o Swift y el servicio StorageGRID Load Balancer en nodos de puerta de enlace o nodos de administrador. Se carga o se genera un certificado de equilibrador de carga cuando se configura 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. **Nota:** el certificado de equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.	**Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**	• "Configuración de los extremos del equilibrador de carga" • Creación de un extremo de equilibrador de carga para FabricPool "Configure StorageGRID para FabricPool"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de servidor de interfaz de gestión	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. Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos. Puede usar el certificado de CA interno o cargar un certificado personalizado.	**Configuración** > **Configuración de red** > **certificados de servidor**	• "Configuración de certificados de servidor" • "Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos"
Certificado de extremo de Cloud Storage Pool	Servidor	Autentica la conexión de Cloud Storage Pool de StorageGRID a una ubicación de almacenamiento externa (como S3 Glacier o almacenamiento blob de Microsoft Azure). Se necesita un certificado diferente para cada tipo de proveedor de cloud.	**ILM** > **agrupaciones de almacenamiento**	"Gestión de objetos con ILM"
Certificado de extremo de servicios de plataforma	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**	"Usar una cuenta de inquilino"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de servidor de extremo de servicio de Object Storage API	Servidor	Autentica conexiones de cliente Swift o S3 seguras con el servicio LDR (Local Distribution Router, LDR) en un nodo de almacenamiento o con el servicio Connection Load Balancer (CLB) obsoleto en un nodo de puerta de enlace.	**Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**	"Configuración de un certificado de servidor personalizado para las conexiones al nodo de almacenamiento o al servicio CLB"

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.

Controlando el acceso del administrador a StorageGRID

Puede controlar el acceso de administrador al sistema StorageGRID abriendo o cerrando puertos de firewall, gestionando grupos de administradores y usuarios, configurando el inicio de sesión único (SSO) y proporcionando certificados de cliente para permitir un acceso externo seguro a las métricas de StorageGRID.

- "Controlar el acceso mediante firewalls"
- "Mediante la federación de identidades"
- "Gestión de los grupos de administración"
- "Gestión de usuarios locales"
- "Uso del inicio de sesión único (SSO) para StorageGRID"
- "Configurar certificados de cliente de administrador"

Controlar el acceso mediante firewalls

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

Control del acceso en el 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. **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. • 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. • Se rechazarán las solicitudes de contenido interno.

Puerto	Descripción	Si el puerto está abierto…
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. • 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. • 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

"Iniciando sesión en Grid Manager"

"Creación de una cuenta de inquilino si StorageGRID no utiliza SSO"

"Resumen: Direcciones IP y puertos para conexiones cliente"

"Administración de redes de clientes que no son de confianza"

"Instalar Ubuntu o Debian"

"Instale VMware"

"Instale Red Hat Enterprise Linux o CentOS"

Mediante 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.

Configurando la federación de identidades

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

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Si planea habilitar el inicio de sesión único (SSO), debe utilizar Active Directory como el origen de identidad federado y AD FS como proveedor de identidades. Véase «'requisitos para el uso de la entrada única».
- Debe utilizar Active Directory, OpenLDAP o Oracle Directory Server como proveedor de identidades.

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

- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3.

Acerca de esta tarea

Debe configurar un origen de identidad para el Gestor de grid si desea importar los siguientes tipos de grupos federados:

- Grupos administrativos. 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.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Federación de identidades**.
2. Seleccione **Activar federación de identidades**.

   Aparecen los campos para configurar el servidor LDAP.

3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.

   Puede seleccionar **Active Directory**, **OpenLDAP** o **otros**.

   Si selecciona **OpenLDAP**, debe configurar el servidor OpenLDAP. Consulte las directrices para configurar un servidor OpenLDAP.

   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 .
   - **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. En la sección Configure LDAP Server, introduzca la información sobre el servidor LDAP y las conexiones de red necesarias.
   - **Hostname**: El nombre de host del servidor 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`

   - **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.

6. En la sección **Seguridad de la capa de transporte (TLS)**, seleccione una configuración de seguridad.
   - **Usar STARTTLS (recomendado)**: Usar STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada.
   - **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Esta opción es compatible por motivos de compatibilidad.
   - **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido.

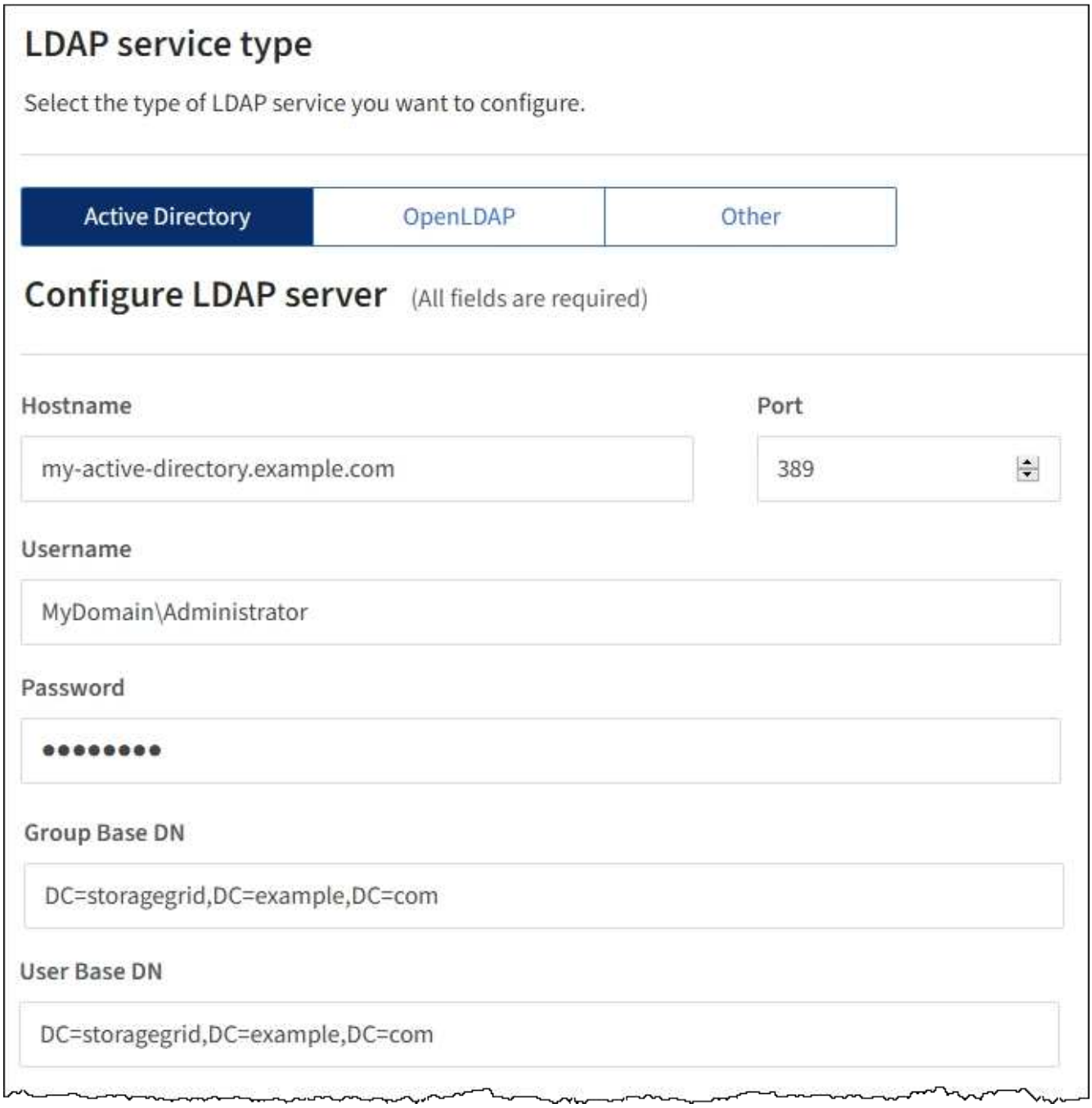
     El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado 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.
8. Opcionalmente, seleccione **probar conexión** para validar la configuración de conexión para el servidor LDAP.

   Si la conexión es válida, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.
9. Si la conexión es válida, seleccione **Guardar**.

   La siguiente captura de pantalla muestra valores de configuración de ejemplo para un servidor LDAP que utiliza Active Directory.



Información relacionada

"Cifrados compatibles para conexiones TLS salientes"

"Requisitos para usar el inicio de sesión único"

"Crear una cuenta de inquilino"

"Usar una cuenta de inquilino"

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.

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 en la Guía del administrador para OpenLDAP.

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 revertidos en la Guía del administrador para OpenLDAP.

Información relacionada

"Documentación de OpenLDAP: Guía del administrador de la versión 2.4"

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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- El origen de identidades debe estar activado.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Federación de identidades**.

   Aparece la página Federación de identidades. El botón **Sincronizar** se encuentra en la parte inferior de la página.

2. Haga clic en **Sincronizar**.

   Un mensaje de confirmación indica que la sincronización se ha iniciado correctamente. 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.

Desactivar 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.

Lo que necesitará

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

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.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Federación de identidades**.
2. Desactive la casilla de verificación **Activar Federación de identidades**.
3. Haga clic en **Guardar**.

Información relacionada

"Desactivar el inicio de sesión único"

Gestión de los grupos de administración

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.

Creando grupos de administradores

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.

Lo que necesitará

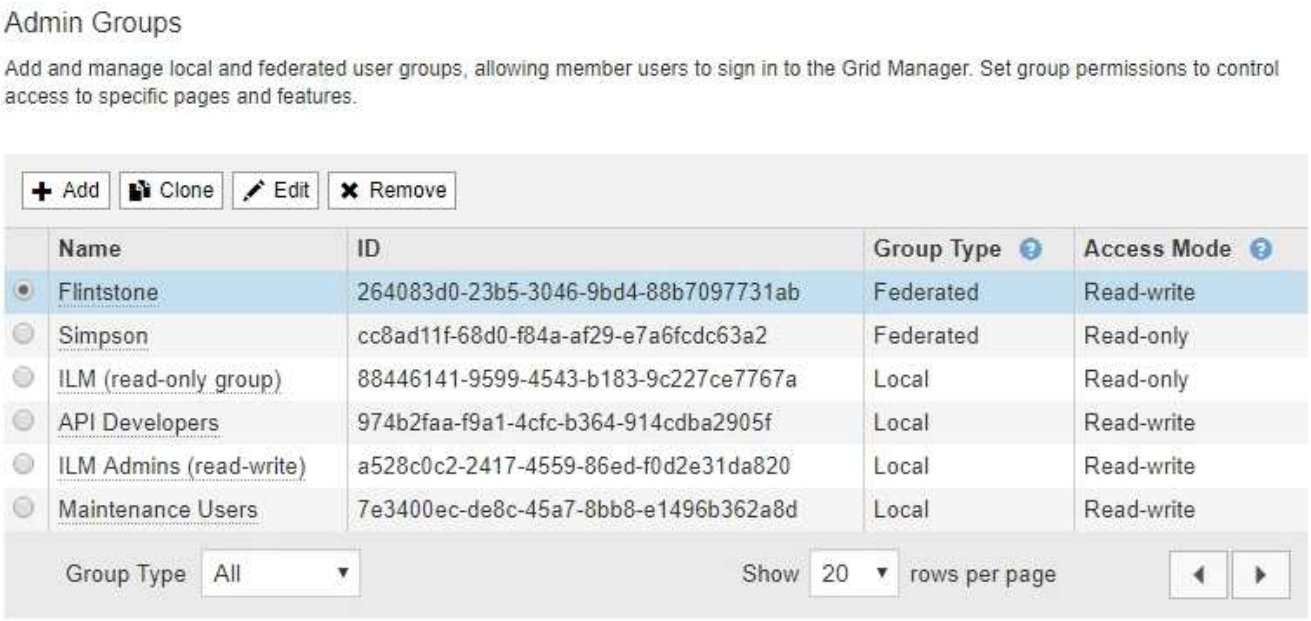
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

- Debe tener permisos de acceso específicos.
- Si planea importar un grupo federado, debe haber configurado la federación de identidades y el grupo federado debe existir ya en el origen de identidades configurado.

Pasos

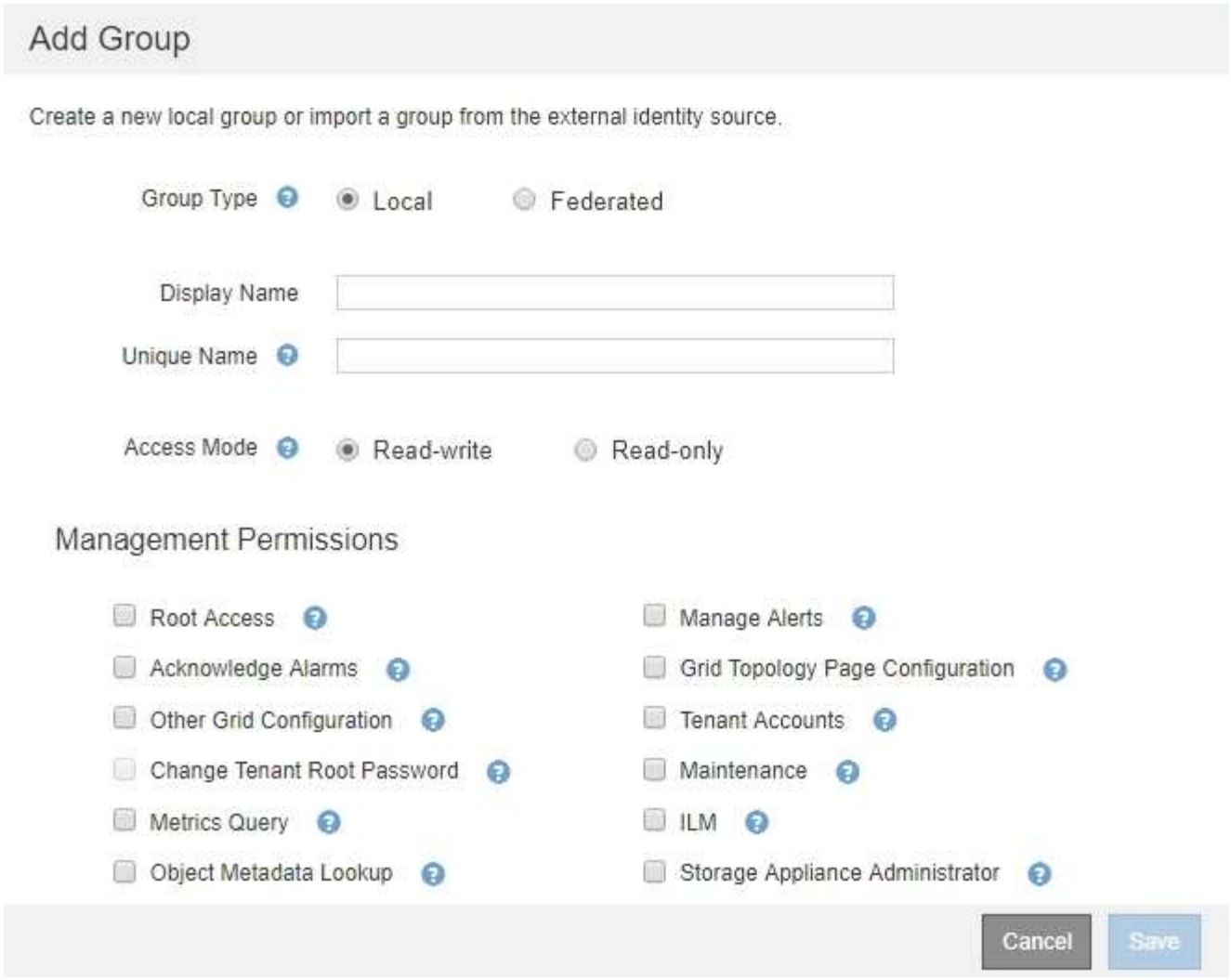
1. Seleccione **Configuración** > **Control de acceso** > **grupos de administración**.

   Se mostrará la página Admin Groups, donde se enumeran los grupos de administración existentes.



2. Seleccione **Agregar**.

   Aparece el cuadro de diálogo Agregar grupo.



3. En Tipo de grupo, seleccione **local** si desea crear un grupo que sólo se utilizará dentro de StorageGRID, o seleccione **federado** si desea importar un grupo desde el origen de identidades.
4. Si ha seleccionado **local**, introduzca un nombre para mostrar para el grupo. El nombre para mostrar es el nombre que aparece en el Gestor de cuadrícula. Por ejemplo, «usuarios de mantenimiento» o «Administradores de ILM».
5. Introduzca un nombre único para el grupo.
   - **Local**: Introduzca el nombre único que desee. Por ejemplo, «'Administradores de ILM».
   - **Federado**: Introduzca el nombre del grupo exactamente como aparece en el origen de identidad configurado.
6. 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.

7. Seleccione uno o más permisos de gestión.

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

8. Seleccione **Guardar**.

   Se creará el nuevo grupo. Si se trata de un grupo local, ahora puede agregar uno o más usuarios. Si se trata de un grupo federado, el origen de identidades gestiona los usuarios que pertenecen al grupo.

Información relacionada

"Gestión de usuarios locales"

Permisos de grupo de administradores

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 que pertenezcan a ese grupo no podrán iniciar sesión en Grid Manager.

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

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.

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.

Reconocer alarmas (sistema heredado)

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.

Configuración de la página de topología de la cuadrícula

Este permiso permite acceder a las siguientes opciones de menú:

- Fichas de configuración disponibles en las páginas de **Soporte** > **Herramientas** > **Topología de cuadrícula**.
- **Restablecer recuentos de eventos** enlace en la ficha **nodos** > **Eventos**.

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.

- **Alarmas** (sistema heredado):
  - Alarmas globales
  - Configuración de correo electrónico heredado
- **ILM**:
  - Pools de almacenamiento
  - Grados de almacenamiento
- **Configuración** > **Configuración de red**
  - Coste del enlace
- **Configuración** > **Configuración del sistema**:
  - Opciones de visualización
  - Opciones de cuadrícula
  - Opciones de almacenamiento
- **Configuración** > **Supervisión**:
  - Eventos
- **Soporte**:
  - AutoSupport

Cuentas de inquilino

Este permiso permite acceder a la página **arrendatarios** > **Cuentas de inquilino**.

> La versión 1 de la API de gestión de grid (que se ha obsoleto) utiliza este permiso para gestionar las políticas de grupos de inquilinos, restablecer las contraseñas de administrador de Swift y gestionar las claves de acceso de S3 de usuario raíz.

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página Cuentas de arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.

Debe asignar el permiso Cuentas de inquilino al grupo para poder asignar este permiso.

Mantenimiento

Este permiso permite acceder a las siguientes opciones de menú:

- **Configuración** > **Configuración del sistema**:
  - Nombres de dominio*
  - Certificados de servidor*
- **Configuración** > **Supervisión**:
  - Auditoría*
- **Configuración** > **Control de acceso**:
  - Contraseñas de grid
- **Mantenimiento** > **tareas de mantenimiento**
  - Retirada
  - Expansión
  - Recuperación
- **Mantenimiento** > **Red**:
  - Servidores DNS*
  - Red de red*
  - Servidores NTP*
- **Mantenimiento** > **sistema**:
  - Licencia*
  - Paquete de recuperación
  - Actualización de software
- **Soporte** > **Herramientas**:
  - Registros
- Los usuarios que no tienen permiso de mantenimiento pueden ver, pero no editar, las páginas marcadas con un asterisco.

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.

ILM

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

- **Código de borrado**
- **Reglas**
- **Políticas**
- **Regiones**

> El acceso a las opciones de menú **ILM** > **agrupaciones de almacenamiento** y **ILM** > **grados de almacenamiento** está controlado por los permisos de configuración de páginas de configuración de cuadrícula y topología de cuadrícula.

Búsqueda de metadatos de objetos

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

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.

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 funciones 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.

Desactivación de funciones de la API de Grid Management

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 manera de impedir que el usuario raíz o los usuarios que pertenecen a grupos de administrador con el 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 inquilino** en el administrador de grid (tanto la interfaz de usuario como la API), la empresa A puede garantizar que ningún usuario de administrador (incluido el usuario raíz y los usuarios pertenecientes a grupos con permiso de acceso raíz) puede cambiar la contraseña para el usuario raíz de cualquier cuenta de arrendatario.*

Reactivación de 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.

Para obtener detalles, consulte las instrucciones para implementar las aplicaciones cliente S3 o Swift.

Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management.
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, se desactiva la función Cambiar contraseña raíz de inquilino. El permiso Cambiar la administración de la contraseña raíz del inquilino 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'".

4. 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 de inquilino. El permiso Cambiar la administración de contraseña raíz de arrendatario ahora aparece 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 de 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 inquilino y continuar desactivando la función de confirmación de alarma, envíe esta solicitud DE PUT:

   ```
   { "grid": { "alarmAcknowledgment": true } }
   ```

Información relacionada

"Uso de la API de gestión de grid"

Modificar un grupo de administración

Es posible modificar un grupo admin para cambiar los permisos asociados con el grupo. Para los grupos de administración locales, también puede actualizar el nombre para mostrar.

Lo que necesitará

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

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **grupos de administración**.
2. Seleccione el grupo.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Editar**.
4. Opcionalmente, para grupos locales, introduzca el nombre del grupo que aparecerá a los usuarios, por ejemplo, "usuarios de mantenimiento".

   No se puede cambiar el nombre único, que es el nombre del grupo interno.

5. Si lo desea, puede cambiar el modo de acceso del grupo.
   - **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.

6. Opcionalmente, añada o elimine permisos de grupo.

   Consulte la información sobre los permisos del grupo de administración.

7. Seleccione **Guardar**.

Información relacionada

Permisos de grupo de administradores

Eliminar un grupo de administrador

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 de administrador del grupo, pero no se eliminan los usuarios de administrador.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Al eliminar un grupo, los usuarios asignados a ese grupo perderán todos los privilegios de acceso al Gestor de cuadrícula, a menos que un grupo diferente les conceda privilegios.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **grupos de administración**.
2. Seleccione el nombre del grupo.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Seleccione **Quitar**.
4. Seleccione **OK**.

Gestión de usuarios locales

Puede crear usuarios locales y asignarles grupos de administración locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Grid Manager incluye un usuario local predefinido denominado «'root'». Aunque puede agregar y quitar usuarios locales, no puede quitar el usuario raíz.

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

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

Creando un usuario local

Si creó grupos de administración locales, puede crear uno o más usuarios locales y asignar cada usuario a uno o más grupos. Los permisos del grupo controlan a qué funciones de Grid Manager puede acceder el usuario.

Acerca de esta tarea

Solo es posible crear usuarios locales, y solo es posible asignar estos usuarios a grupos de administración locales. Los usuarios federados y los grupos federados se gestionan usando el origen de identidades externo.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **usuarios de administración**.
2. Haga clic en **Crear**.
3. Introduzca el nombre para mostrar, el nombre exclusivo y la contraseña del usuario.
4. Asigne el usuario a uno o varios grupos que rijan los permisos de acceso.

   La lista de nombres de grupo se genera a partir de la tabla grupos.

5. Haga clic en **Guardar**.

Información relacionada

"Gestión de los grupos de administración"

Modificar una cuenta de usuario local

Puede modificar la cuenta de un usuario administrador local para actualizar el nombre para mostrar del usuario o la pertenencia a grupos. También es posible impedir temporalmente que un usuario acceda al sistema.

Acerca de esta tarea

Solo puede editar usuarios locales. Los detalles de usuario federado se sincronizan automáticamente con el origen de identidad externo.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **usuarios de administración**.
2. Seleccione el usuario que desea editar.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Editar**.
4. Si lo desea, puede realizar cambios en el nombre o la pertenencia al grupo.
5. Opcionalmente, para evitar que el usuario acceda temporalmente al sistema, marque **Denegar acceso**.
6. Haga clic en **Guardar**.

   La nueva configuración se aplica la próxima vez que el usuario cierre sesión y vuelva a acceder al Gestor de cuadrícula.

Eliminar una cuenta de usuario local

Puede eliminar cuentas de usuarios locales que ya no requieran acceso a Grid Manager.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **usuarios de administración**.
2. Seleccione el usuario local que desea eliminar.

   > No se puede eliminar el usuario local raíz predefinido.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Quitar**.
4. Haga clic en **Aceptar**.

Cambiar la contraseña de un usuario local

Los usuarios locales pueden cambiar sus propias contraseñas mediante la opción **Cambiar contraseña** del banner de Grid Manager. Además, los usuarios que tienen acceso a la página Admin Users pueden cambiar

las contraseñas de otros usuarios locales.

Acerca de esta tarea

Solo es posible cambiar contraseñas para usuarios locales. Los usuarios federados deben cambiar sus propias contraseñas en el origen de identidades externo.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **usuarios de administración**.
2. En la página Users, seleccione el usuario.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. A continuación, puede utilizar la función de búsqueda de su navegador para buscar un elemento específico en las filas mostradas actualmente.

3. Haga clic en **Cambiar contraseña**.
4. Introduzca y confirme la contraseña y haga clic en **Guardar**.

Uso del inicio de sesión único (SSO) para StorageGRID

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). Cuando se habilita SSO, todos los usuarios deben estar autenticados por un proveedor de identidades externo antes de poder acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid o a la API de gestión de inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

- "Cómo funciona el inicio de sesión único"
- "Requisitos para usar el inicio de sesión único"
- "Configuración del inicio de sesión único"

Cómo funciona el inicio de sesión único

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.

Inicio de sesión cuando SSO está 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.

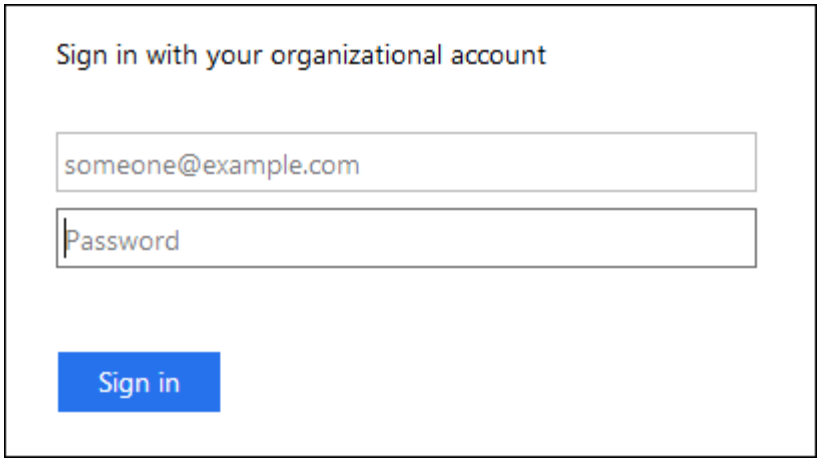
   - Si es la primera vez que accede a la URL en este navegador, se le pedirá un ID de cuenta:

- 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 en blanco el campo**ID de cuenta**, introduzca **0** como ID de cuenta o seleccione **Grid Manager** 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. Haga clic en **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 que tiene el permiso de acceso adecuado, se ha iniciado sesión en el Gestor de grid o en el Gestor de inquilinos, según la cuenta seleccionada.

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.

Cerrar sesión cuando SSO está 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. Haga clic en **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
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

Si ha iniciado sesión en…	Y salir de…	Se ha cerrado sesión en…
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.

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.

Requisitos del proveedor de identidades

El proveedor de identidades (IDP) para SSO debe cumplir los siguientes requisitos:

- Cualquiera de las siguientes versiones del servicio de Federación de Active Directory (AD FS):
  - AD FS 4.0, incluido en Windows Server 2016

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

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

StorageGRID utiliza un certificado de servidor de interfaz de gestión en cada nodo de administración para garantizar el acceso al administrador de grid, al administrador de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos. Cuando configura las confianzas de la parte de confianza de SSO para StorageGRID en AD FS, el certificado de servidor se utiliza como el certificado de firma para las solicitudes de StorageGRID a AD FS.

Si todavía no ha instalado un certificado de servidor personalizado para la interfaz de gestión, debe hacerlo ahora. Cuando se instala un certificado de servidor personalizado, se utiliza para todos los nodos de administración y se puede usar en todas las confianzas de parte que confía de StorageGRID.

No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en la confianza de parte de confianza de AD FS. 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 en AD FS 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`.

Información relacionada

"Controlar el acceso mediante firewalls"

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

Configuración del 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.

- "Confirmación de que los usuarios federados pueden iniciar sesión"
- "Uso del modo de recinto de seguridad"
- "Creación de confianzas de parte de confianza en AD FS"
- "Prueba de fideicomisos de la parte de confianza"
- "Habilitar el inicio de sesión único"
- "Desactivar el inicio de sesión único"
- "Desactive y vuelva a habilitar temporalmente el inicio de sesión único para un nodo de administración"

Confirmación de 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Está utilizando Active Directory como origen de identidad federado y AD FS como proveedor de identidades.

  "Requisitos para usar el inicio de sesión único"

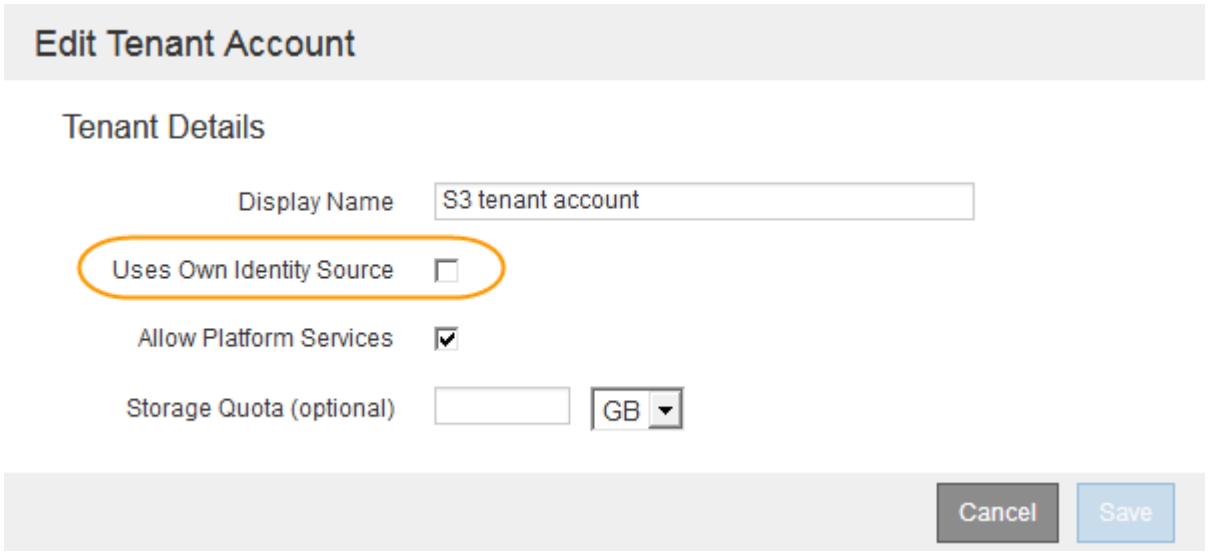
Pasos

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 **Control 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 haga clic en **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 haga clic en **Editar cuenta**.
   c. Si la casilla de verificación **Usos own Identity Source** está activada, desmarque la casilla y haga clic en **Guardar**.



Aparece la página Cuentas de arrendatario.

   a. Seleccione la cuenta de arrendatario, haga clic en **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
   b. En el Administrador de arrendatarios, haga clic en **Control de acceso** > **grupos**.
   c. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso 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"

"Gestión de los grupos de administración"

"Usar una cuenta de inquilino"

Uso del modo de recinto de seguridad

Puede utilizar el modo de recinto de seguridad para configurar y probar las confianzas de partes de Active Directory Federation Services (AD FS) antes de aplicar el inicio de sesión único (SSO) para los usuarios de StorageGRID. Una vez habilitado SSO, puede volver a habilitar el modo Sandbox para configurar o probar confianzas de partes de confianza nuevas y existentes. Al volver a habilitar el modo de recinto limitado, se deshabilita temporalmente SSO para los usuarios de StorageGRID.

Lo que necesitará

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

Acerca de esta tarea

Cuando se habilita SSO y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación a AD FS. A su vez, AD FS envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autorización se ha realizado correctamente. En el caso de las solicitudes correctas, la respuesta incluye un identificador único universal (UUID) para el usuario.

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

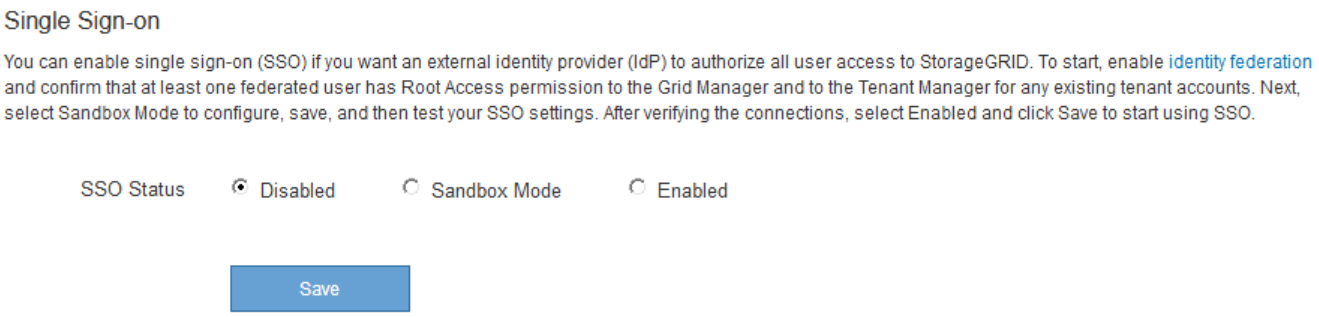
El modo de recinto de seguridad facilita la realización de esta configuración de fondo y la realización de pruebas de todos los ajustes antes de habilitar SSO.

> Se recomienda utilizar el modo de recinto de seguridad, pero no estrictamente necesario. Si está preparado para crear confianzas de parte de confianza de AD FS inmediatamente después de configurar SSO en StorageGRID, Además, no es necesario probar los procesos de inicio de sesión único (SLO) y cierre de sesión único (SLO) para cada nodo de administración, haga clic en **habilitado**, introduzca la configuración de StorageGRID, cree una confianza de parte de confianza para cada nodo de administración en AD FS y, a continuación, haga clic en **Guardar** para habilitar SSO.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.

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



Si las opciones de estado de SSO no aparecen, confirme que ha configurado Active Directory como origen de identidad federado. Véase «'requisitos para el uso de la entrada única».

2. Seleccione la opción **modo Sandbox**.

   Aparece la configuración del proveedor de identidades y de la parte de confianza. En la sección Proveedor de identidades, el campo **Tipo de servicio** es de sólo lectura. Muestra el tipo de servicio de federación de identidades que está utilizando (por ejemplo, Active Directory).

3. En la sección Proveedor de identidades:

   a. Escriba el nombre del Servicio de Federación, exactamente como aparece en AD FS.

      Para buscar el nombre del servicio de Federación, vaya al Administrador del servidor de Windows. 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.

   b. Especifique si desea utilizar TLS (Seguridad de la capa de transporte) para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a 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 este ajuste, copie y pegue el certificado en el cuadro de texto **Certificado CA**.

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

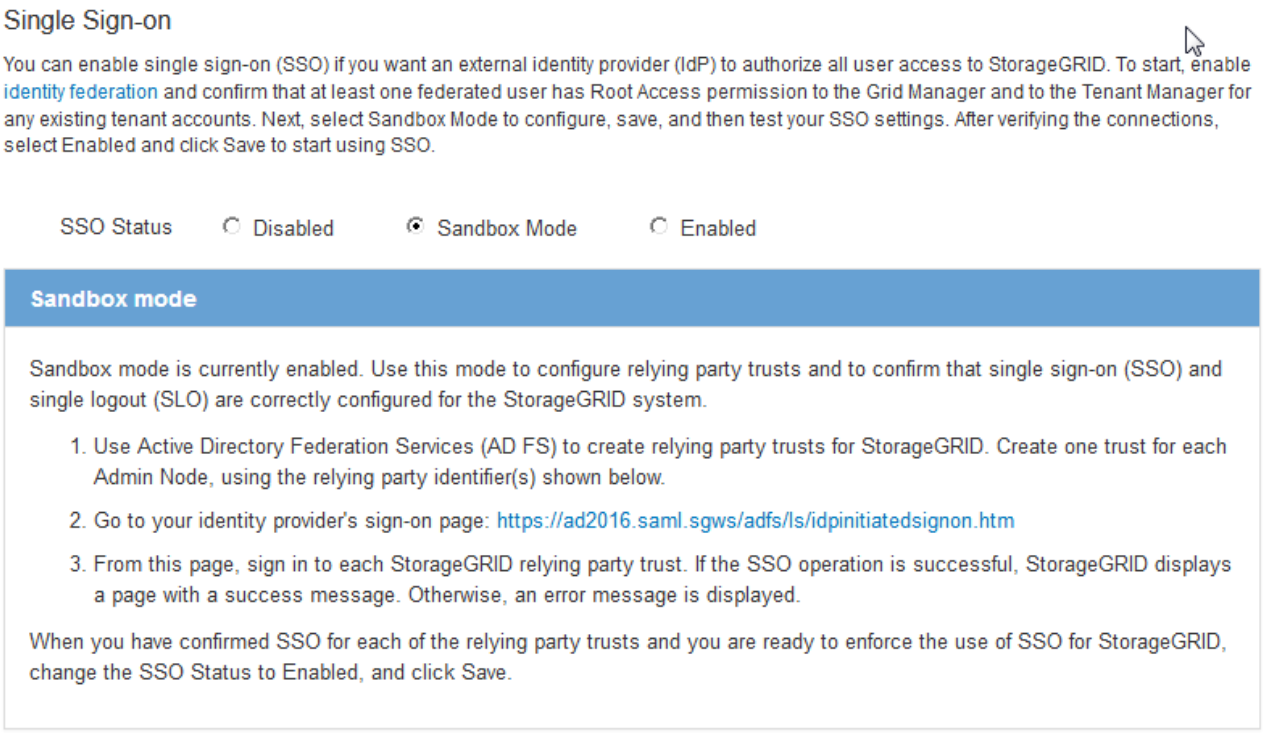
4. En la sección parte de confianza , especifique el identificador de parte de confianza que utilizará para los nodos de administración de StorageGRID cuando configure confianzas de parte de confianza.

   - 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]`. Esto genera una tabla que incluye un identificador de parte de confianza para cada nodo de administración, en función del nombre de host del nodo. + NOTA: Debe crear una confianza de parte de confianza para cada nodo de administración en su 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.

5. Haga clic en **Guardar**.
   - Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

   - Aparece el aviso de confirmación del modo Sandbox, que confirma que el modo Sandbox está habilitado. Puede utilizar este modo mientras utiliza AD FS para configurar una confianza de parte de confianza para cada nodo de administración y probar los procesos de inicio de sesión único (SSO) y cierre de sesión único (SLO).

Información relacionada

"Requisitos para usar el inicio de sesión único"

Creación de 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.

Crear una confianza de parte de confianza mediante Windows PowerShell

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

Lo que necesitará

- Configuró SSO en StorageGRID y conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administrador del sistema.

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.

Acerca de esta tarea

Estas instrucciones se aplican a AD FS 4.0, que se incluye en Windows Server 2016. Si está utilizando AD FS 3.0, que se incluye con Windows 2012 R2, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

Pasos

1. En el menú de inicio de Windows, haga clic con el botón derecho del ratón en 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. Haga clic en **aplicar** y haga clic en **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. Haga clic en **Agregar regla**.

d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **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. Haga clic en **Finalizar** y haga clic en **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 la parte de confianza" para confirmar que están correctamente configurados.

Crear una confianza de parte de confianza mediante la importación de 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.

Lo que necesitará

- Configuró SSO en StorageGRID y conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administrador del sistema.

> ⓘ 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.

Acerca de esta tarea

Estas instrucciones se aplican a AD FS 4.0, que se incluye en Windows Server 2016. Si está utilizando AD FS 3.0, que se incluye con Windows 2012 R2, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

Pasos

1. En Windows Server Manager, haga clic en **Herramientas** y, a continuación, seleccione **Administración**

de AD FS.

2. En acciones, haga clic en **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y haga clic en **Inicio**.
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. Haga clic en **Agregar regla**:
   c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **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. Haga clic en **Finalizar** y haga clic en **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 la parte de confianza" para confirmar que están correctamente configurados.

Crear 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.

Lo que necesitará

- Configuró SSO en StorageGRID y conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administrador del sistema.

> 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 el certificado personalizado que se cargó para la interfaz de gestión StorageGRID, o bien sabe cómo iniciar sesión en un nodo de administrador desde el shell de comandos.
- 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.

Acerca de esta tarea

Estas instrucciones se aplican a AD FS 4.0, que se incluye en Windows Server 2016. Si está utilizando AD FS 3.0, que se incluye con Windows 2012 R2, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

Pasos

1. En Windows Server Manager, haga clic en **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, haga clic en **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y haga clic en **Inicio**.
4. Seleccione **introducir datos sobre la parte que confía manualmente** y haga clic en **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, haga clic en **Agregar regla**:
   a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y haga clic en **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. Haga clic en **Finalizar** y haga clic en **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. Haga clic en **Agregar 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. Haga clic en **Aceptar**.
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. Haga clic en **aplicar** y haga clic en **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 la parte de confianza" para confirmar que están correctamente configurados.

Prueba de fideicomisos de la parte de confianza

Antes de aplicar el uso de inicio de sesión único (SSO) para StorageGRID, confirme que el inicio de sesión único y el cierre de sesión único (SLO) se han configurado correctamente. Si ha creado una confianza de parte de confianza para cada nodo de administrador, confirme que puede usar SSO y SLO para cada nodo de administración.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Ha configurado una o más confianzas de parte de confianza en AD FS.

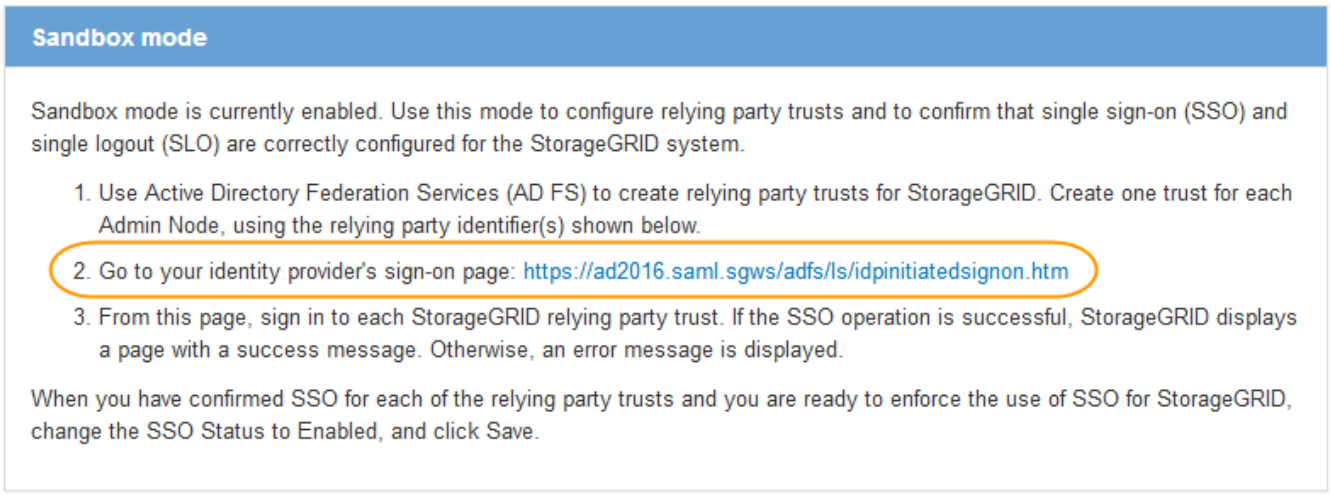
Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.

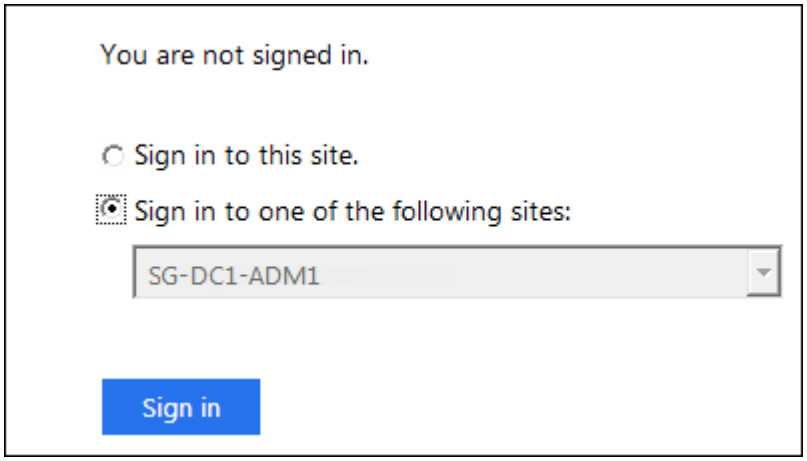
   Aparece la página Single Sign-On, con la opción **modo Sandbox** seleccionada.

2. En las instrucciones para el modo de recinto de seguridad, busque el vínculo a la página de inicio de sesión del proveedor de identidades.

   La dirección URL se deriva del valor especificado en el campo **Nombre de servicio federado**.

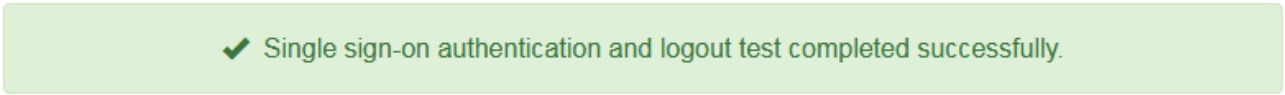


3. Haga clic en el vínculo o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión del proveedor de identidades.
4. Para confirmar que puede utilizar SSO para iniciar sesión en StorageGRID, seleccione **Iniciar sesión en uno de los siguientes sitios**, seleccione el identificador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



Se le solicitará que introduzca su nombre de usuario y contraseña.

5. 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.
6. Repita los pasos anteriores para confirmar que puede iniciar sesión en cualquier otro nodo de administrador.

Si todas las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, estará listo para habilitar SSO.

Después de usar el modo de Sandbox para probar todas sus confianzas de partes de confianza de StorageGRID, estará listo para habilitar el inicio de sesión único (SSO).

Lo que necesitará

- Debe haber importado al menos un grupo federado del origen de identidades y los permisos de administración de acceso raíz asignados al grupo. Debe confirmar que al menos un usuario federado tiene permiso de acceso raíz al administrador de grid y al administrador de inquilinos para las cuentas de arrendatario existentes.
- Debe haber probado todas las confianzas de partes de confianza mediante el modo de Sandbox.

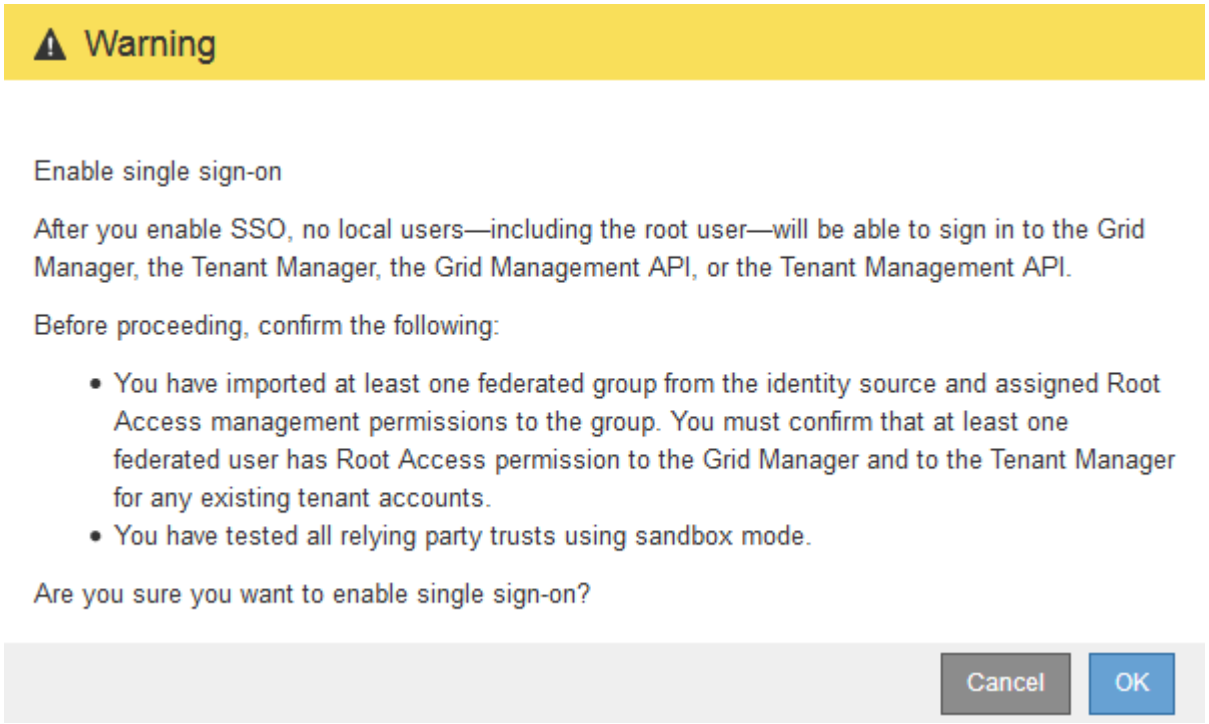
Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.

   Aparece la página Single Sign-On con **modo Sandbox** seleccionado.

2. Cambie el estado de SSO a **habilitado**.
3. Haga clic en **Guardar**.

   Aparecerá un mensaje de advertencia.



4. Revise la advertencia y haga clic en **Aceptar**.

   El inicio de sesión único ahora está activado.

> Todos los usuarios deben utilizar SSO para acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Desactivar 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

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

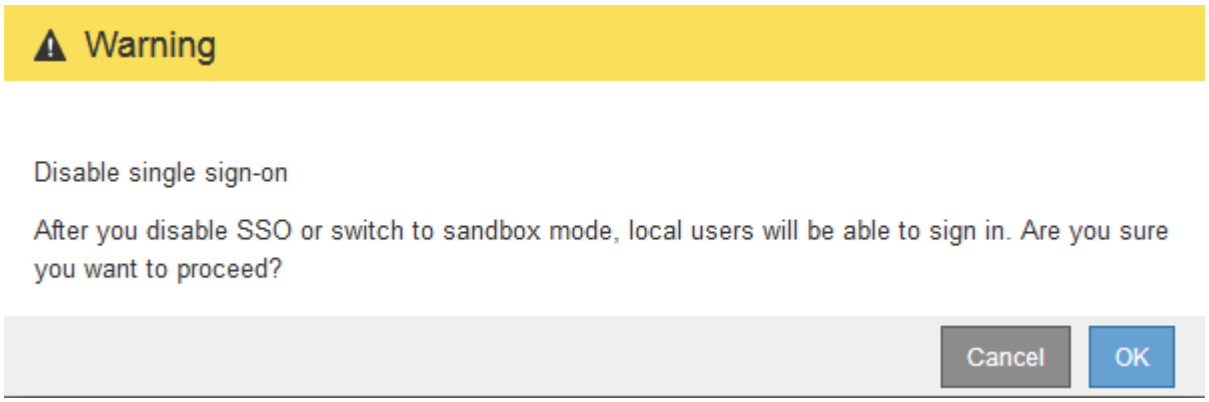
Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.

   Aparece la página Single Sign-On.

2. Seleccione la opción **Desactivado**.
3. Haga clic en **Guardar**.

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



4. Haga clic en **Aceptar**.

   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

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer 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** > **Inicio de sesión único**.
   b. Cambie la configuración incorrecta o obsoleta de SSO.
   c. Haga clic en **Guardar**.

   Al hacer clic en **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. Haga clic en **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.

Información relacionada

"Configuración del inicio de sesión único"

Configurar certificados de cliente de administrador

Puede utilizar certificados de cliente para permitir que clientes externos autorizados accedan a la base de datos Prometheus de StorageGRID. Los certificados de cliente proporcionan una forma segura de utilizar herramientas externas para supervisar 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.

Añadiendo certificados de cliente de administrador

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

Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe conocer la dirección IP o el nombre de dominio del nodo de administrador.
- Debe haber configurado el certificado de servidor de interfaz de gestión de StorageGRID y tener el bundle de CA correspondiente
- Si desea cargar su propio certificado, la clave pública y la clave privada del certificado deben estar disponibles en el equipo local.

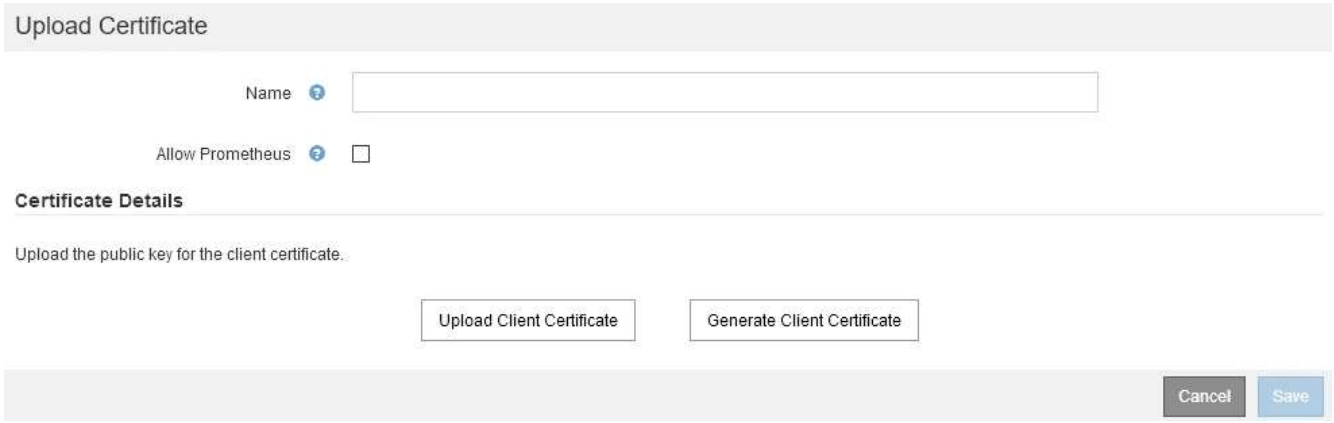
Pasos

1. En Grid Manager, seleccione **Configuración** > **Control de acceso** > **certificados de cliente**.

   Aparece la página certificados de cliente.

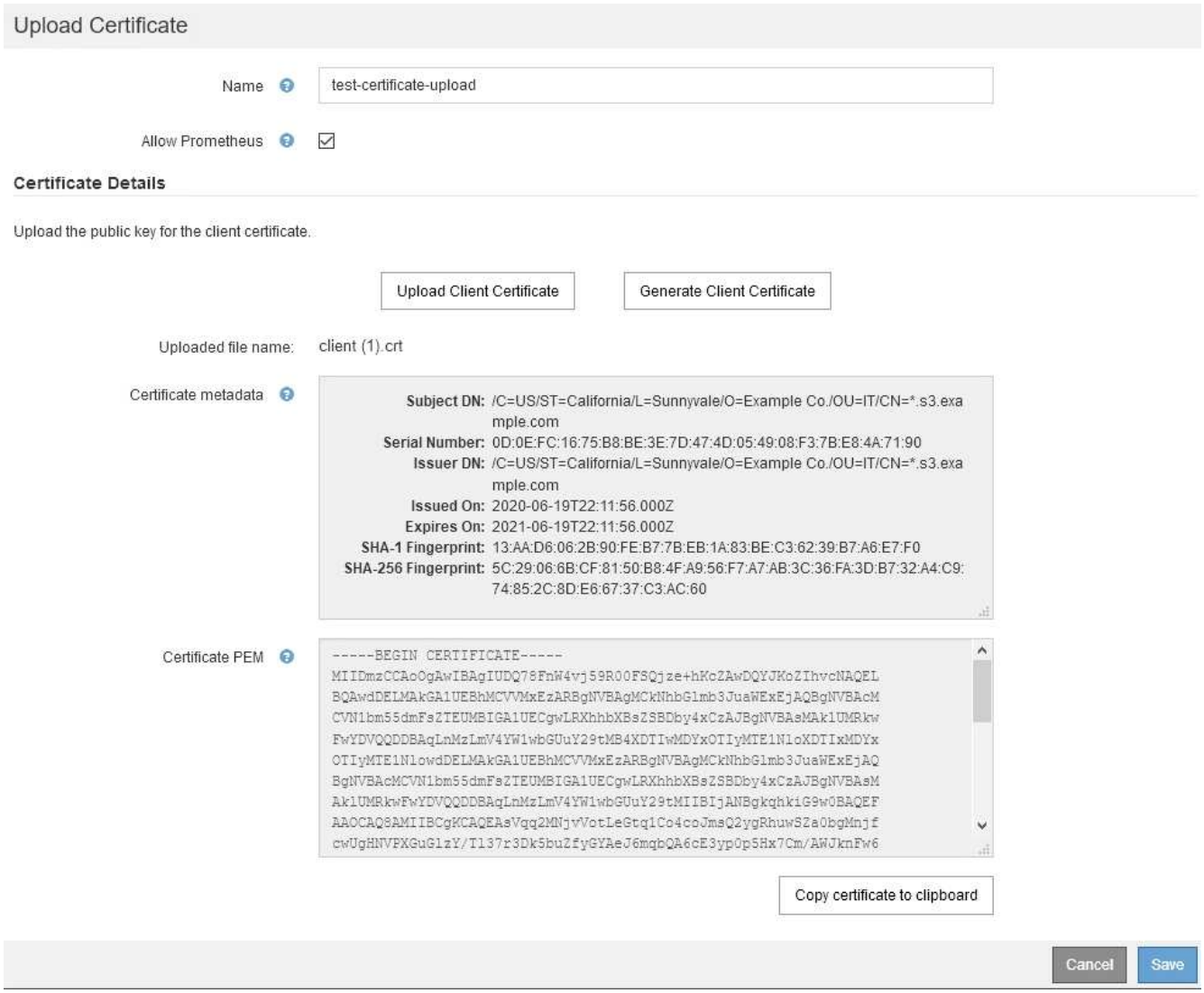
2. Seleccione **Agregar**.

   Aparece la página cargar certificado.



3. Escriba un nombre entre 1 y 32 caracteres para el certificado.
4. Para acceder a las métricas de Prometheus mediante la herramienta de supervisión externa, active la casilla de verificación **permitir Prometheus** .
5. Cargar o generar un certificado:
   a. Para cargar un certificado, vaya aquí.
   b. Para generar un certificado, vaya aquí.
6. para cargar un certificado:
   a. Seleccione **cargar certificado de cliente**.
   b. Busque la clave pública del certificado.

      Después de cargar la clave pública para el certificado, se rellenan los campos **metadatos de certificado** y **PEM de certificado**.



a. Seleccione **Copiar certificado en el portapapeles** y pegue el certificado en la herramienta de supervisión externa.

b. Utilice una herramienta de edición para copiar y pegar la clave privada en su herramienta de supervisión externa.

c. Seleccione **Guardar** para guardar el certificado en Grid Manager.

7. para generar un certificado:

a. Seleccione **generar certificado de cliente**.

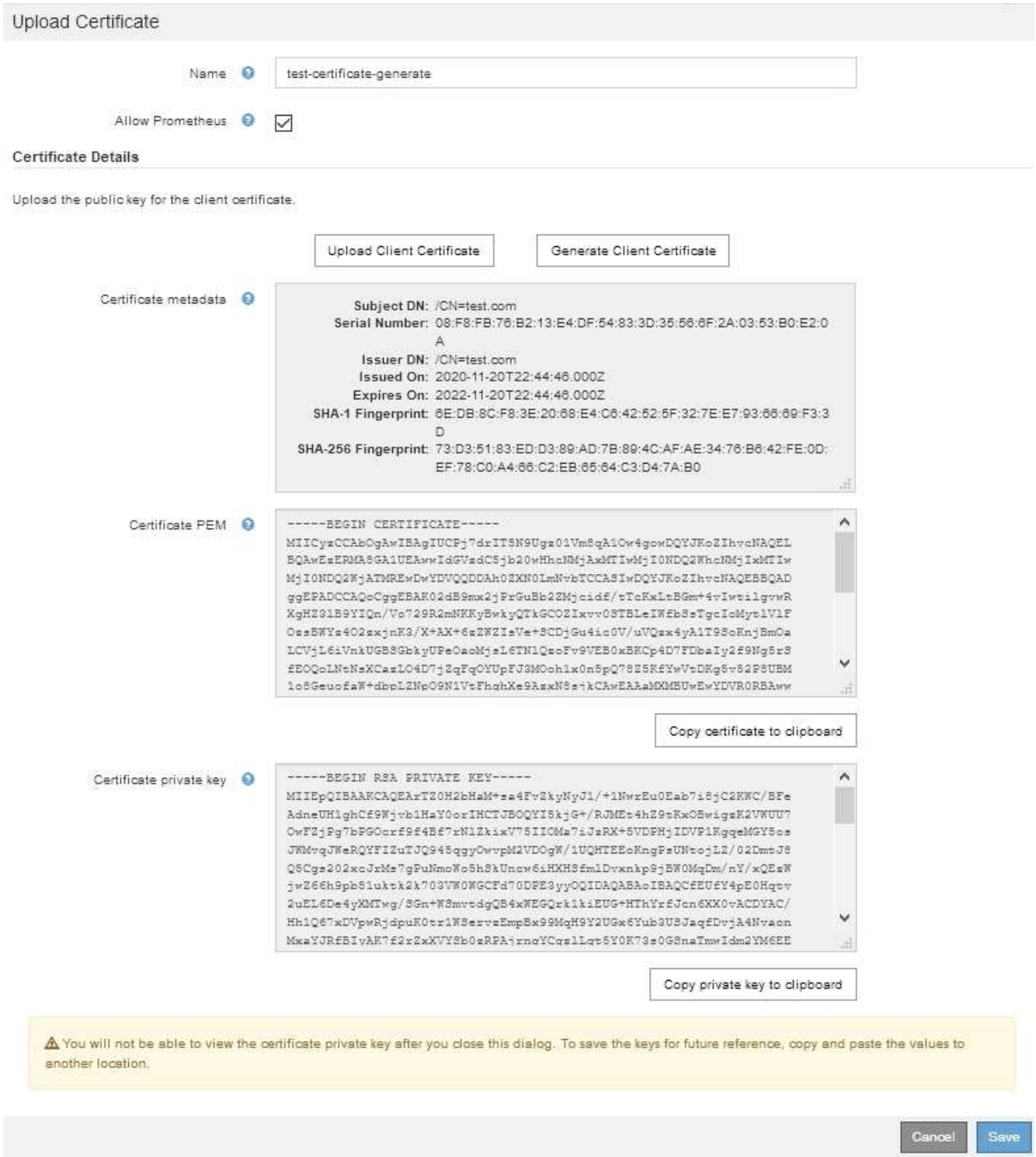
b. Introduzca el nombre de dominio o la dirección IP del nodo de administración.

c. Opcionalmente, introduzca un asunto X.509, también denominado Nombre distintivo (DN), para identificar al administrador que posee el certificado.

d. De manera opcional, seleccione el número de días en los que el certificado es válido. El valor predeterminado es 730 días.

e. Seleccione **generar**.

Se rellenan los campos **metadatos de certificado**, **PEM de certificado** y **clave privada de certificado**.



a. Seleccione **Copiar certificado en el portapapeles** y pegue el certificado en la herramienta de supervisión externa.

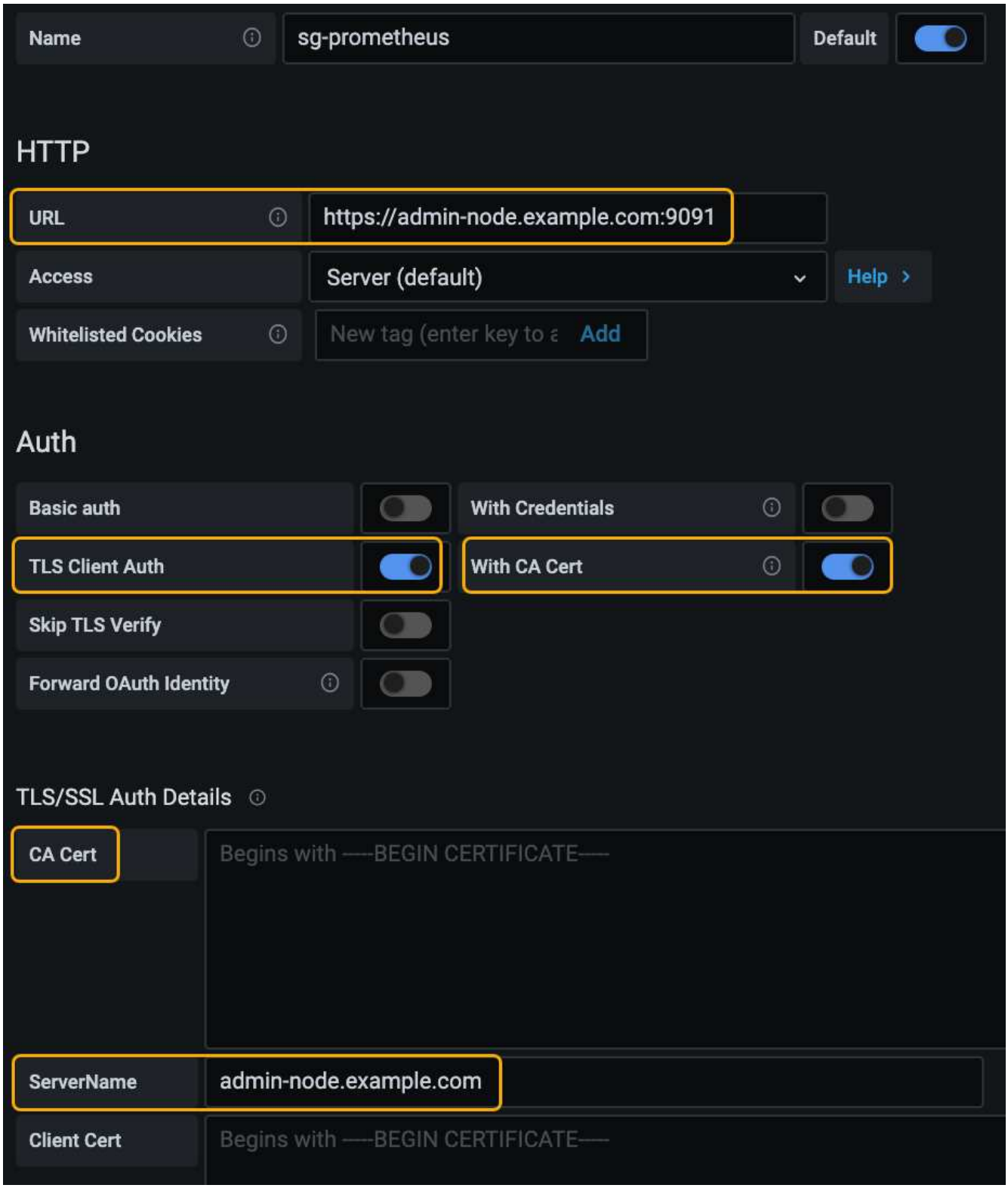
b. Seleccione **Copiar clave privada en el portapapeles** y pegue la clave en su herramienta de monitorización externa.

> No podrá ver la clave privada después de cerrar el cuadro de diálogo. Copie la llave en una ubicación segura.

c. Seleccione **Guardar** para guardar el certificado en Grid Manager.

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

   En la siguiente captura de pantalla se muestra un ejemplo de 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 **autorización de cliente TLS** y **con CA Cert**.

d. Copie y pegue el certificado de servidor de interfaz de administración o el paquete de CA en**CA Cert** en Detalles de autenticación TLS/SSL.

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 servidor 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 información acerca de las métricas, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.

Información relacionada

"Usar certificados de seguridad StorageGRID"

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

"Solución de problemas de monitor"

Editar certificados de cliente de administrador

Un certificado se puede editar para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o cargar un nuevo certificado cuando el actual haya caducado.

Lo que necesitará

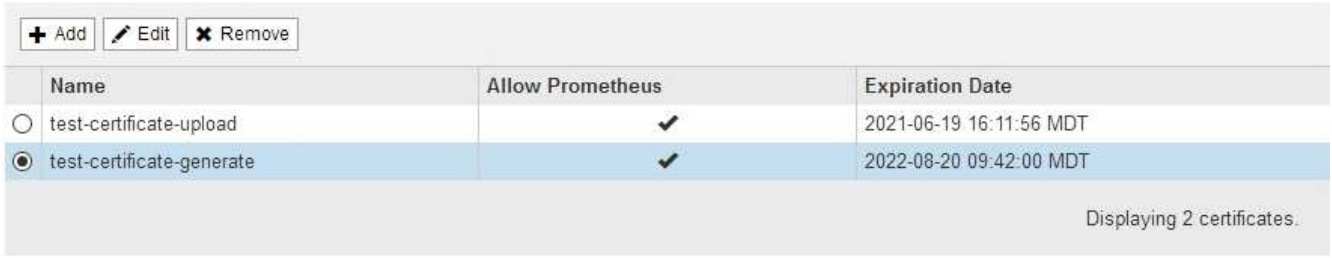
- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe conocer la dirección IP o el nombre de dominio del nodo de administrador.
- Si desea cargar un nuevo certificado y una clave privada, deben estar disponibles en el equipo local.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **certificados de cliente**.

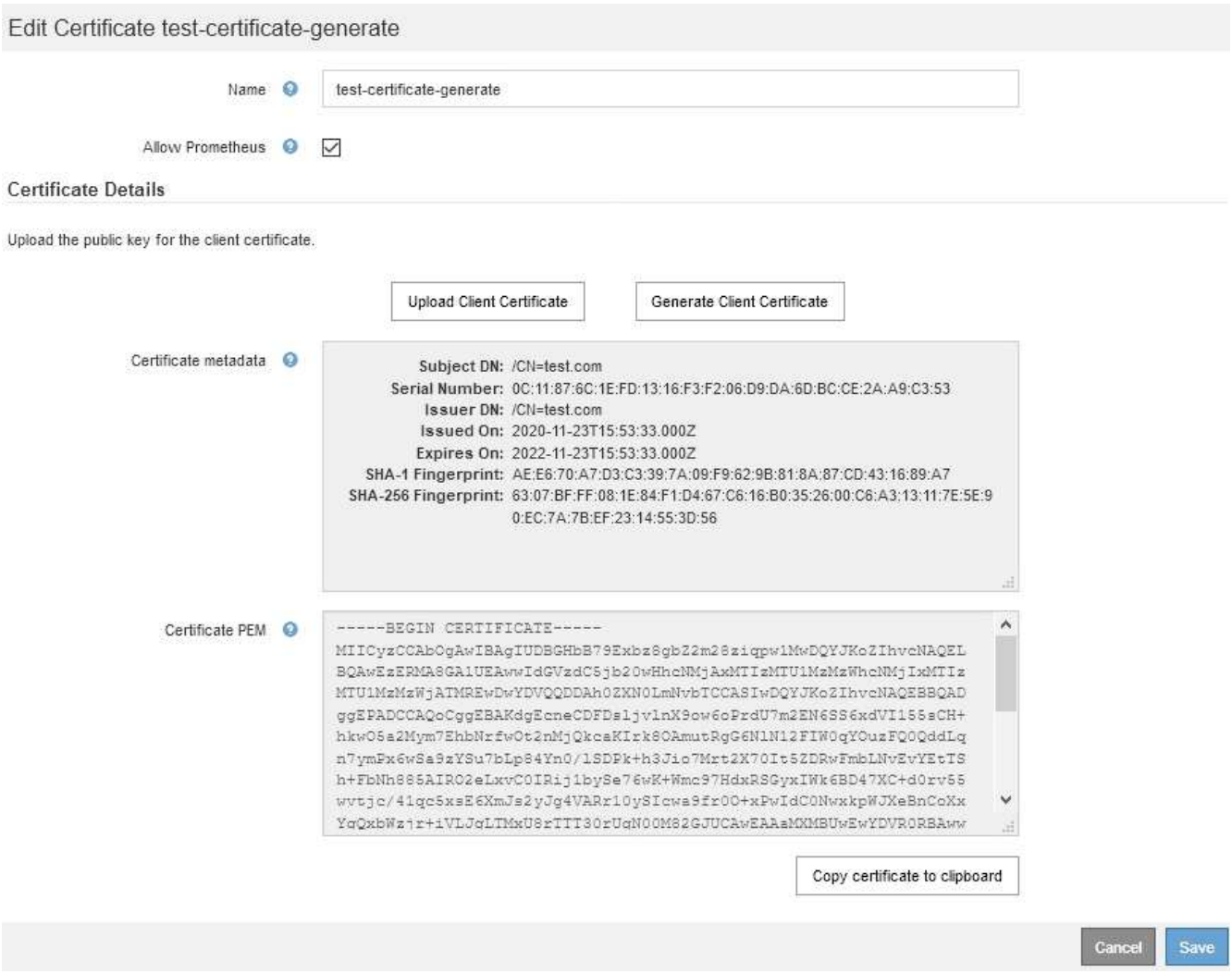
   Aparece la página certificados de cliente. Se muestra una lista de los certificados existentes.

   Las fechas de vencimiento del certificado se muestran 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 botón de opción situado a la izquierda del certificado que desea editar.
3. Seleccione **Editar**.

   Se muestra el cuadro de diálogo Editar certificado.



4. Realice los cambios que desee en el certificado.
5. Seleccione **Guardar** para guardar el certificado en Grid Manager.
6. Si cargó un nuevo certificado:
   a. Seleccione **Copiar certificado en el portapapeles** para pegar el certificado en la herramienta de supervisión externa.
   b. Utilice una herramienta de edición para copiar y pegar la nueva clave privada en su herramienta de supervisión externa.

c. Guarde y pruebe el certificado y la clave privada en la herramienta de supervisión externa.

7. Si generó un nuevo certificado:
   a. Seleccione **Copiar certificado en el portapapeles** para pegar el certificado en la herramienta de supervisión externa.
   b. Seleccione **Copiar clave privada en el portapapeles** para pegar el certificado en la herramienta de supervisión externa.

> No podrá ver ni copiar la clave privada después de cerrar el cuadro de diálogo. Copie la llave en una ubicación segura.

   c. Guarde y pruebe el certificado y la clave privada en la herramienta de supervisión externa.

Quitar certificados de cliente de administrador

Si ya no necesita un certificado, es posible eliminarlo.

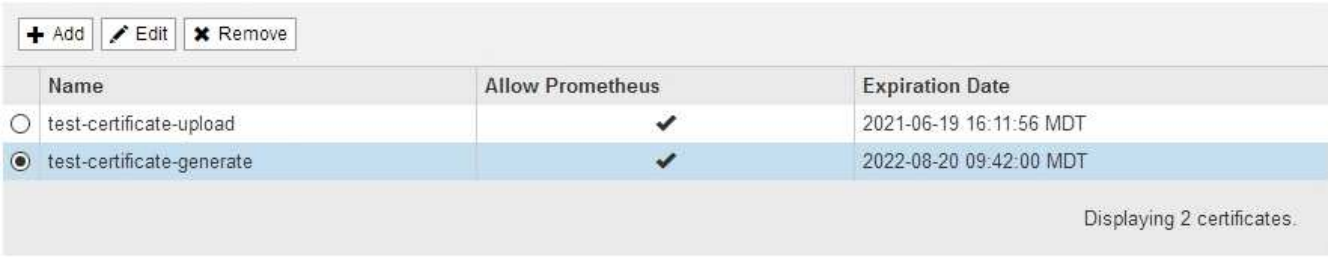
Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **certificados de cliente**.

   Aparece la página certificados de cliente. Se muestra una lista de los certificados existentes.



2. Seleccione el botón de opción situado a la izquierda del certificado que desea eliminar.
3. Seleccione **Quitar**.

   Se muestra un cuadro de diálogo de confirmación.

4. Seleccione **OK**.

El certificado se eliminará.

Configuración de servidores de gestión de claves

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.

Revisión de los métodos de cifrado 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** > **Configuración del sistema** > **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. Se puede usar con algunos dispositivos de almacenamiento y servicios de StorageGRID.

Opción de cifrado	Cómo funciona	Se aplica a.
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. "Dispositivos de almacenamiento SG6000" "Dispositivos de almacenamiento SG5700" "Dispositivos de almacenamiento SG5600"
Opción de cuadrícula de cifrado de objetos almacenados	La opción **cifrado de objetos almacenados** se puede habilitar en Grid Manager (**Configuración** > **Configuración del 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.	Los datos de objetos S3 y Swift recién ingeridos.los objetos almacenados existentes no se cifran. Los metadatos de objetos y otros datos confidenciales no se cifran. "Configurar el cifrado de objetos almacenados"
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.se debe especificar el cifrado para el bloque. Los objetos de bloque existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran. "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.se debe especificar el cifrado para el objeto. Los metadatos de objetos y otros datos confidenciales no se cifran. StorageGRID gestiona las claves. "Use S3"

Opción de cifrado	Cómo funciona	Se aplica a.
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. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo datos de objetos S3 procesados recientemente.se debe especificar el cifrado para el objeto. Los metadatos de objetos y otros datos confidenciales no se cifran. Las claves se gestionan fuera de StorageGRID. "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. 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.
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). 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. "Amazon simple Storage Service - Guía para desarrolladores: Protección de datos mediante cifrado en el cliente"

Utilizando varios métodos de cifrado

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

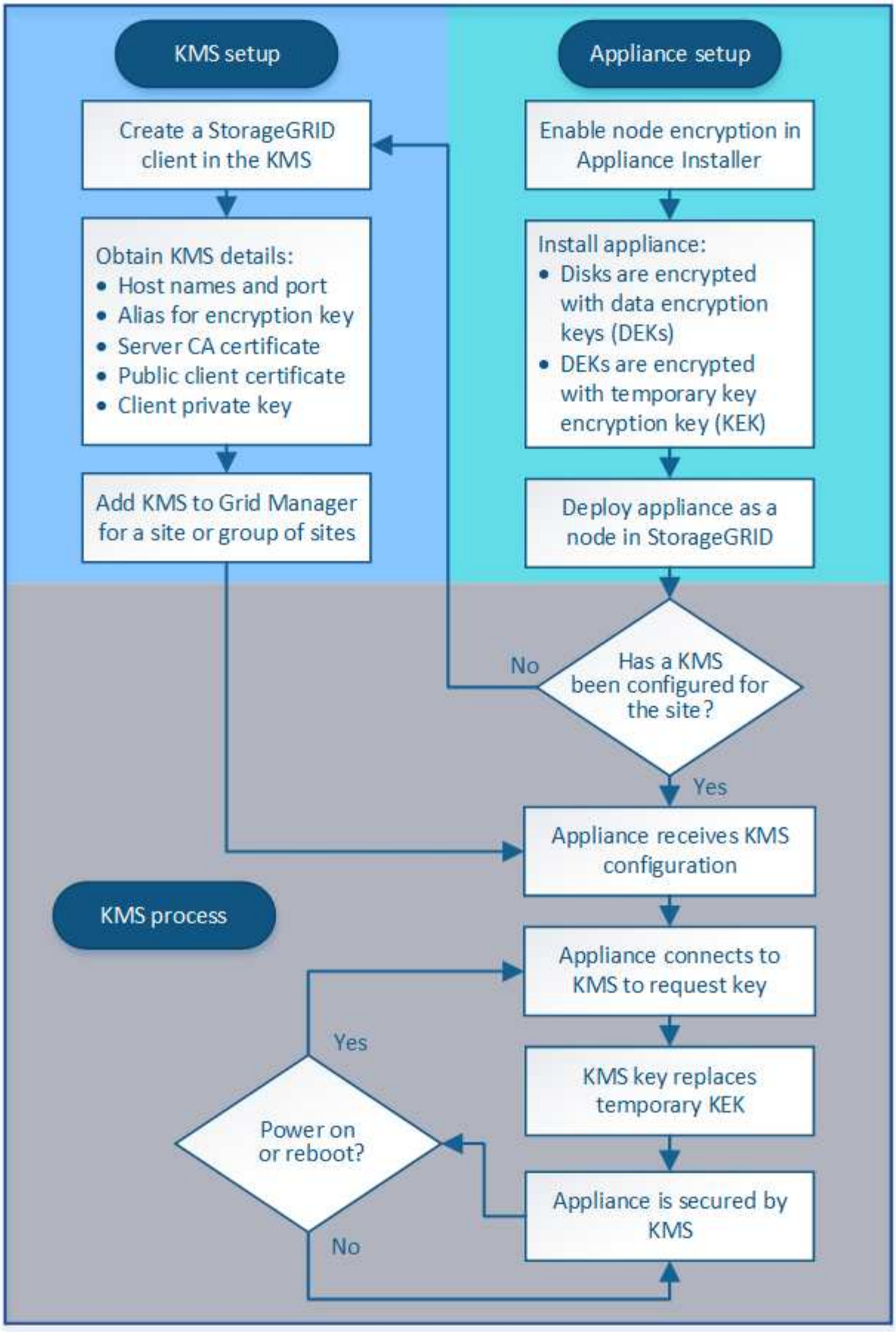
- Puede utilizar un KMS para proteger los nodos de dispositivos y también para usar la función de seguridad de unidades de System Manager de SANtricity a fin de «doble cifrado» de datos de las unidades de autocifrado de los mismos dispositivos.
- Puede usar un KMS para proteger los datos en los nodos 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.

Configuración del 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.	"Configurar StorageGRID como cliente en el KMS"
Obtenga la información necesaria para el cliente StorageGRID en el KMS.	"Configurar StorageGRID como cliente en el 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.	"Adición de un servidor de gestión de claves (KMS)"

Configuración del 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:

- "SG100 servicios de aplicaciones 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 puestos en marcha en contenedores Docker 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?

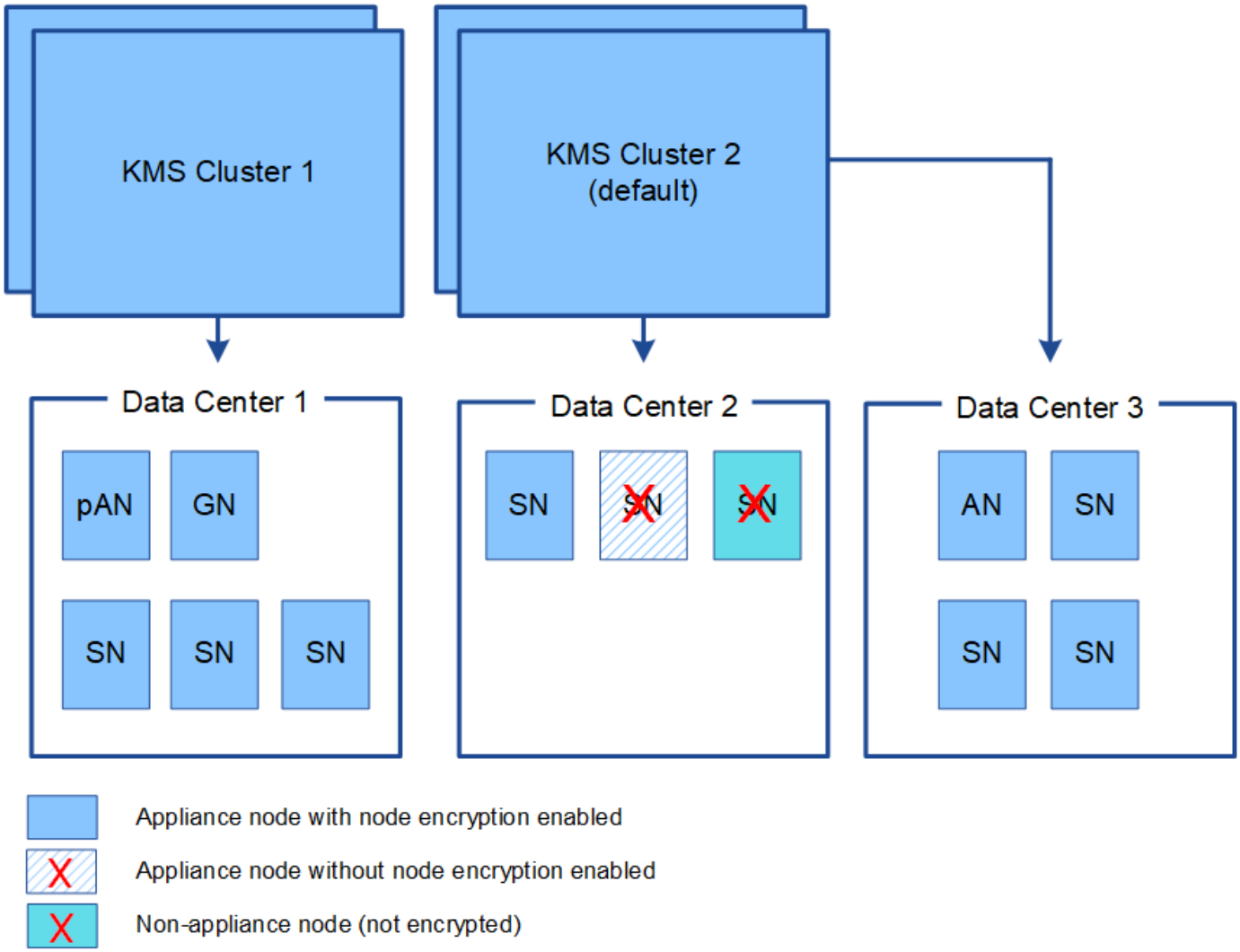
Puede configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de dispositivos en el sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de dispositivos StorageGRID en un único sitio o a un grupo de sitios.

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.

"SG100 servicios de aplicaciones SG1000"

"Dispositivos de almacenamiento SG6000"

"Dispositivos de almacenamiento SG5700"

"Dispositivos de almacenamiento SG5600"

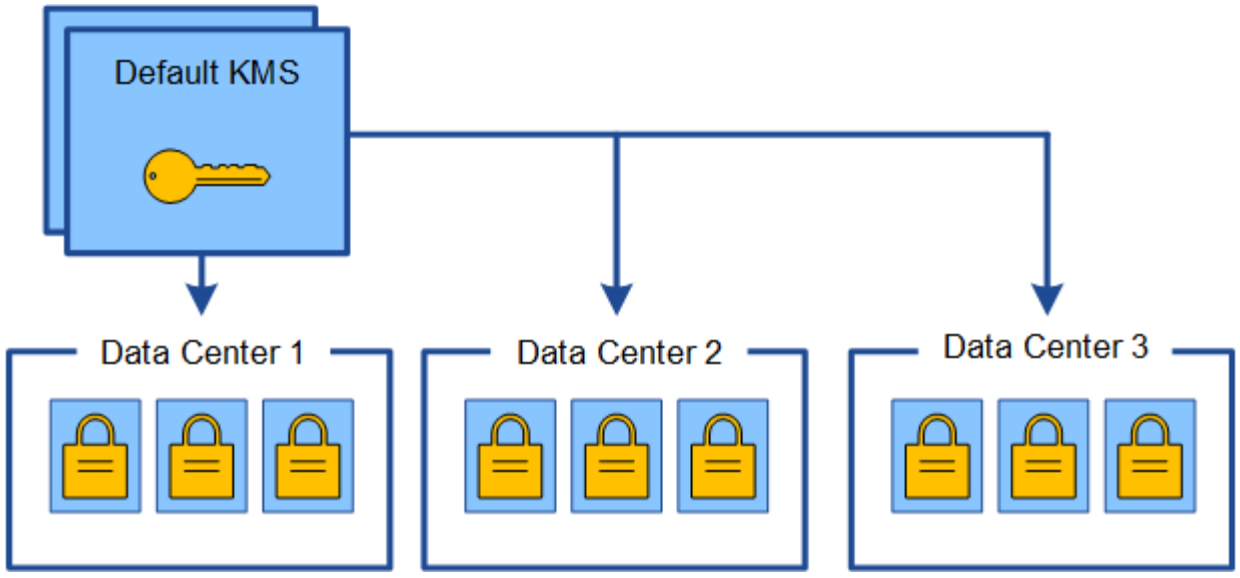
Consideraciones para cambiar el KMS de un sitio

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.

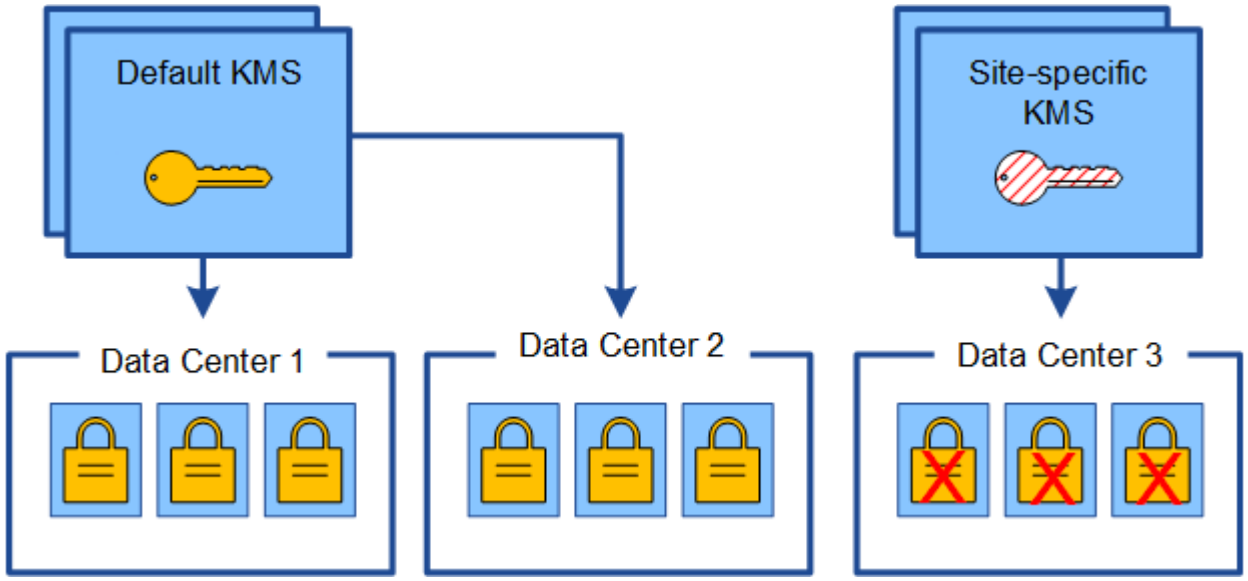
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original 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:

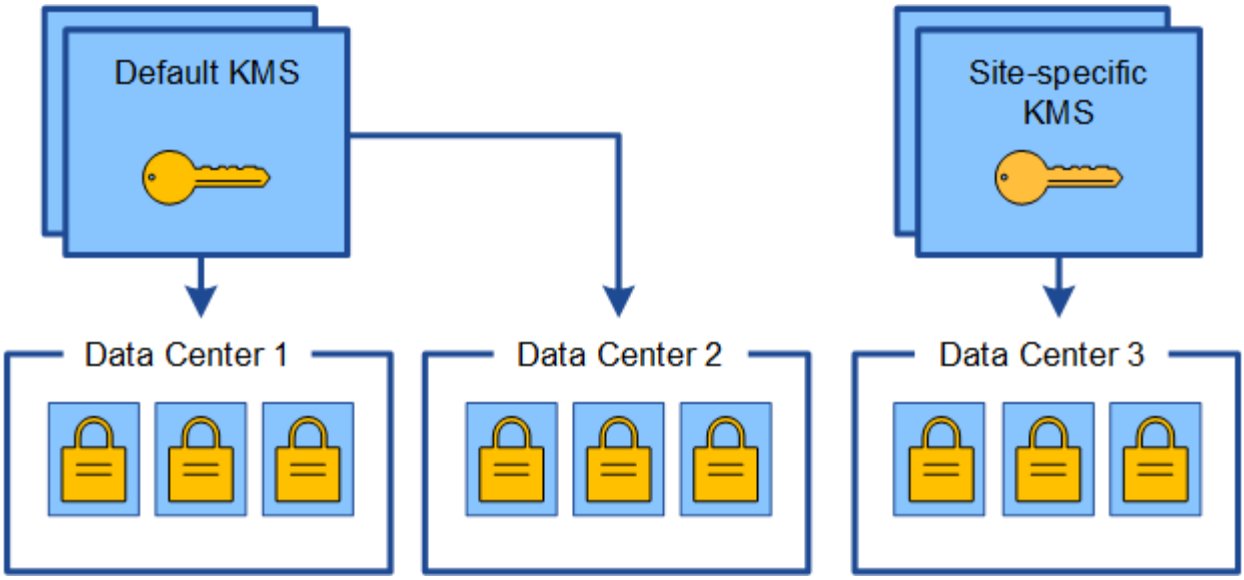
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa 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. "Edición de 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. 2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Adición de 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. 2. Con el Administrador de cuadrícula, edite la configuración de KMS existente e introduzca el nuevo nombre de host o la dirección IP. "Adición de un servidor de gestión de claves (KMS)"

Configurar StorageGRID como cliente en el 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.

Adición de 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

- Debe haber revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Debe tener "Se ha configurado StorageGRID como cliente en el KMS"Y debe tener la información necesaria para cada clúster KMS o KMS
- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

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.

"Consideraciones para cambiar el KMS de un sitio"

Pasos

1. "Paso 1: Introduzca los detalles de KMS"
2. "Paso 2: Cargar certificado de servidor"
3. "Paso 3: Cargar certificados de cliente"

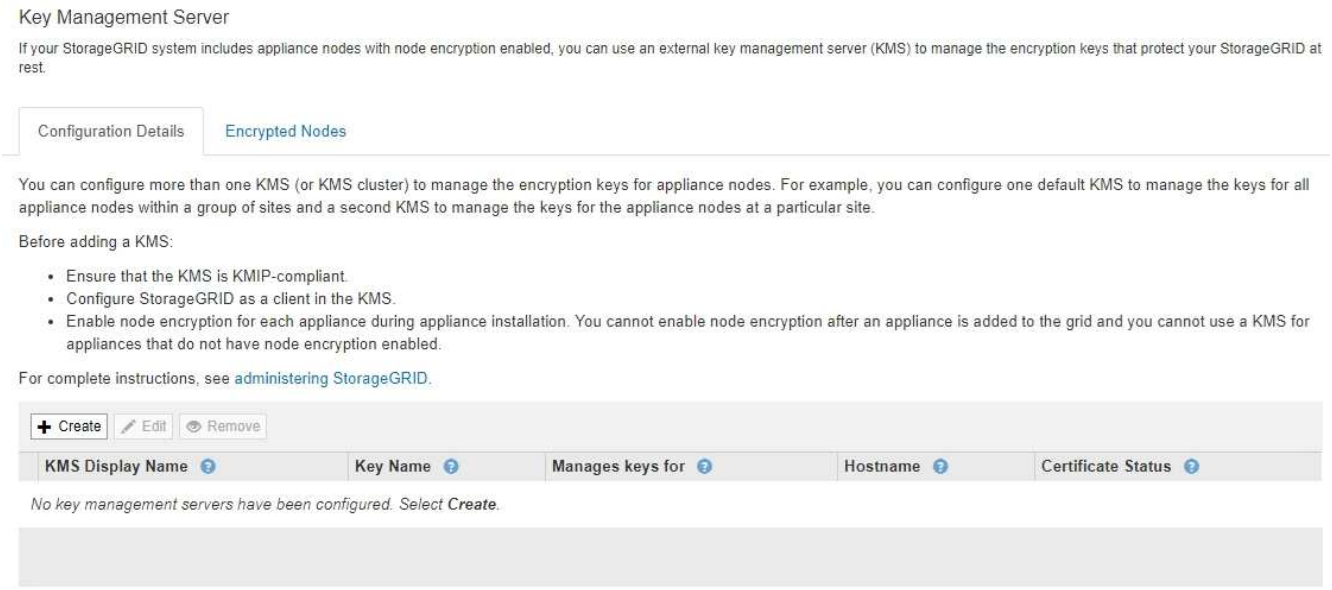
Paso 1: Introduzca los detalles de KMS

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

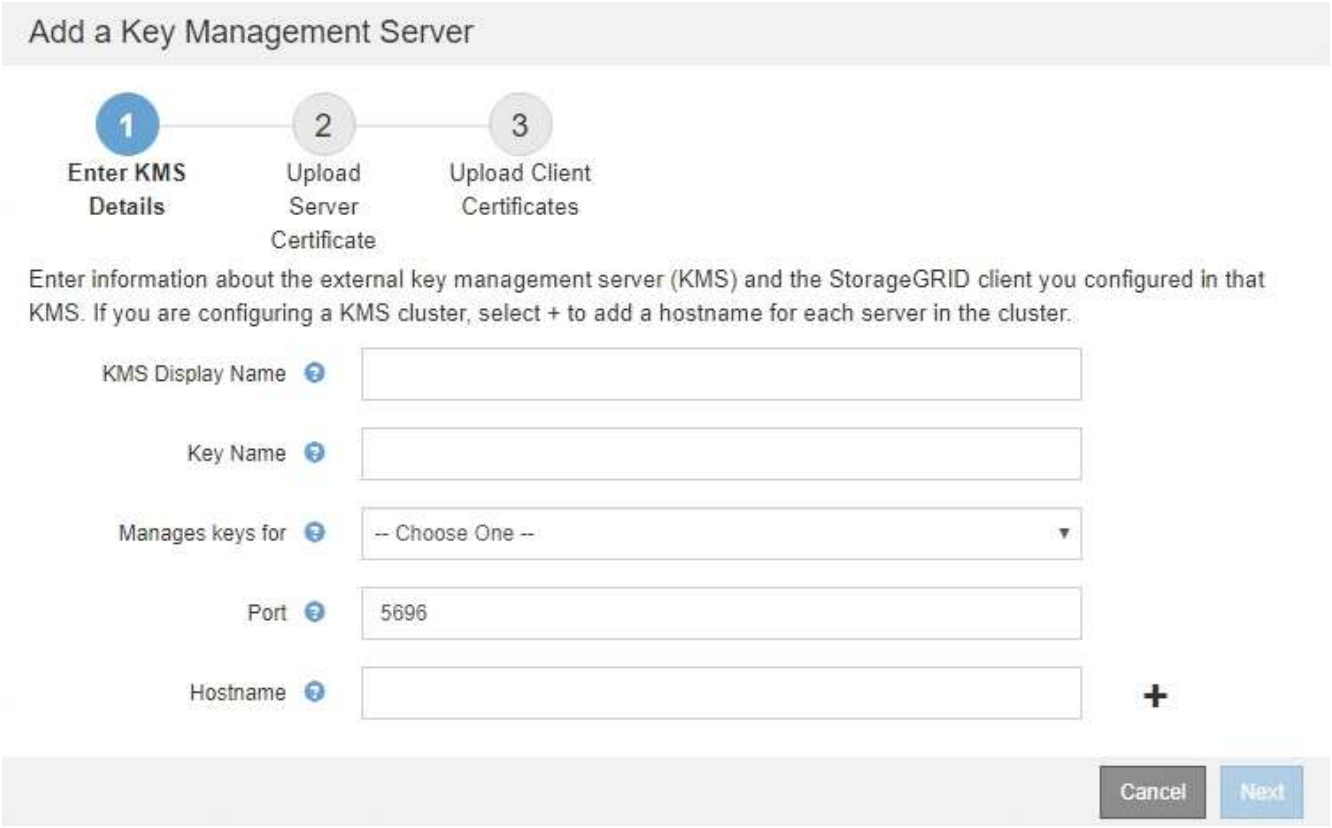
1. Seleccione **Configuración** > **Configuración del sistema** > **servidor de administración de claves**.

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.
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. • Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos en un sitio específico. • 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. **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. **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**.

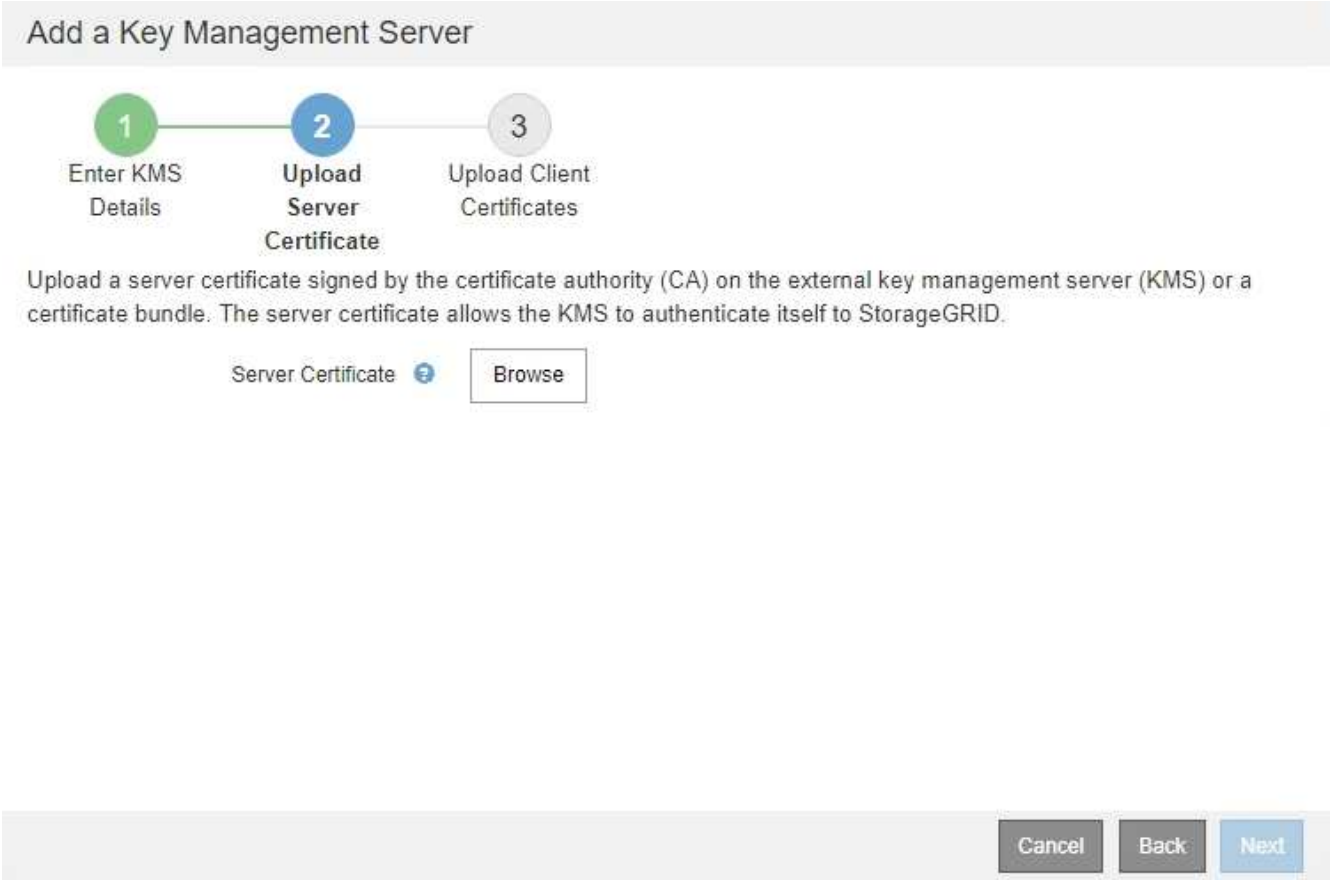
   Aparece el paso 2 (cargar certificado de servidor) del asistente Añadir un servidor de gestión de claves.

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.

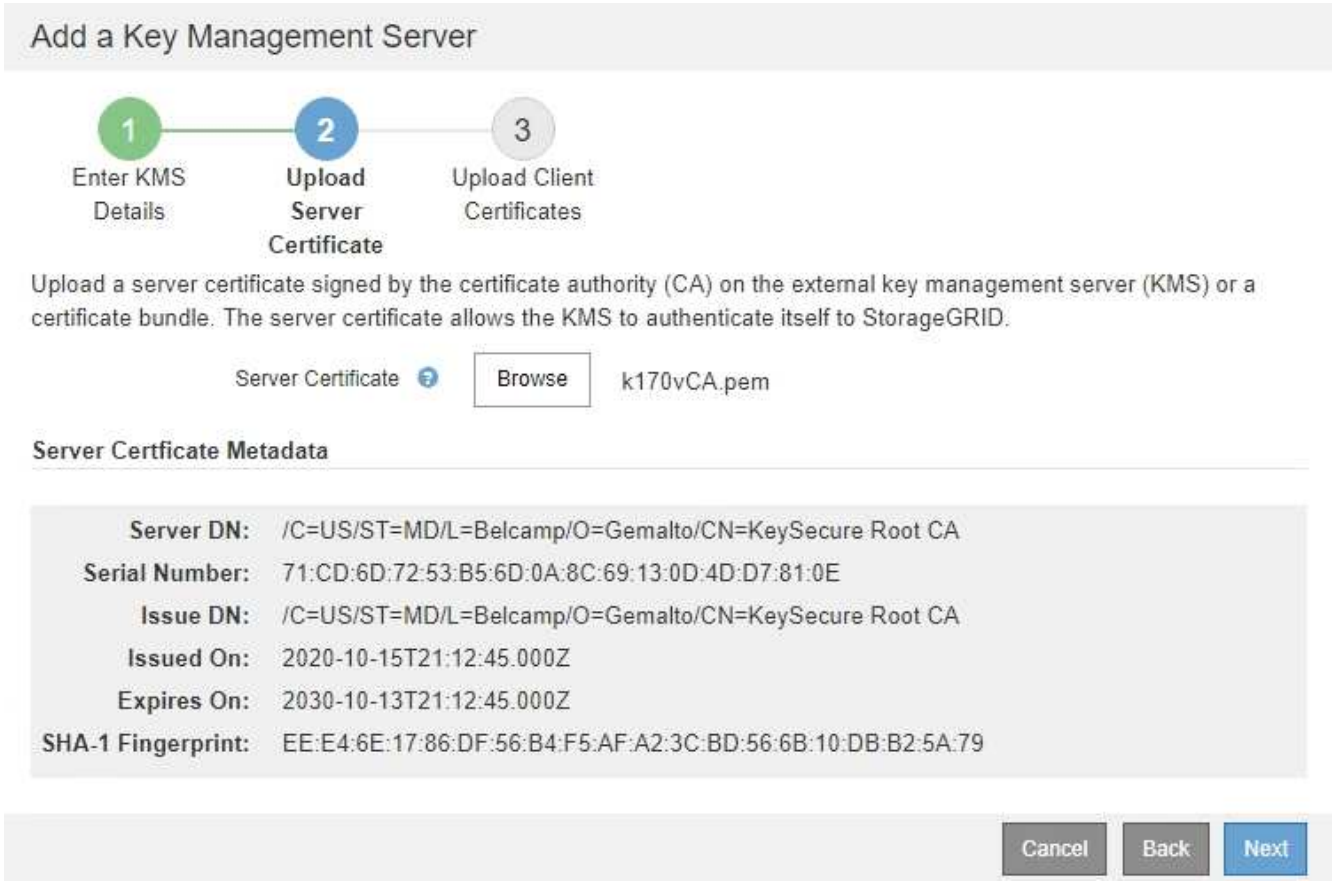
Pasos

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**.

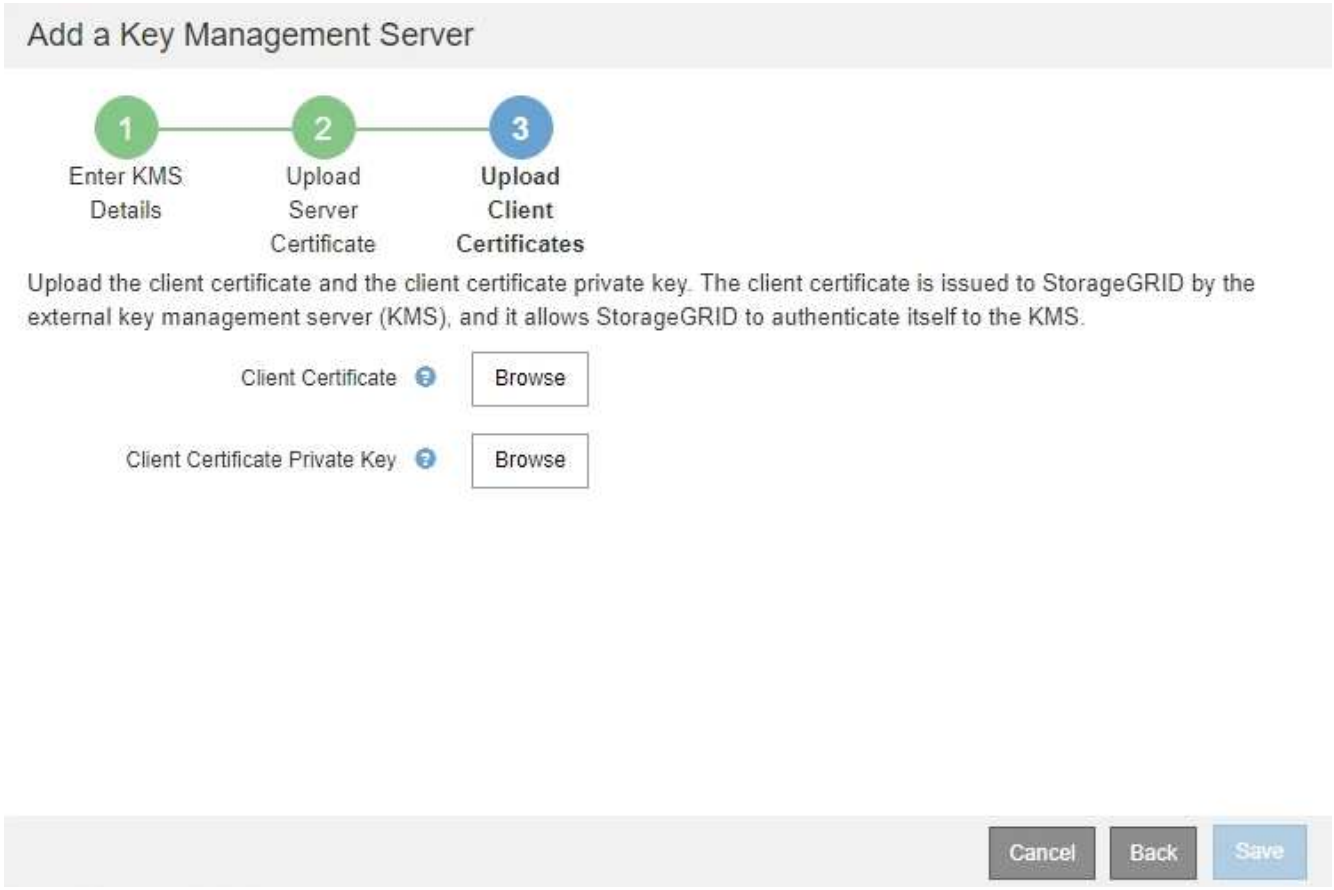
   Aparece el paso 3 (cargar certificados de cliente) del asistente Agregar un servidor de gestión de claves.

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.

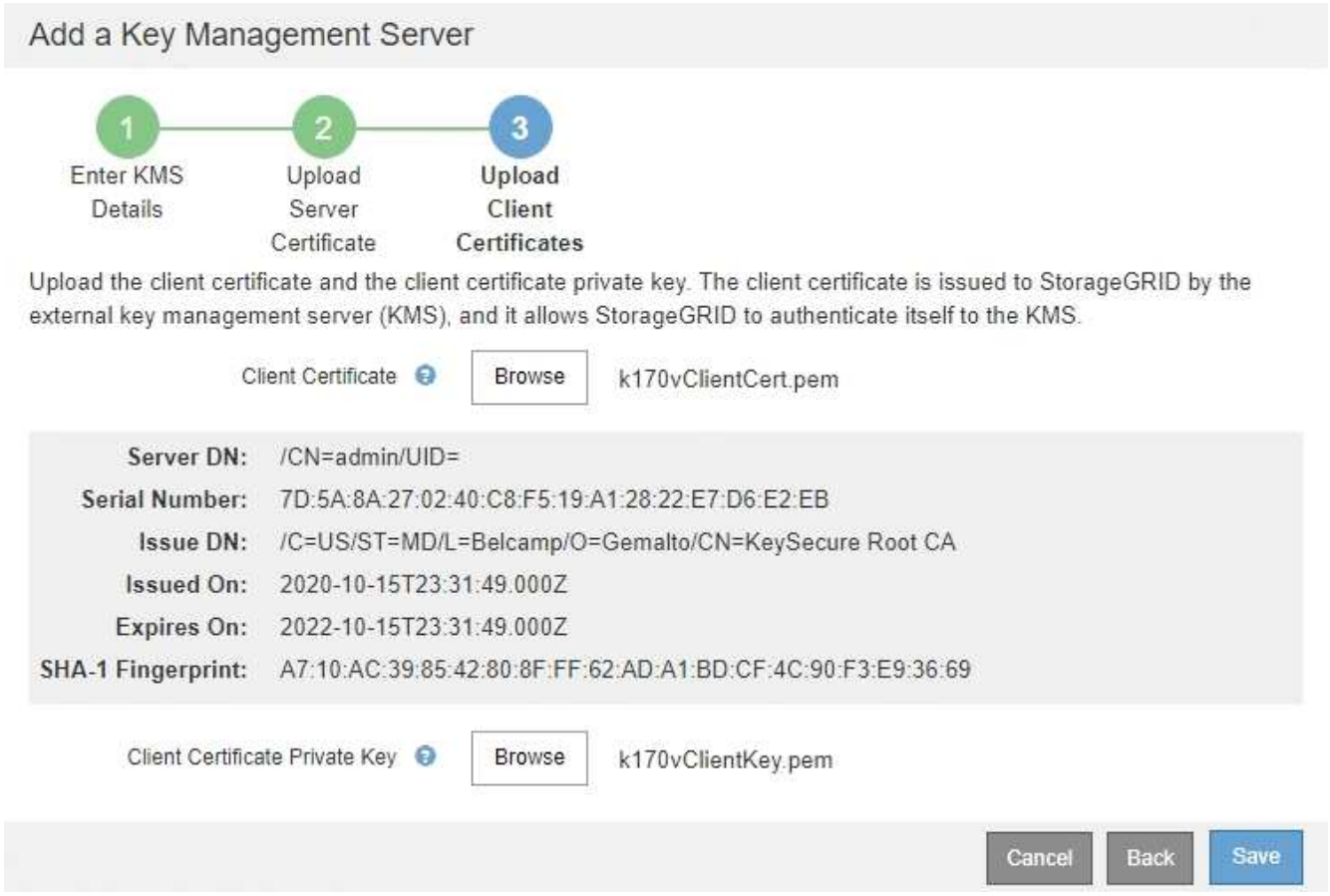


2. Cargue el archivo de certificado de cliente.

   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**.

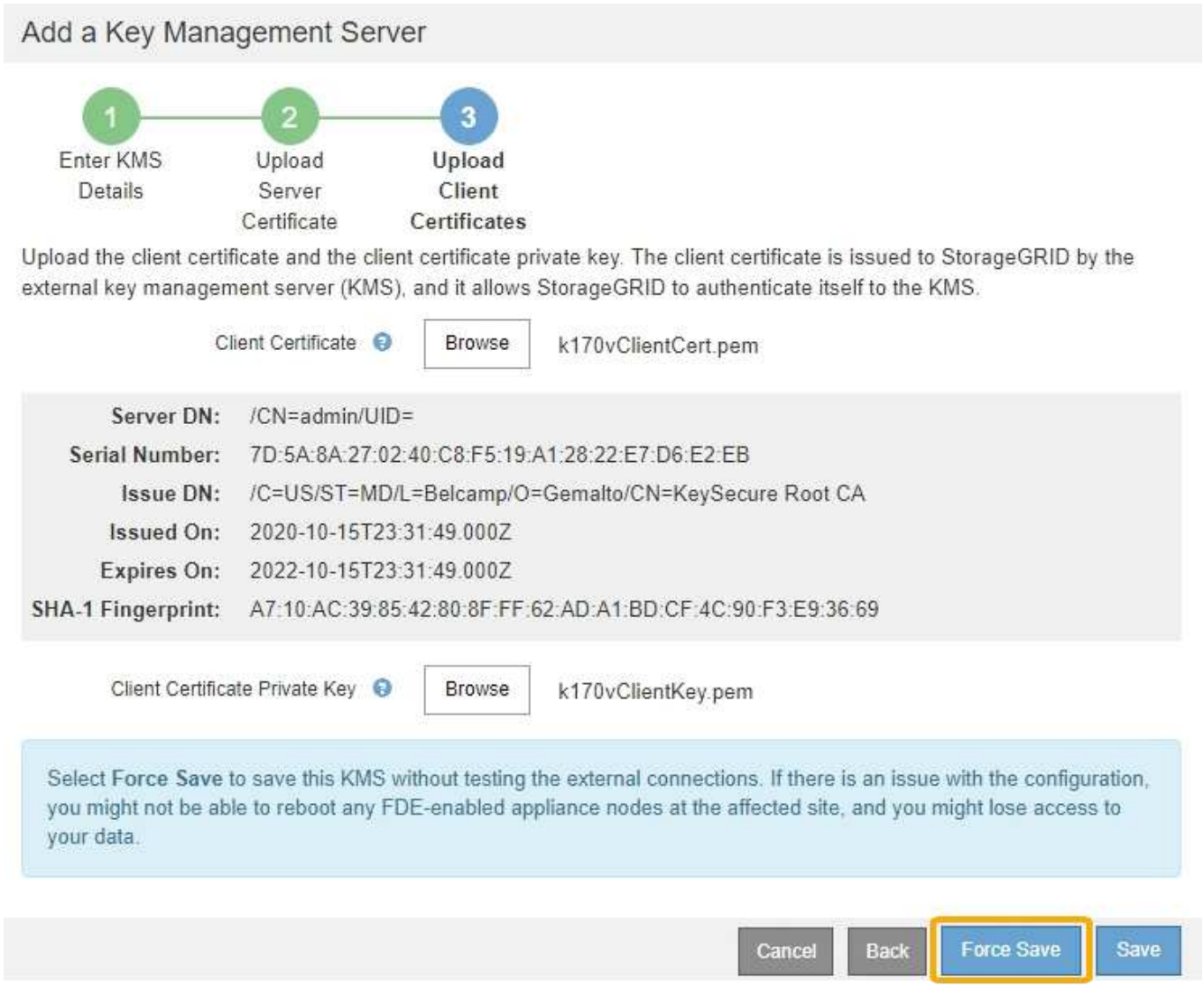
   Se prueban las conexiones entre el servidor de gestión de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves nuevo se añade a la tabla de la página del servidor de gestión de claves.

   > 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**.

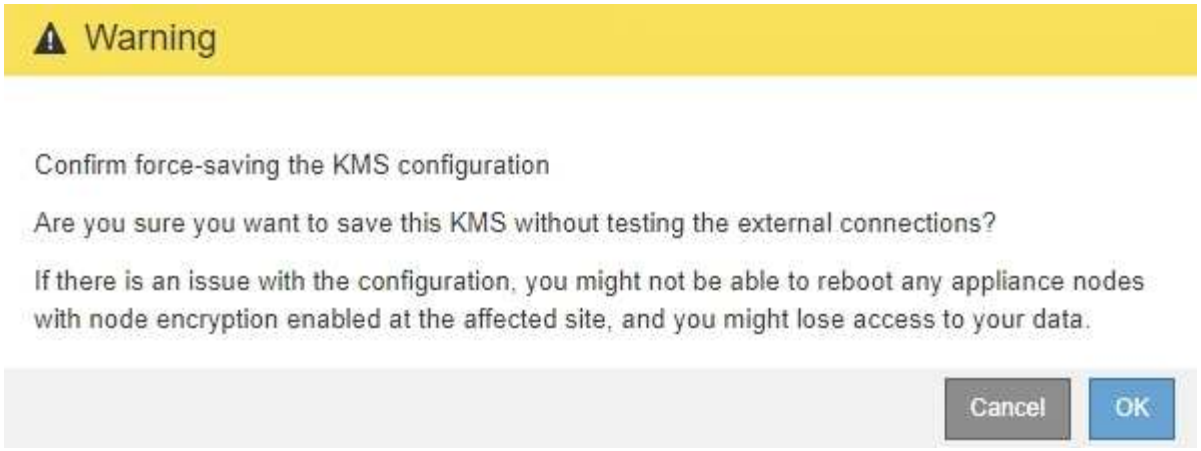
   Por ejemplo, puede recibir un error 422: Entidad no procesable si se produjo un error en una prueba de conexión.

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.

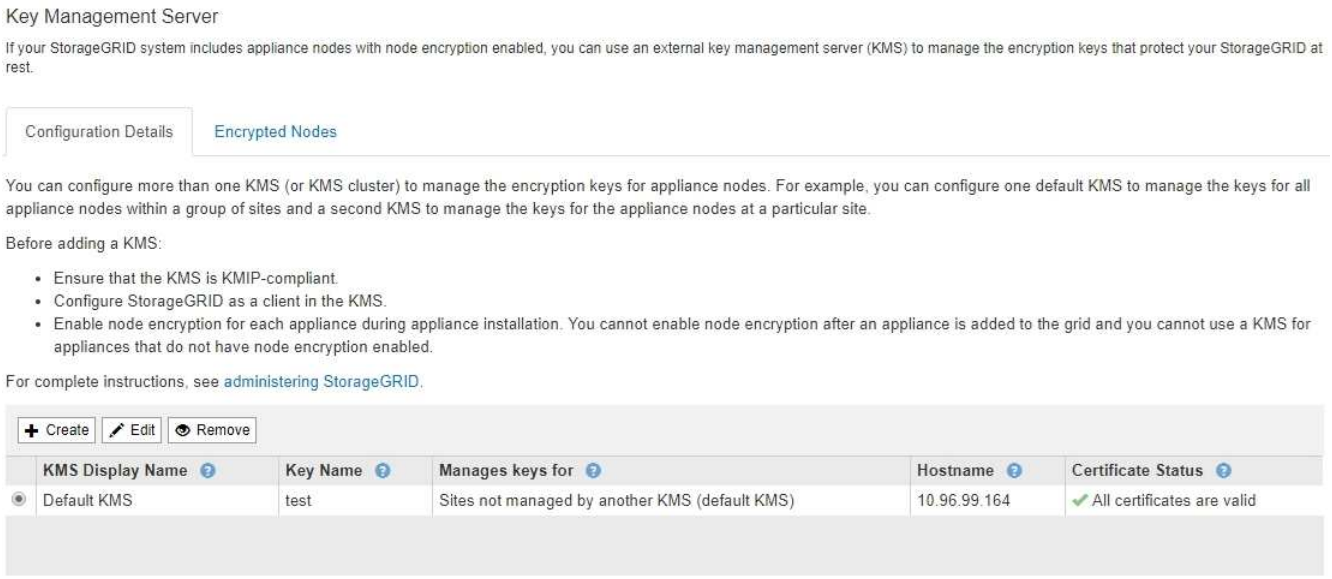
Ver detalles de KMS

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** > **Configuración del sistema** > **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. 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. 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. Por ejemplo: `10.10.10.10 and 10.10.10.11` o. `10.10.10.10 and 2 others`. 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. **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 supervisar y solucionar problemas de StorageGRID.

Debe solucionar cualquier problema con los certificados Lo antes posible. para mantener el acceso a los datos.

Información relacionada

"Solución de problemas de monitor"

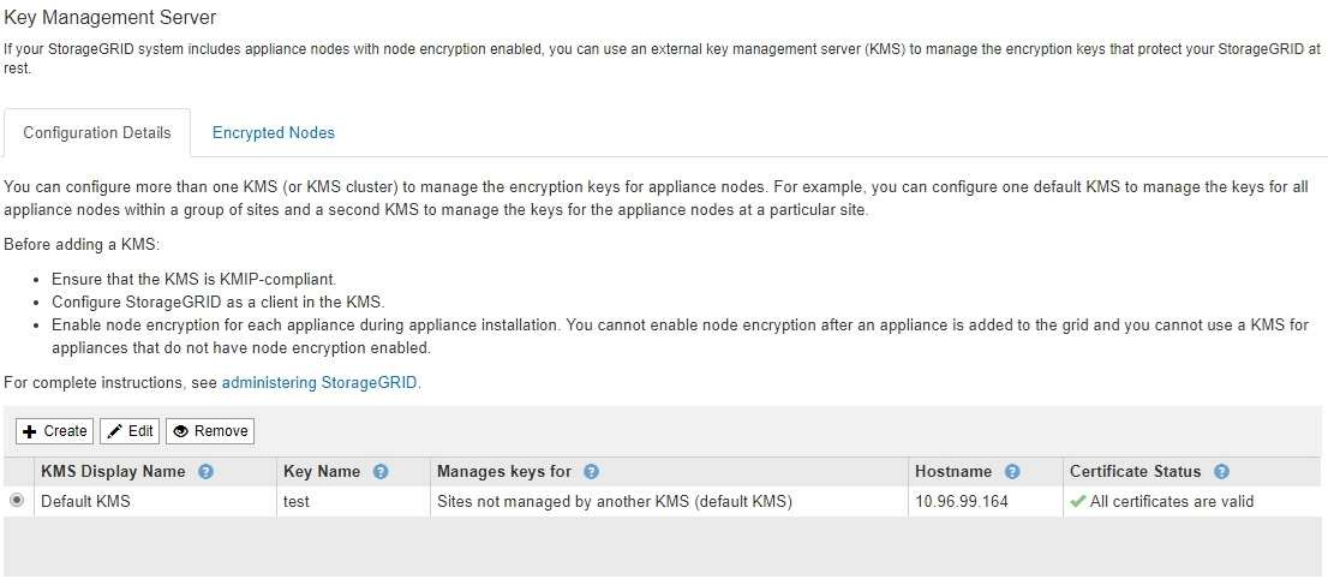
Ver nodos cifrados

Puede ver información acerca de los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

Pasos

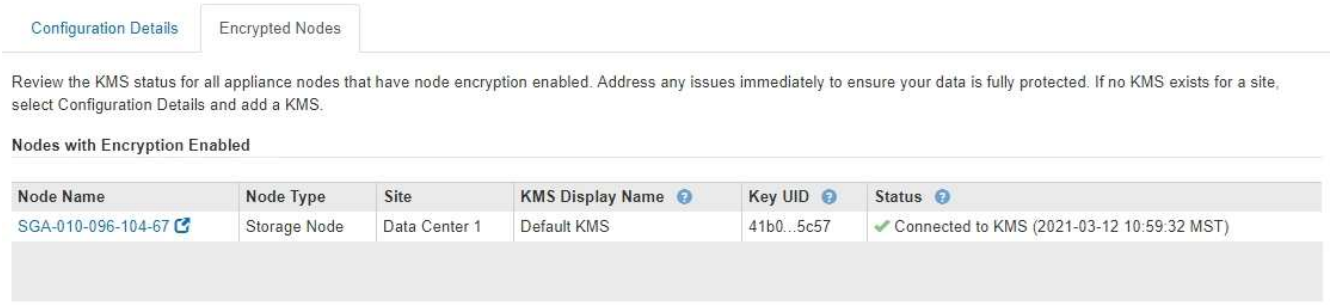
1. Seleccione **Configuración** > **Configuración del sistema** > **servidor de administración de claves**.

   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. Si no aparece ningún KMS, seleccione la ficha Detalles de configuración para agregar un KMS. "Adición de 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. 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. **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 para supervisar y solucionar problemas de StorageGRID.

> Debe solucionar cualquier problema inmediatamente para garantizar que los datos están totalmente protegidos.

Información relacionada

"Solución de problemas de monitor"

Edición de 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.

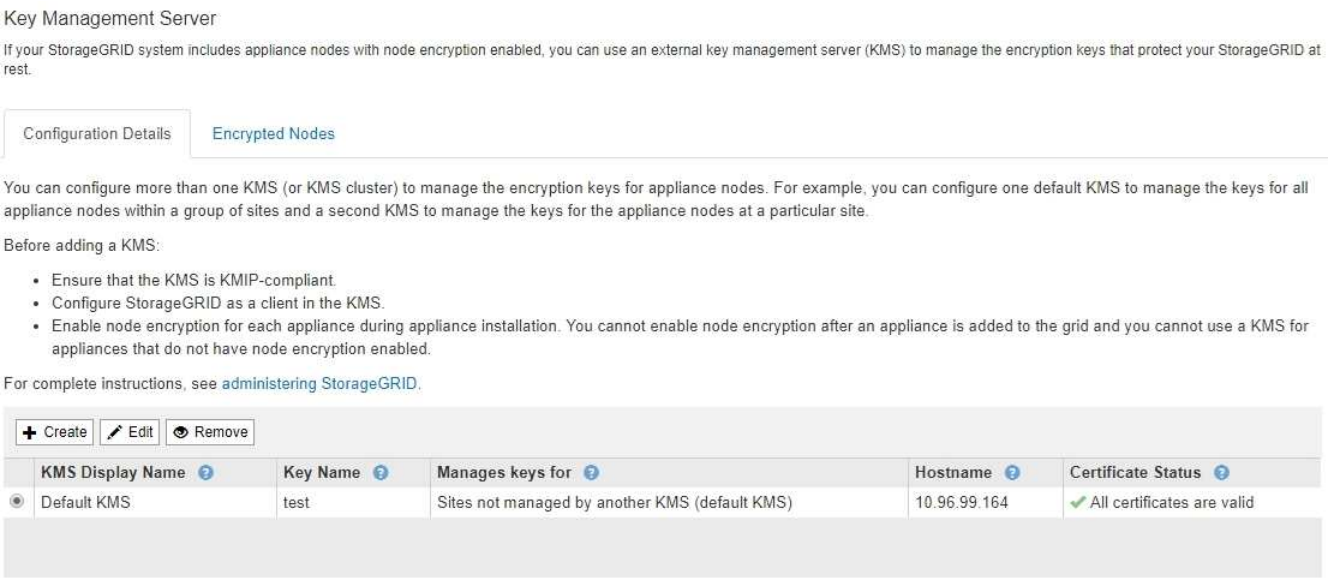
Lo que necesitará

- Debe haber revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Si planea actualizar el sitio seleccionado para un KMS, debe haber revisado el "Consideraciones para cambiar el KMS de un sitio".
- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Pasos

1. Seleccione **Configuración** > **Configuración del sistema** > **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. 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. 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. "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. **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.

Campo	Descripción
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **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**.

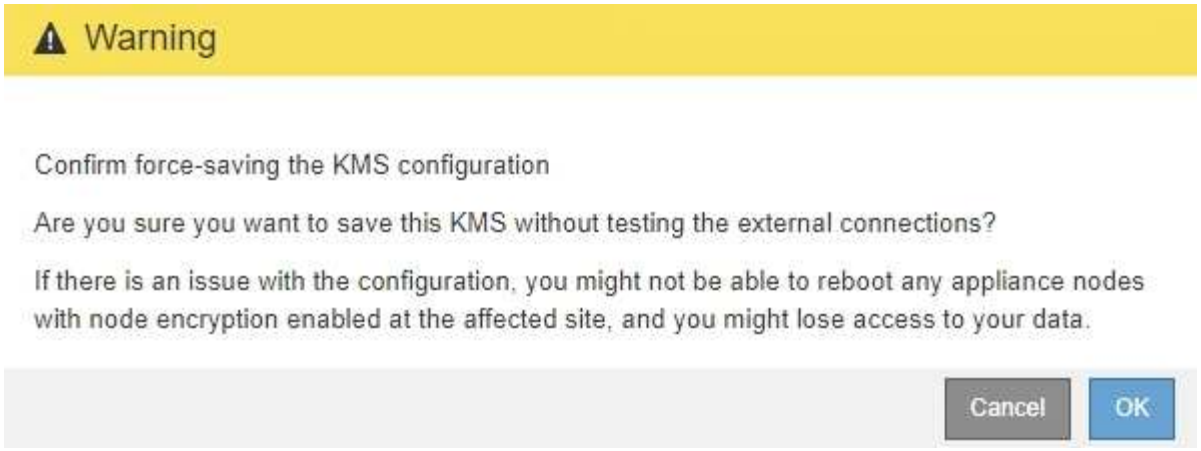
    Por ejemplo, puede recibir un error 422: Entidad no procesable si el sitio seleccionado para este KMS ya está administrado por otro KMS o si se produjo un error en una prueba de conexión.

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.

Eliminar 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

- Debe haber revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Acerca de esta tarea

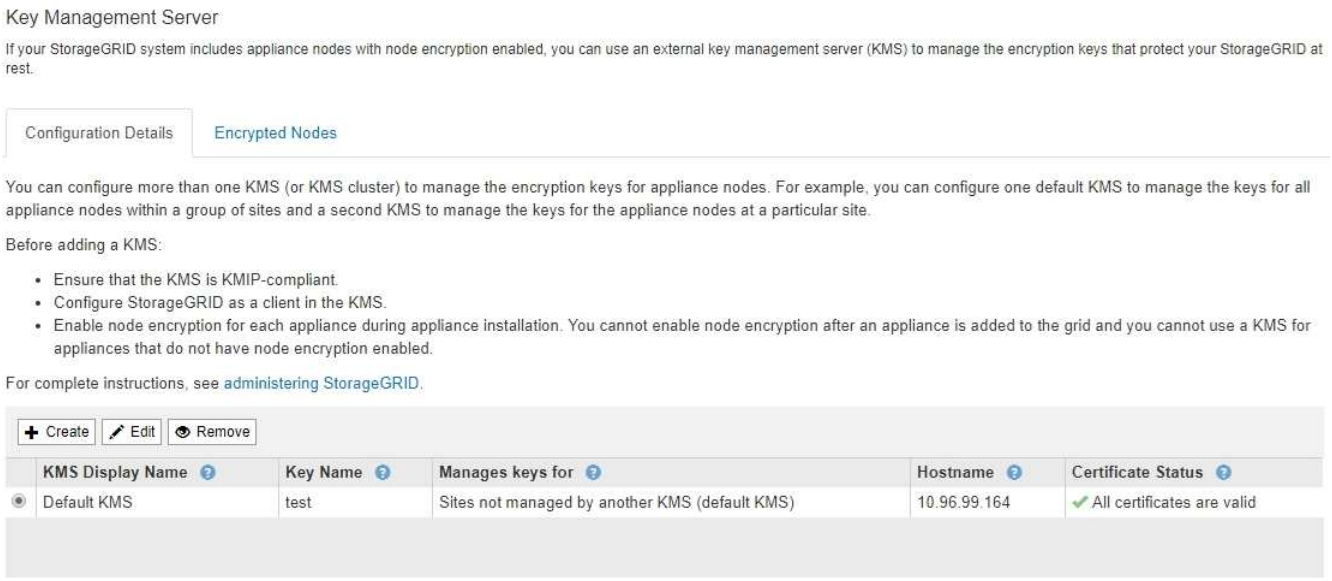
Puede eliminar un KMS en los siguientes casos:

- 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.

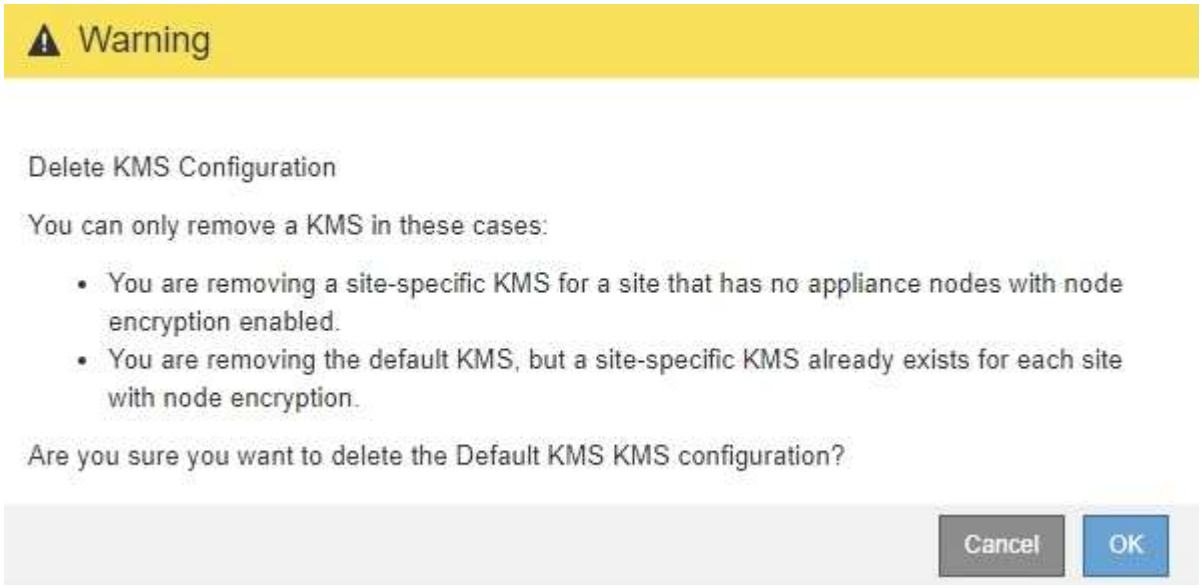
Pasos

1. Seleccione **Configuración** > **Configuración del sistema** > **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.

Gestión de 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.

Que son las cuentas de inquilino

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.

Crear y configurar 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.

  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.

Configuración de inquilinos de 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.

Configurar 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 acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access 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"

Crear una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema de StorageGRID.

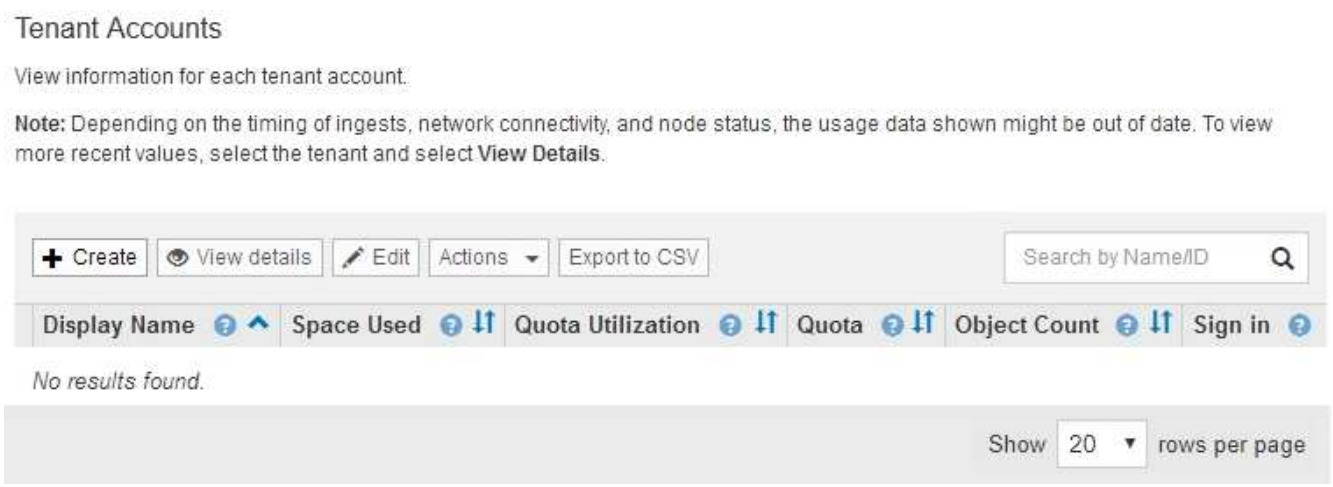
Lo que necesitará

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

Pasos

1. Seleccione **arrendatarios**.

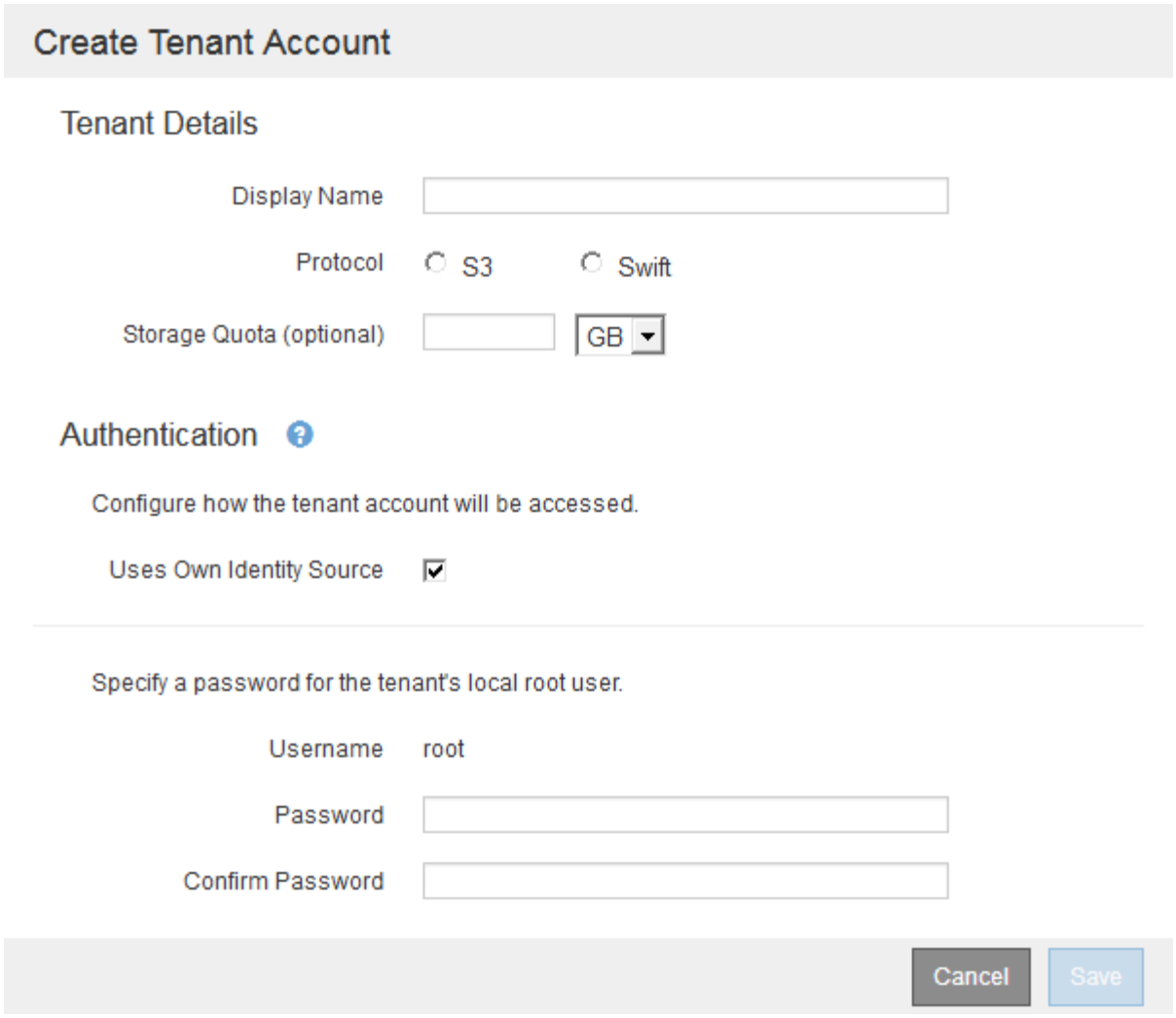
   Aparece la página Cuentas de arrendatarios y enumera todas las cuentas de arrendatario existentes.



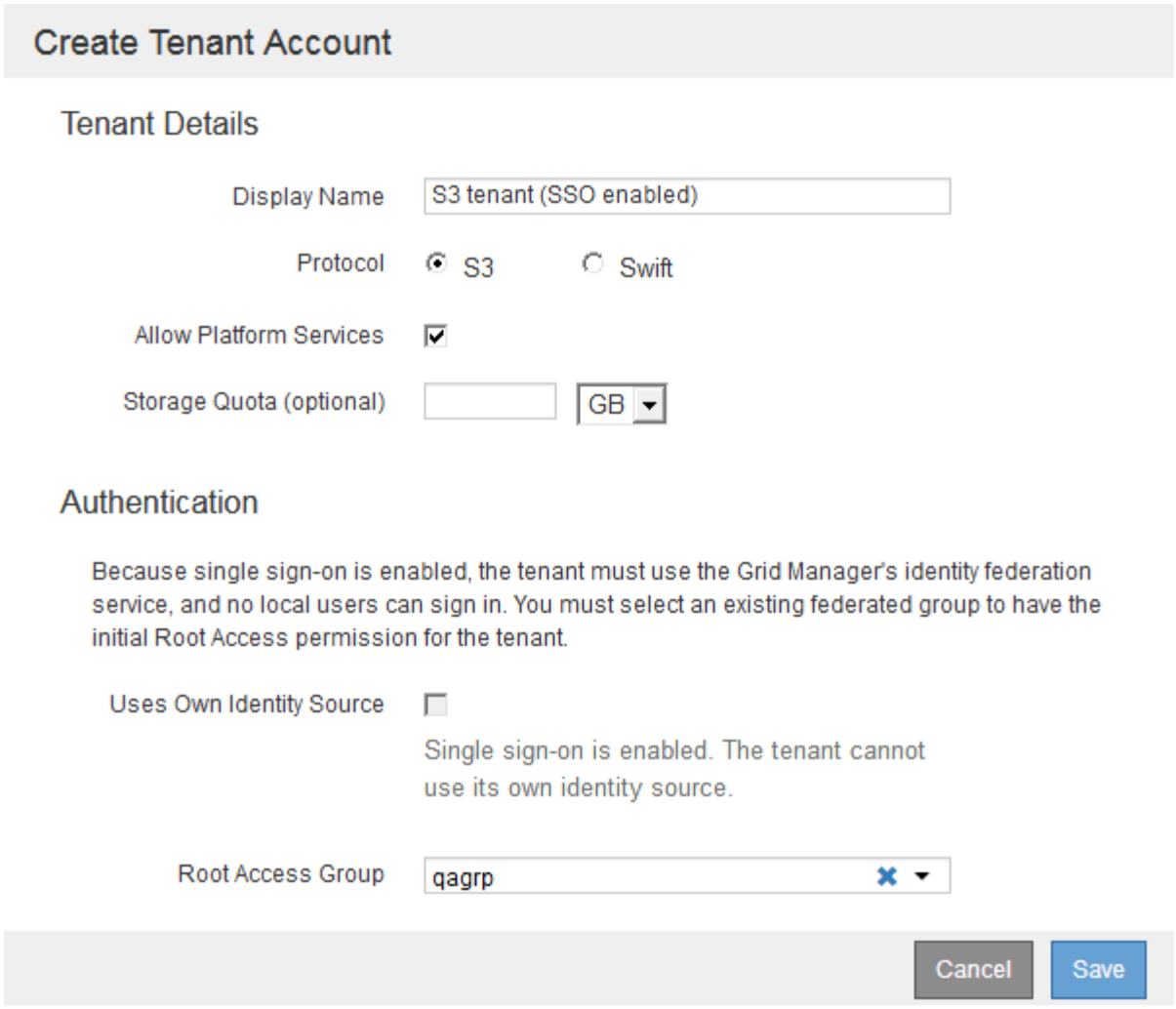
2. Seleccione **Crear**.

   Aparece la página Crear cuenta de inquilino. Los campos incluidos en la página dependen de si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID.

   - Si no se utiliza SSO, la página Crear cuenta de inquilino tiene el aspecto siguiente.



- Si SSO está habilitado, la página Crear cuenta de inquilino tiene el aspecto siguiente.



Información relacionada

"Mediante la federación de identidades"

"Configuración del inicio de sesión único"

Creación de una cuenta de inquilino si StorageGRID no utiliza SSO

Al crear una cuenta de inquilino, se especifica un nombre, un protocolo de cliente y, opcionalmente, una cuota de almacenamiento. Si StorageGRID no utiliza el inicio de sesión único (SSO), también debe especificar si la cuenta de inquilino usará su propio origen de identidad y configurar la contraseña inicial para el usuario raíz local del inquilino.

Acerca de esta tarea

Si la cuenta de arrendatario utilizará el origen de identidad configurado para el Administrador de grid y desea otorgar el permiso acceso raíz para la cuenta de arrendatario a un grupo federado, debe haber importado ese grupo federado en el Gestor de grid. No es necesario asignar ningún permiso de Grid Manager a este grupo de administración. Consulte las instrucciones para "gestión de los grupos de administración".

Pasos

1. En el cuadro de texto **Nombre para mostrar**, introduzca un nombre para mostrar para esta cuenta de

arrendatario.

No es necesario que los nombres de presentación sean únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.

2. Seleccione el protocolo de cliente que utilizará esta cuenta de arrendatario, ya sea **S3** o **Swift**.
3. Para las cuentas de inquilinos S3, mantenga seleccionada la casilla de verificación **permitir servicios de plataforma** a menos que no desee que este inquilino utilice servicios de plataforma para bloques S3.

   Si se habilitan los servicios de plataforma, un inquilino puede usar características, como la replicación de CloudMirror, que accedan a servicios externos. Puede que desee deshabilitar el uso de estas funciones para limitar la cantidad de ancho de banda de red u otros recursos que consume un cliente. Consulte «gestionar servicios de plataforma».

4. En el cuadro de texto **cuota de almacenamiento**, introduzca opcionalmente el número máximo de gigabytes, terabytes o petabytes que desea poner a disposición de los objetos de este arrendatario. A continuación, seleccione las unidades en la lista desplegable.

   Deje este campo en blanco si desea que este arrendatario tenga una cuota ilimitada.

   > La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco). Las copias de ILM y la codificación de borrado no contribuyen a la cantidad de cuota utilizada. Si se supera la cuota, la cuenta de arrendatario no puede crear nuevos objetos.

   > Para supervisar el uso de almacenamiento de cada cuenta de inquilino, seleccione **uso**. Las cuentas de inquilino también pueden supervisar su propio uso de almacenamiento desde la consola de Administrador de inquilinos o con la API de gestión de inquilinos. Tenga en cuenta que los valores de uso de almacenamiento de un inquilino pueden dejar de estar actualizados si los nodos están aislados de otros nodos del grid. Los totales se actualizarán cuando se restaure la conectividad de red.

5. Si el inquilino va a administrar sus propios grupos y usuarios, siga estos pasos.
   a. Seleccione la casilla de verificación **usa el origen de identidad propio** (predeterminado).

      > Si esta casilla de verificación está seleccionada y desea utilizar la federación de identidades para grupos de inquilinos y usuarios, el inquilino debe configurar su propio origen de identidad. Consulte las instrucciones de uso de cuentas de inquilino.

   b. Especifique una contraseña para el usuario raíz local del inquilino.
6. Si el inquilino utilizará los grupos y usuarios configurados para el administrador de grid, siga estos pasos.
   a. Anule la selección de la casilla de verificación **usa el origen de identidad propio**.
   b. Realice una o ambas de las siguientes acciones:
      - En el campo Grupo de acceso raíz, seleccione un grupo federado existente en el Administrador de grid que tenga el permiso acceso raíz inicial para el arrendatario.

        > Si dispone de los permisos adecuados, los grupos federados existentes del Gestor de grid se mostrarán al hacer clic en el campo. De lo contrario, introduzca el nombre exclusivo del grupo.

- Especifique una contraseña para el usuario raíz local del inquilino.

7. Haga clic en **Guardar**.

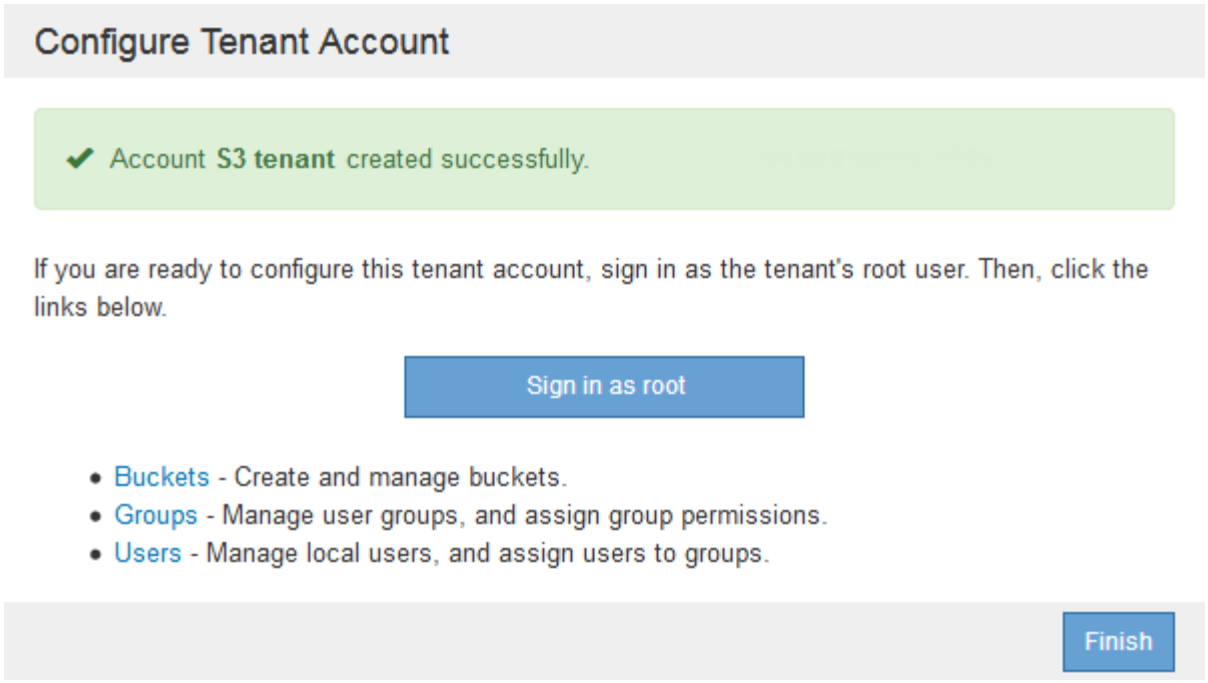
   Se crea la cuenta de inquilino.

8. De manera opcional, acceda al nuevo inquilino. De lo contrario, vaya al paso correspondiente acceder al inquilino más tarde.

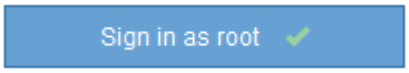
Si está…	Realice lo siguiente…
Acceso a Grid Manager en un puerto restringido	Haga clic en **restringido** para obtener más información sobre cómo acceder a esta cuenta de arrendatario. La dirección URL del administrador de inquilinos tiene el siguiente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *`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
Acceso a Grid Manager en el puerto 443 pero no ha establecido una contraseña para el usuario raíz local	Haga clic en **Iniciar sesión** e introduzca las credenciales de un usuario en el grupo federado de acceso raíz.
Acceso a Grid Manager en el puerto 443 y una contraseña para el usuario raíz local	Vaya al paso siguiente a. inicie sesión como raíz.

9. Iniciar sesión en el arrendatario como root:

   a. En el cuadro de diálogo Configurar cuenta de inquilino, haga clic en el botón **Iniciar sesión como raíz**.



Aparece una Marca de verificación verde en el botón, que indica que ahora ha iniciado sesión en la cuenta de arrendatario como usuario root.



a. Haga clic en los vínculos para configurar la cuenta de arrendatario.

   Cada enlace abre la página correspondiente en el Administrador de arrendatarios. Para completar la página, consulte las instrucciones de uso de cuentas de arrendatario.

b. Haga clic en **Finalizar**.

10. para acceder al arrendatario más adelante:

Si está usando…	Realice una de estas…
Puerto 443	• En Grid Manager, seleccione **arrendatarios** y haga clic en **Iniciar sesión** a la derecha del nombre del arrendatario. • Introduzca la URL del inquilino en un navegador web: `https://FQDN_or_Admin_Node_IP/?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 ◦ *`20-digit-account-id`* Es el ID de cuenta único del inquilino

Si está usando…	Realice una de estas…
Un puerto restringido	• En Grid Manager, seleccione **arrendatarios** y haga clic en **restringido**. • Introduzca la URL del inquilino en un navegador web: `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 restringido solo para inquilinos ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino

Información relacionada

"Controlar el acceso mediante firewalls"

"Se gestionan los servicios de la plataforma para cuentas de inquilinos de S3"

"Usar una cuenta de inquilino"

Creación de una cuenta de inquilino si SSO está habilitado

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.

Pasos

1. En el cuadro de texto **Nombre para mostrar**, introduzca un nombre para mostrar para esta cuenta de arrendatario.

   No es necesario que los nombres de presentación sean únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.

2. Seleccione el protocolo de cliente que utilizará esta cuenta de arrendatario, ya sea **S3** o **Swift**.
3. Para las cuentas de inquilinos S3, mantenga seleccionada la casilla de verificación **permitir servicios de plataforma** a menos que no desee que este inquilino utilice servicios de plataforma para bloques S3.

   Si se habilitan los servicios de plataforma, un inquilino puede usar características, como la replicación de CloudMirror, que accedan a servicios externos. Puede que desee deshabilitar el uso de estas funciones para limitar la cantidad de ancho de banda de red u otros recursos que consume un cliente. Consulte «gestionar servicios de plataforma».

4. En el cuadro de texto **cuota de almacenamiento**, introduzca opcionalmente el número máximo de gigabytes, terabytes o petabytes que desea poner a disposición de los objetos de este arrendatario. A continuación, seleccione las unidades en la lista desplegable.

   Deje este campo en blanco si desea que este arrendatario tenga una cuota ilimitada.

La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco). Las copias de ILM y la codificación de borrado no contribuyen a la cantidad de cuota utilizada. Si se supera la cuota, la cuenta de arrendatario no puede crear nuevos objetos.

Para supervisar el uso de almacenamiento de cada cuenta de inquilino, seleccione **uso**. Las cuentas de inquilino también pueden supervisar su propio uso de almacenamiento desde la consola de Administrador de inquilinos o con la API de gestión de inquilinos. Tenga en cuenta que los valores de uso de almacenamiento de un inquilino pueden dejar de estar actualizados si los nodos están aislados de otros nodos del grid. Los totales se actualizarán cuando se restaure la conectividad de red.

5. Observe que la casilla de verificación **usa el origen de identidades** está desactivada y desactivada.

   Dado que SSO está habilitado, el inquilino debe utilizar el origen de identidades configurado para Grid Manager. Ningún usuario local puede iniciar sesión.

6. En el campo **Grupo de acceso raíz**, seleccione un grupo federado existente en Grid Manager para tener el permiso acceso raíz inicial para el arrendatario.

   Si dispone de los permisos adecuados, los grupos federados existentes del Gestor de grid se mostrarán al hacer clic en el campo. De lo contrario, introduzca el nombre exclusivo del grupo.

7. Haga clic en **Guardar**.

   Se crea la cuenta de inquilino. Aparece la página Cuentas de arrendatarios e incluye una fila para el nuevo arrendatario.

8. Si es usuario del grupo acceso raíz, haga clic opcionalmente en el enlace **Iniciar sesión** para que el nuevo arrendatario acceda inmediatamente al Administrador de arrendatarios, donde puede configurar el arrendatario. De lo contrario, proporcione la dirección URL para el enlace **Iniciar sesión** al administrador de la cuenta del inquilino. (La URL de un inquilino es el nombre de dominio completo o la dirección IP de cualquier nodo de administrador, seguido de `/?accountId=20-digit-account-id`.)

   Se muestra un mensaje de acceso denegado si hace clic en **Iniciar sesión**, pero no pertenece al grupo acceso raíz de la cuenta de arrendatario.

Información relacionada

"Configuración del inicio de sesión único"

"Se gestionan los servicios de la plataforma para cuentas de inquilinos de S3"

"Usar una cuenta de inquilino"

Cambiar la contraseña del usuario raíz local de un 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

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

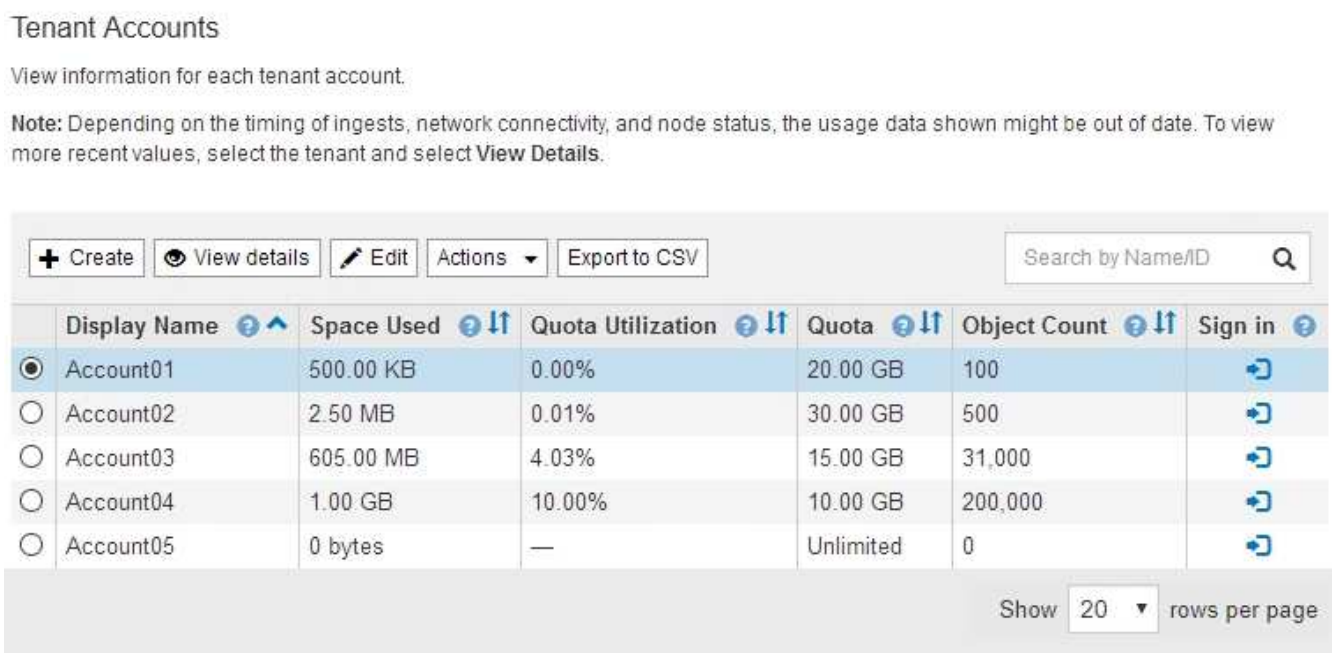
Acerca de esta tarea

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**.

   Aparece la página Cuentas de arrendatario y enumera todas las cuentas de arrendatario existentes.

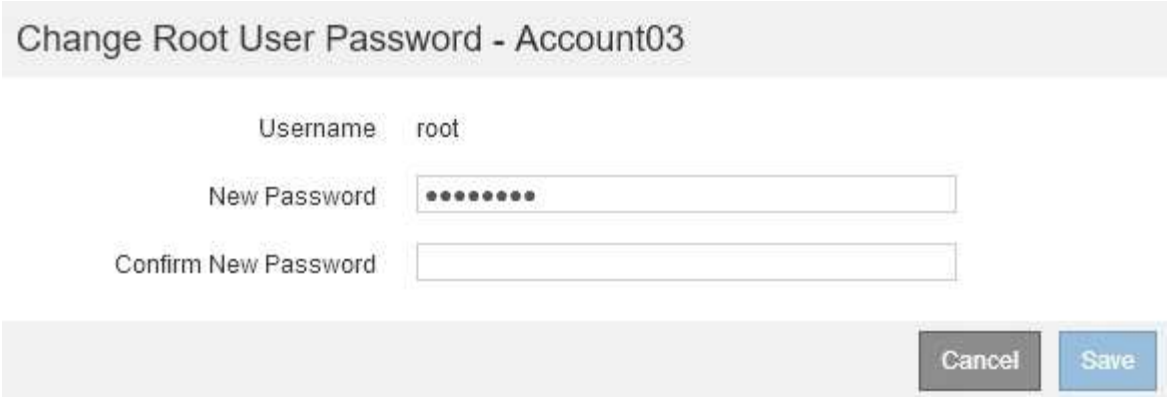


2. Seleccione la cuenta de arrendatario que desee editar.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre para mostrar o ID de inquilino.

   Los botones Ver detalles, Editar y acciones se habilitan.

3. En el menú desplegable **acciones**, seleccione **Cambiar contraseña raíz**.



4. Introduzca la nueva contraseña de la cuenta de inquilino.
5. Seleccione **Guardar**.

Información relacionada

"Controlando el acceso del administrador a StorageGRID"

Edición de una 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.

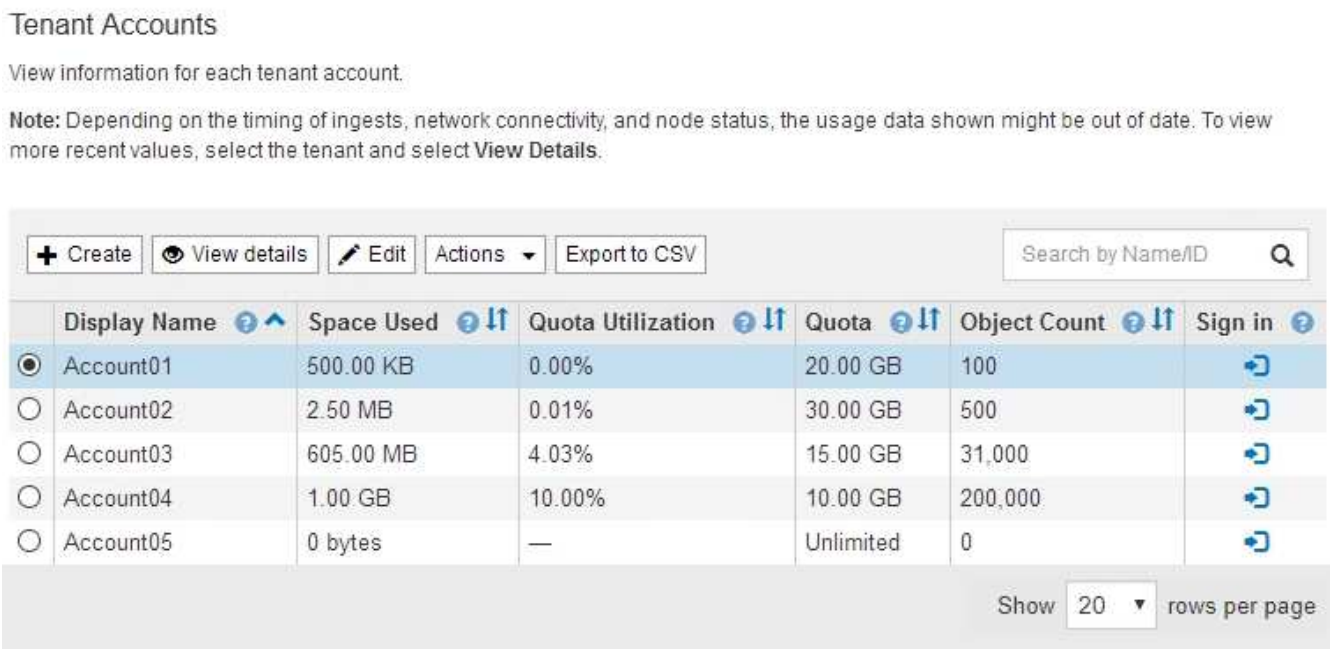
Lo que necesitará

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

Pasos

1. Seleccione **arrendatarios**.

   Aparece la página Cuentas de arrendatario y enumera todas las cuentas de arrendatario existentes.

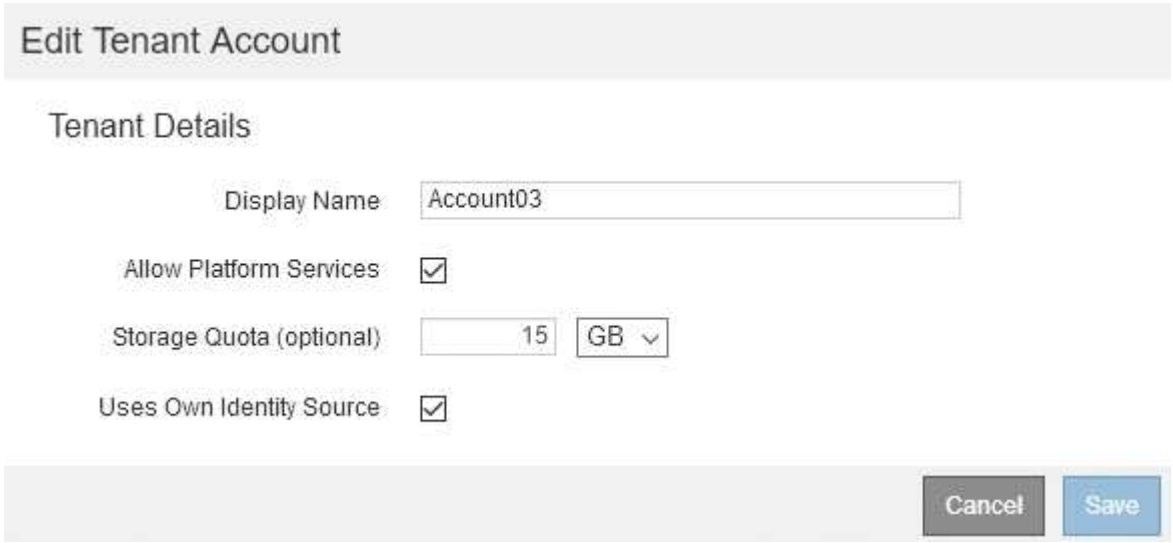


2. Seleccione la cuenta de arrendatario que desee editar.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre para mostrar o ID de inquilino.

3. Seleccione **Editar**.

   Aparece la página Editar cuenta de arrendatario. 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 los campos según sea necesario.
   a. Cambie el nombre para mostrar de esta cuenta de arrendatario.
   b. Cambie la configuración de la casilla de verificación **permitir servicios de plataforma** para determinar si la cuenta de inquilino puede utilizar servicios de plataforma para sus bloques S3.

      Si deshabilita los servicios de plataforma para un inquilino que ya los está utilizando, los servicios que han configurado para sus bloques 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.

   c. Para **cuota de almacenamiento**, cambie el número máximo de gigabytes, terabytes o petabytes disponibles para los objetos de este arrendatario, o deje el campo en blanco si desea que este arrendatario tenga una cuota ilimitada.

      La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco). Las copias de ILM y la codificación de borrado no contribuyen a la cantidad de cuota utilizada.

Para supervisar el uso de almacenamiento de cada cuenta de inquilino, seleccione **uso**. Las cuentas de inquilino también pueden supervisar su propio uso desde la consola de Gestor de inquilinos o con la API de gestión de inquilinos. Tenga en cuenta que los valores de uso de almacenamiento de un inquilino pueden dejar de estar actualizados si los nodos están aislados de otros nodos del grid. Los totales se actualizarán cuando se restaure la conectividad de red.

d. 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.

5. Seleccione **Guardar**.

Información relacionada

"Se gestionan los servicios de la plataforma para cuentas de inquilinos de S3"

"Usar una cuenta de inquilino"

Eliminar una 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 explorador 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.

   Si el sistema incluye más de 20 elementos, puede especificar cuántas filas se muestran en cada página a la vez. Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre para mostrar o ID de inquilino.

3. En el menú desplegable **acciones**, seleccione **Quitar**.
4. Seleccione **OK**.

Información relacionada

"Controlando el acceso del administrador a StorageGRID"

Se gestionan los servicios de la plataforma 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 servicios de plataforma son"
- "Redes y puertos para servicios de plataforma"
- "Entrega de mensajes de servicios de plataforma por sitio"
- "Resolución de problemas de servicios de plataforma"

¿Qué servicios de plataforma son

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, debe tener en cuenta las siguientes recomendaciones:

- 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.
- 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.

Información relacionada

"Usar una cuenta de inquilino"

"Configurando la configuración del proxy de almacenamiento"

"Solución de problemas de monitor"

Redes 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 configurar la configuración del proxy de almacenamiento para permitir que los mensajes se envíen a puntos finales externos, como un punto final de Internet.

Información relacionada

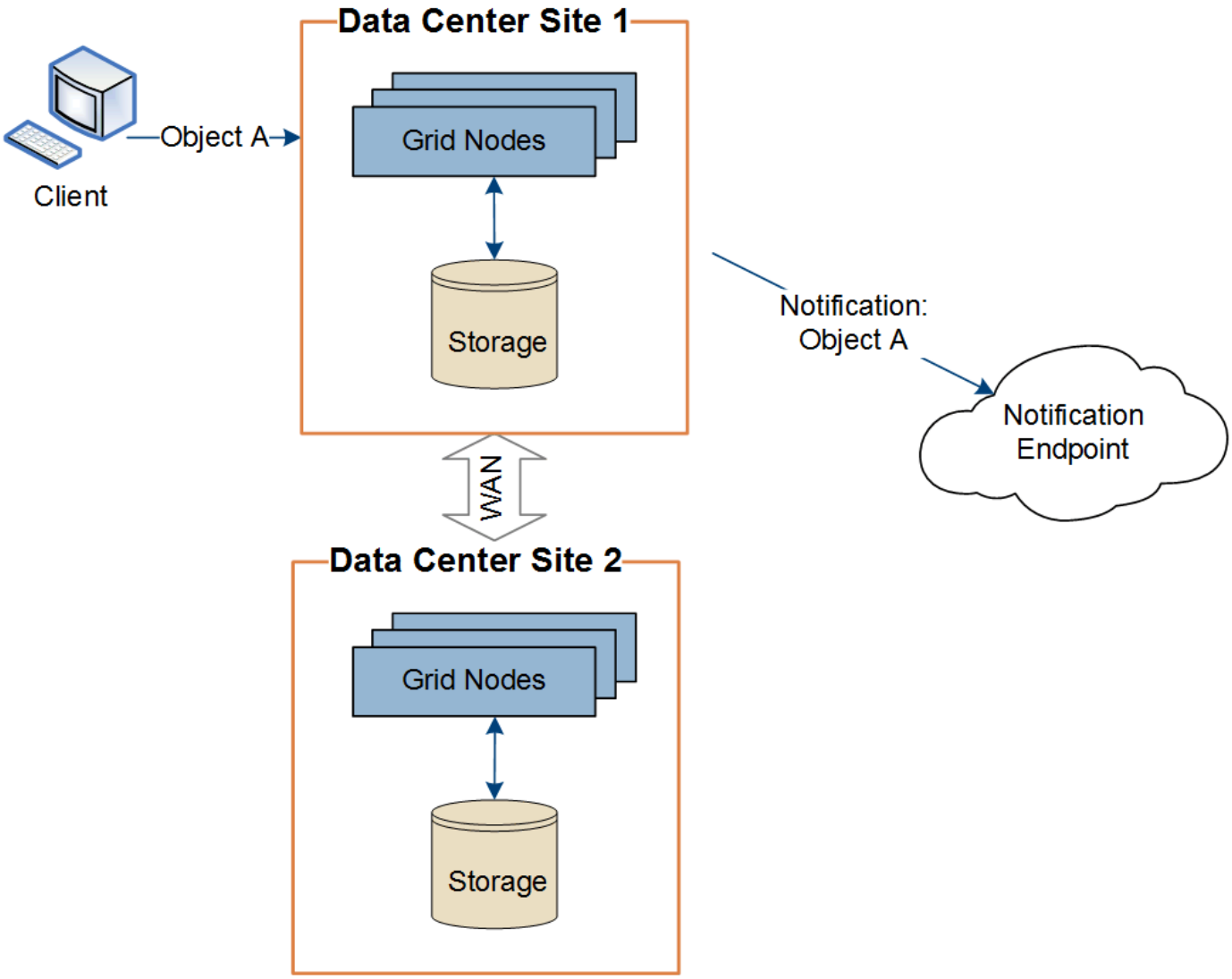
"Configurando la configuración del proxy de almacenamiento"

"Usar una cuenta de inquilino"

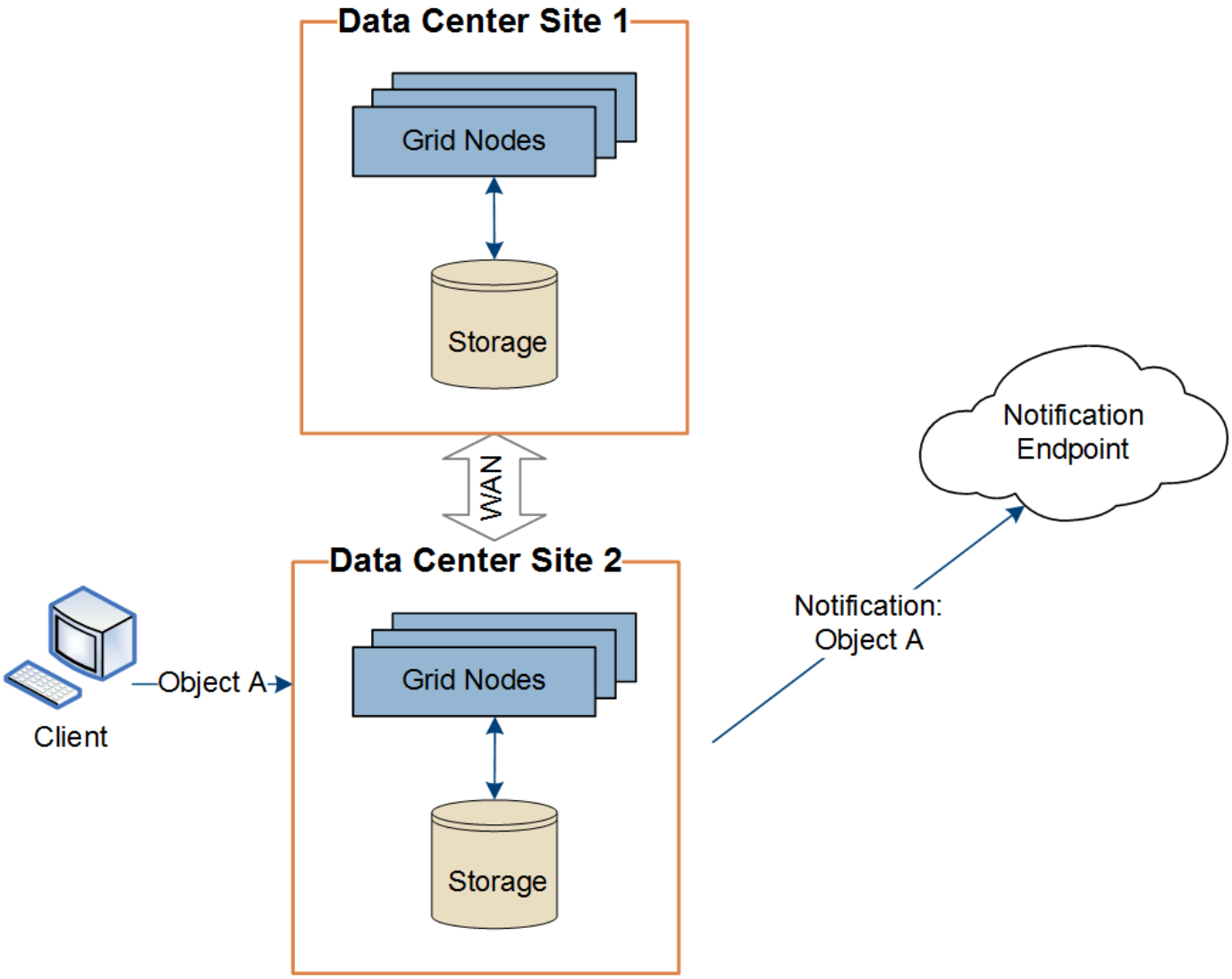
Entrega de mensajes de servicios de plataforma por sitio

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.

Resolución de 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.

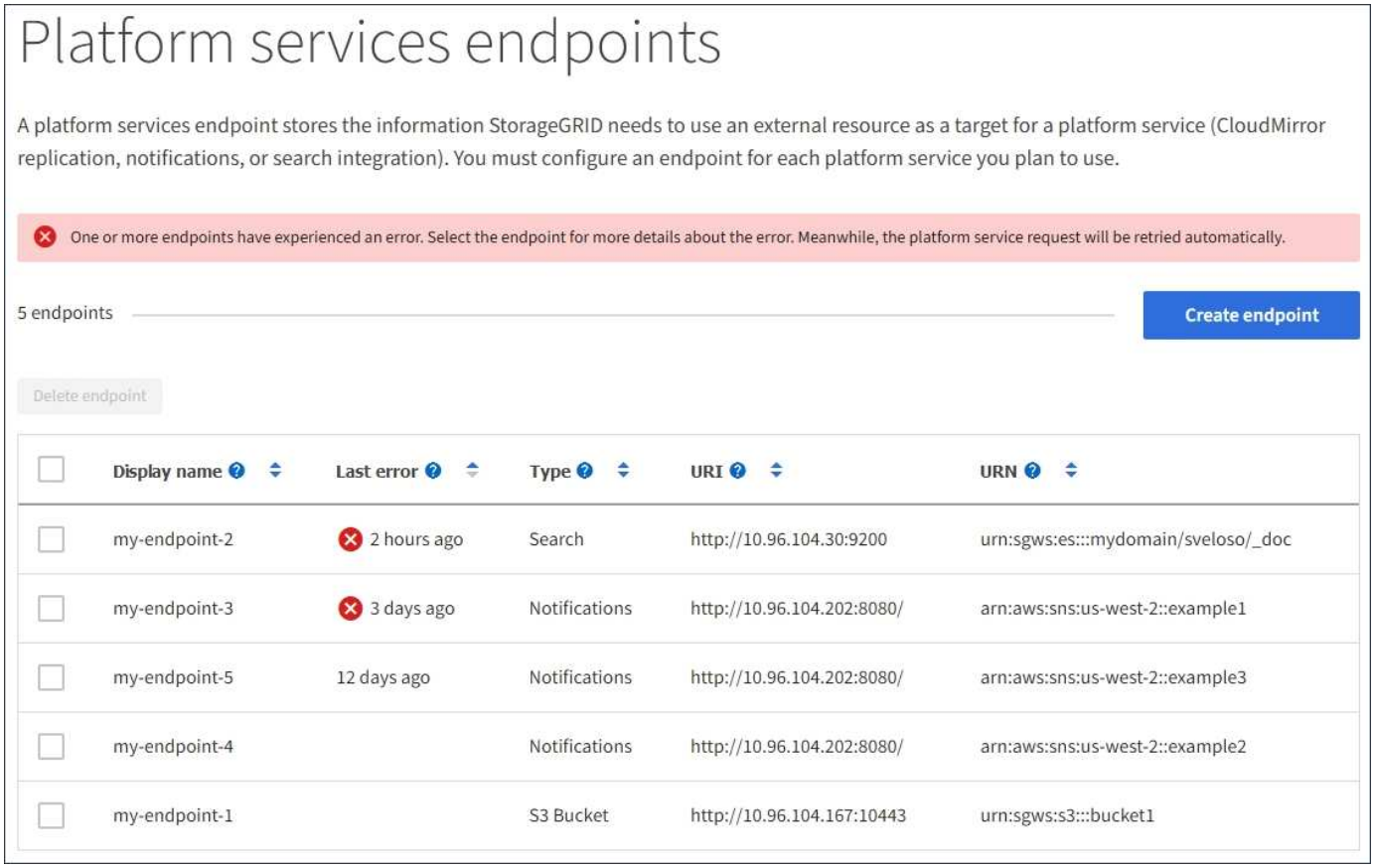
Se producirá un error al crear el extremo si los servicios de plataforma no están habilitados para la cuenta de inquilino.

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.

Determinar 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 **Soporte** > **Herramientas** > **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 total de eventos (SMTT) se activa en el Administrador de grid. Para ver la alarma total de eventos:

1. Seleccione **Nodes**.
2. Seleccione ***site*** > ***grid node*** > **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. Haga clic en **Restablecer 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 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. Consulte el gráfico de tasa de fallos 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 acerca de la solución de problemas de los extremos de servicios de la plataforma, consulte las instrucciones de uso de cuentas de inquilino.

"Usar una cuenta de inquilino"

Información relacionada

"Solución de problemas de monitor"

"Configurando la configuración del proxy de almacenamiento"

Configurar las conexiones de 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:

- **Servicio de equilibrador de carga**: Permite a los clientes utilizar el servicio de equilibrador de carga mediante la creación de puntos finales de equilibrio 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.
- **Grupos de alta disponibilidad**: Puede crear un grupo ha de 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.

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 **Nota:** el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos S3 predeterminados: • HTTPS: 8082 • HTTP: 8084 Puertos Swift predeterminados: • HTTPS:8083 • 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 **Nota:** el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace **Nota:** de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos S3 predeterminados: • HTTPS: 8082 • HTTP: 8084 Puertos Swift predeterminados: • HTTPS:8083 • HTTP: 8085
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: • HTTPS: 18082 • HTTP: 18084 Puertos Swift predeterminados: • HTTPS: 18083 • 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 con un navegador 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. Haga clic en **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** > **Configuración de 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** > **Configuración de red** > **parámetros de equilibrio 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 haga clic en **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, haga clic en **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.

Gestión del equilibrio de carga

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 lograr el equilibrio de carga en el sistema StorageGRID 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.
- Utilice el servicio Connection Load Balancer (CLB), que se instala sólo en nodos Gateway. El servicio CLB proporciona equilibrio de carga de capa 4 y soporta costes de enlace.

  El servicio CLB está 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 (HTTP o HTTPS), un tipo de servicio (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:

- Direcciones IP virtuales de alta disponibilidad (ha) específicas
- Interfaces de red específicas de nodos 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 las instrucciones de recuperación y mantenimiento para eliminar las 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.

Información relacionada

"Mantener recuperar"

Configuración de los extremos del equilibrador de carga

Puede crear, editar y eliminar puntos finales del equilibrador de carga.

Creación de puntos finales del equilibrador de carga

Cada extremo de equilibrio de carga especifica un puerto, un protocolo de red (HTTP o HTTPS) y un tipo de servicio (S3 o Swift). Si se crea un extremo de HTTPS, se debe cargar o generar un certificado de servidor.

Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Si ha reasignado previamente puertos que pretende utilizar para el servicio Load Balancer, debe haber eliminado las reasignaciones.

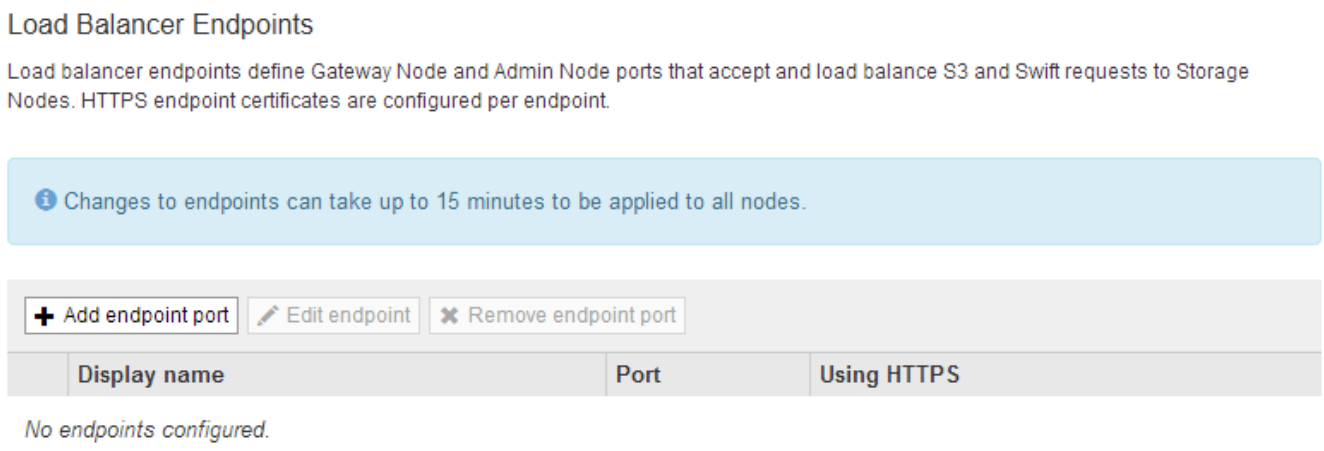
> Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de las instrucciones de recuperación y mantenimiento para eliminar las reasignaciones de puertos.

> El servicio CLB está obsoleto.

Pasos

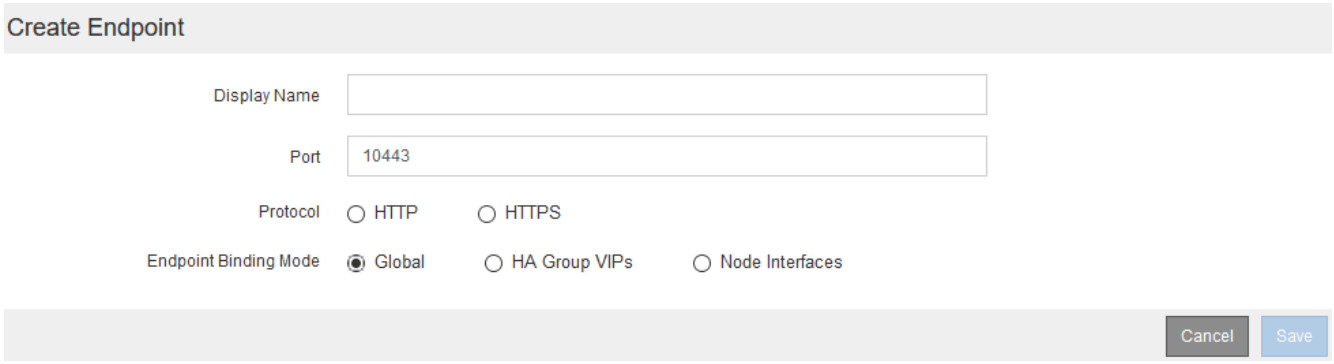
1. Seleccione **Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**.

   Aparece la página Load Balancer Endpoints.



2. Seleccione **Agregar punto final**.

   Se muestra el cuadro de diálogo Create Endpoint.



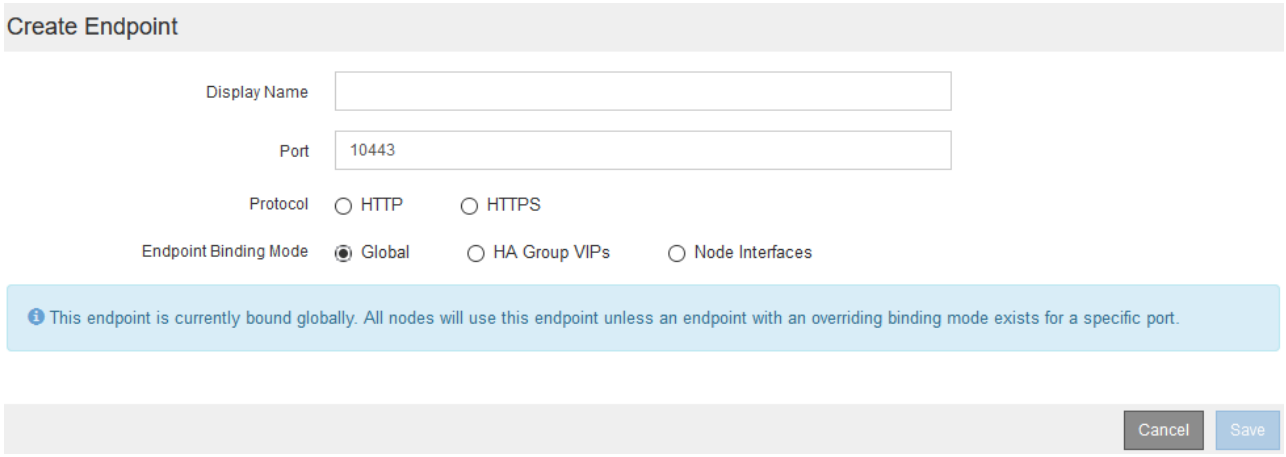
3. Introduzca un nombre para mostrar para el extremo, que aparecerá en la lista de la página Load Balancer Endpoints.
4. Introduzca un número de puerto o deje el número de puerto rellenado previamente como está.

   Si introduce el número de puerto 80 o 443, el extremo se configura únicamente en los nodos de puerta de enlace, ya que estos puertos están reservados en los nodos de administración.

   > Los puertos utilizados por otros servicios de red no están permitidos. Consulte las directrices de red para obtener una lista de los puertos utilizados para las comunicaciones internas y externas.

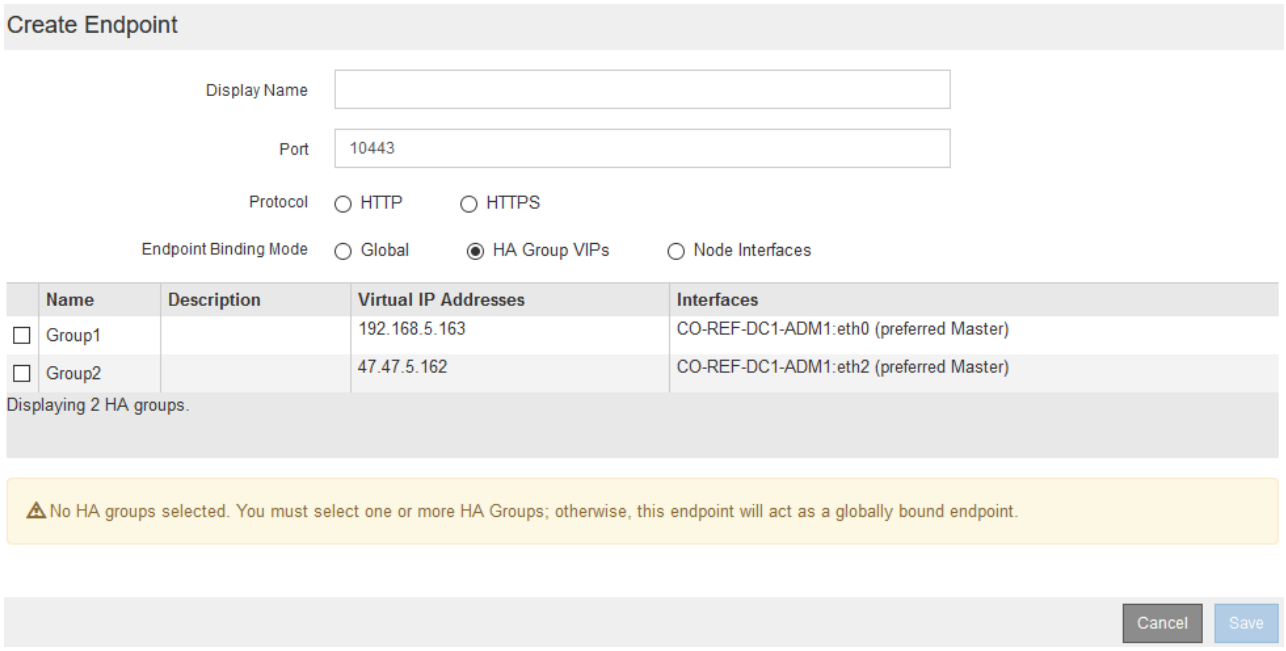
5. Seleccione **HTTP** o **HTTPS** para especificar el protocolo de red para este extremo.
6. Seleccione un modo de enlace de extremo.

   - **Global** (predeterminado): El punto final es accesible en todos los nodos Gateway y Admin en el número de puerto especificado.



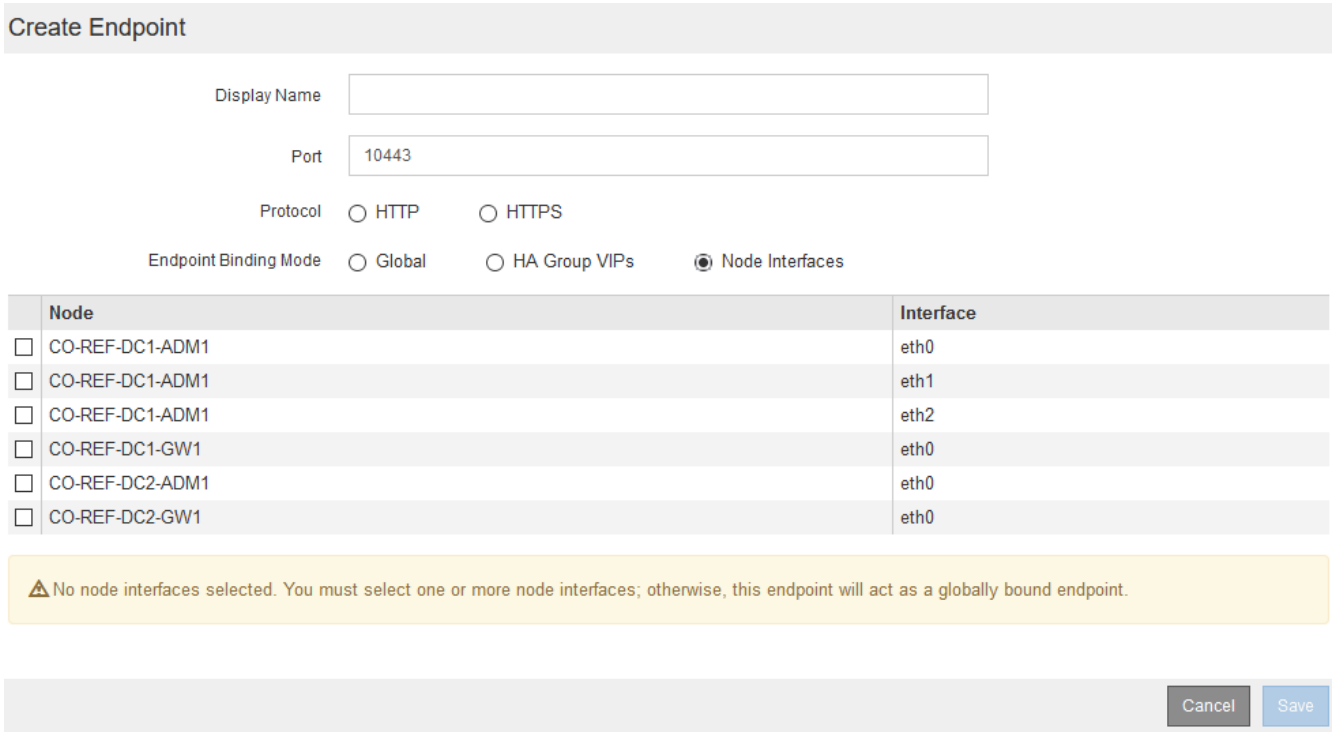
- **VIPS de grupo de alta disponibilidad**: Sólo se puede acceder al terminal a través de las direcciones IP virtuales definidas para los grupos de alta disponibilidad seleccionados. Los extremos definidos en este modo pueden reutilizar el mismo número de puerto, siempre que los grupos de alta disponibilidad definidos por dichos extremos no se superpongan entre sí.

  Seleccione los grupos de alta disponibilidad con las direcciones IP virtuales donde desee que aparezca el extremo.



- **Interfaces de nodo**: Sólo se puede acceder al extremo en los nodos designados y en las interfaces de red. Los extremos definidos en este modo pueden reutilizar el mismo número de puerto siempre que estas interfaces no se superpongan entre sí.

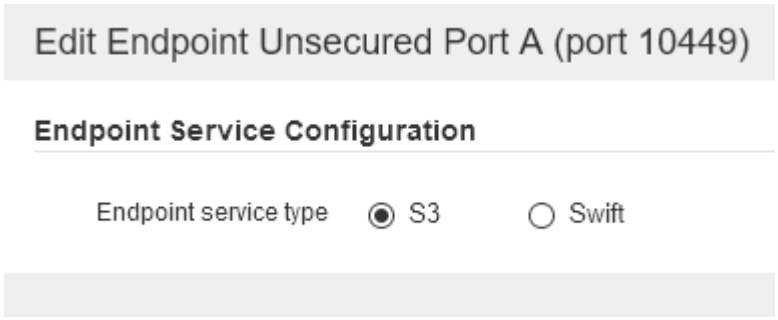
  Seleccione las interfaces de nodo en las que desea que aparezca el extremo.



7. Seleccione **Guardar**.

   Se muestra el cuadro de diálogo Edit Endpoint.

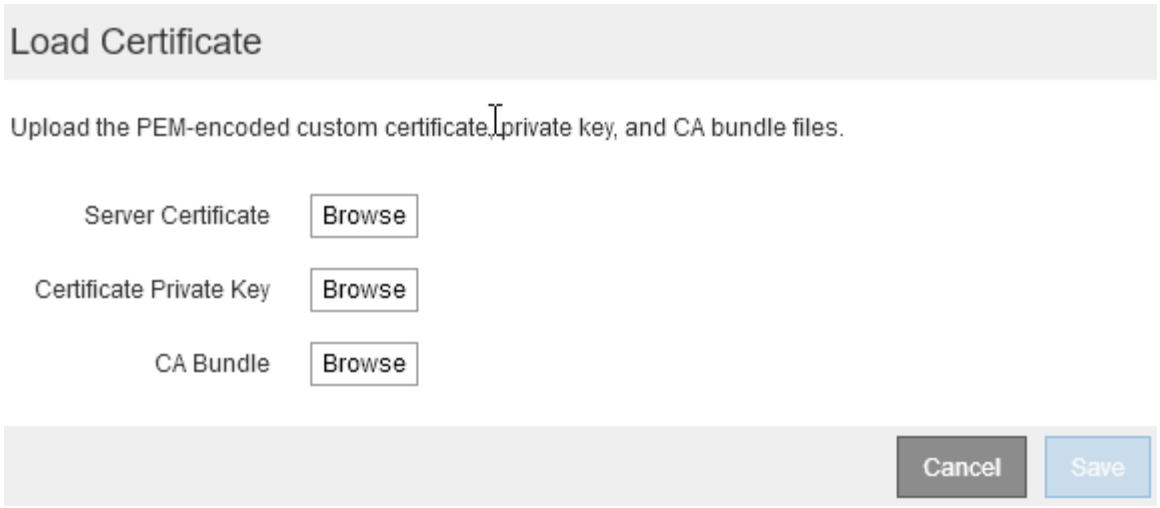
8. Seleccione **S3** o **Swift** para especificar el tipo de tráfico que servirá este extremo.



9. Si ha seleccionado **HTTP**, seleccione **Guardar**.

   Se crea el extremo no seguro. En la tabla de la página Load Balancer Endpoints se muestra el nombre para mostrar, el número de puerto, el protocolo y el ID de extremo del extremo.

10. Si ha seleccionado **HTTPS** y desea cargar un certificado, seleccione **cargar certificado**.



a. Busque el certificado de servidor y la clave privada de certificado.

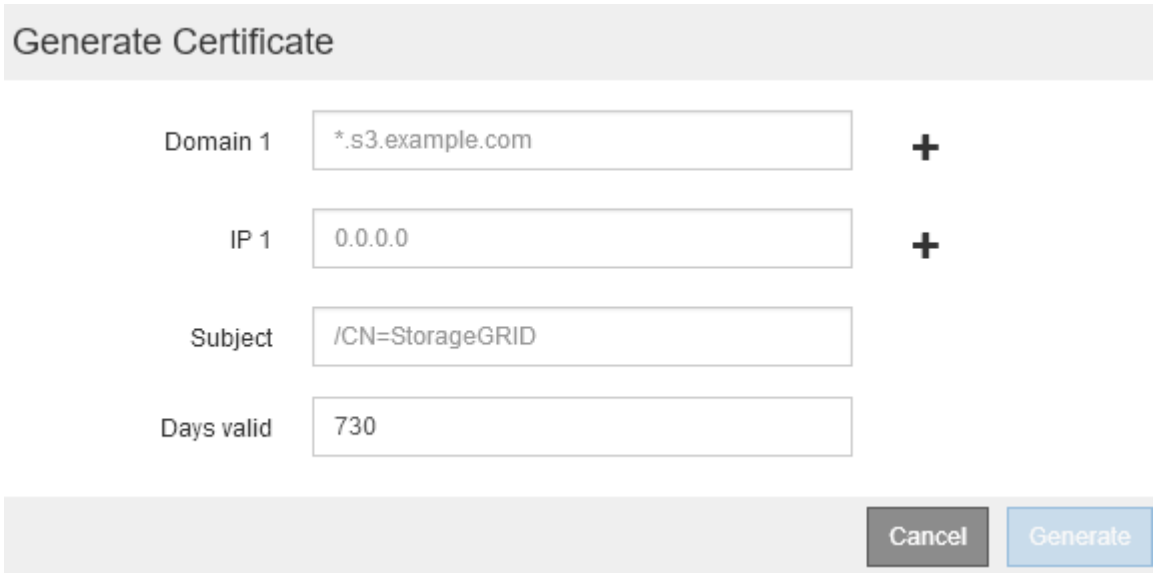
   Para habilitar que los clientes S3 se conecten mediante un nombre de dominio de extremo de API S3, use un certificado comodín o de varios dominios que coincida con todos los nombres de dominio que el cliente podría usar para conectarse al grid. Por ejemplo, el certificado de servidor puede utilizar el nombre de dominio `*.example.com`.

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

a. Opcionalmente, busque un paquete de CA.
b. Seleccione **Guardar**.

   Aparece los datos de certificado codificados con PEM para el extremo.

11. Si ha seleccionado **HTTPS** y desea generar un certificado, seleccione **generar certificado**.



a. Introduzca un nombre de dominio o una dirección IP.

   Puede usar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo: `*.sgws.foo.com` utiliza el comodín * que se va a representar `gn1.sgws.foo.com` y..

`gn2.sgws.foo.com`.

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

a. Seleccione ➕ Para agregar otros nombres de dominio o direcciones IP.

   Si está usando grupos de alta disponibilidad (ha), añada los nombres de dominio y las direcciones IP de las IP virtuales de alta disponibilidad.

b. Opcionalmente, introduzca un sujeto X.509, también denominado Nombre distintivo (DN), para identificar quién posee el certificado.

c. De manera opcional, seleccione el número de días en los que el certificado es válido. El valor predeterminado es 730 días.

d. Seleccione **generar**.

   Se muestran los metadatos del certificado y los datos de certificado codificados con PEM para el extremo.

12. Haga clic en **Guardar**.

    Se crea el extremo. En la tabla de la página Load Balancer Endpoints se muestra el nombre para mostrar, el número de puerto, el protocolo y el ID de extremo del extremo.

Información relacionada

"Mantener recuperar"

"Directrices de red"

"Gestionar grupos de alta disponibilidad"

"Administración de redes de clientes que no son de confianza"

Edición de puntos finales del equilibrador de carga

Para un extremo no seguro (HTTP), puede cambiar el tipo de servicio de extremo entre S3 y Swift. En el caso de un extremo protegido (HTTPS), puede editar el tipo de servicio de extremo y ver o cambiar el certificado de seguridad.

Lo que necesitará

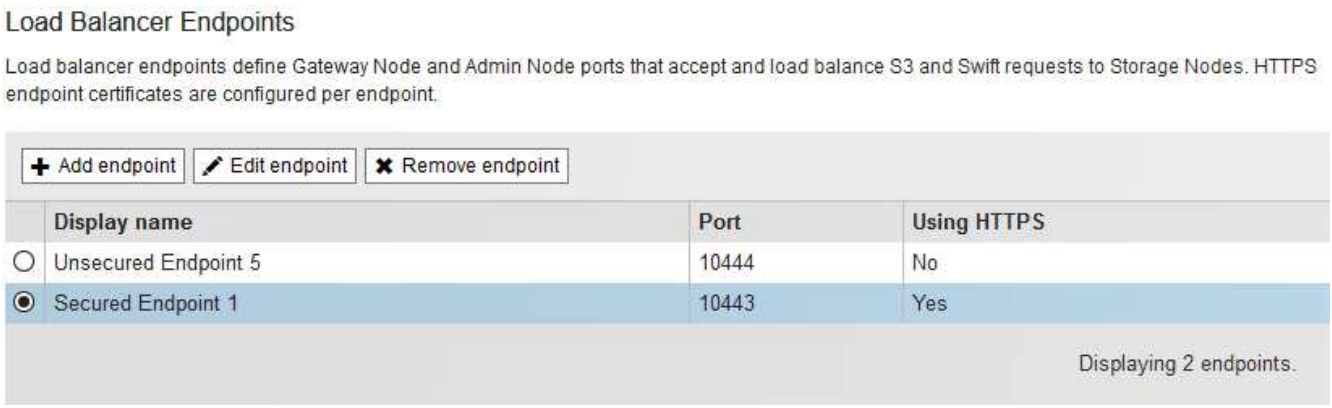
- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**.

   Aparece la página Load Balancer Endpoints. Los extremos existentes se muestran en la tabla.

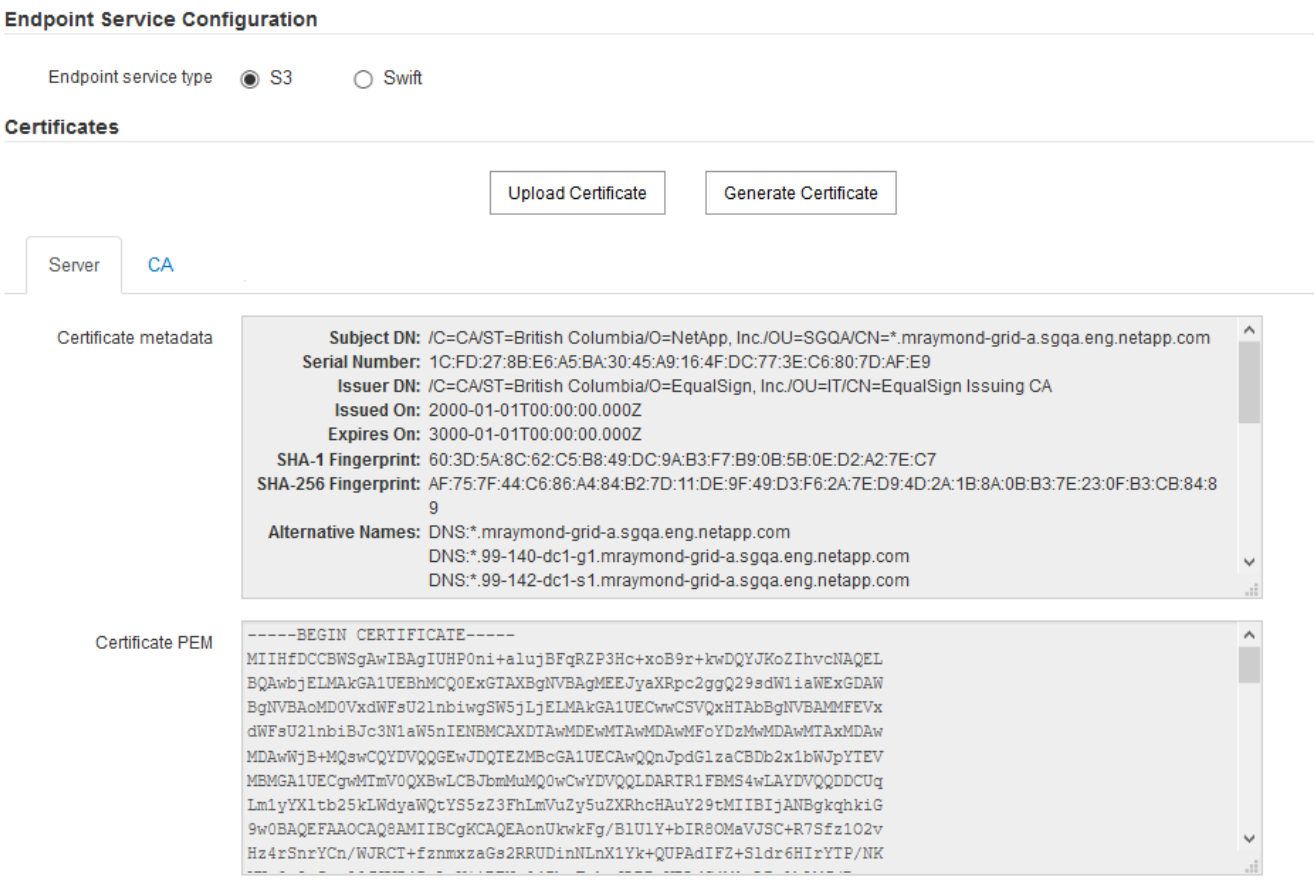
   Los extremos con certificados que caducarán pronto se identifican en la tabla.



2. Seleccione el extremo que desea editar.
3. Haga clic en **Editar punto final**.

   Se muestra el cuadro de diálogo Edit Endpoint.

   En el caso de un extremo no seguro (HTTP), sólo aparece la sección Configuración del servicio de extremo del cuadro de diálogo. En el caso de un extremo protegido (HTTPS), aparecen las secciones Configuración de Endpoint Service y certificados del cuadro de diálogo, como se muestra en el siguiente ejemplo.



4. Realice los cambios deseados en el extremo.

   En el caso de un extremo no seguro (HTTP), puede:

- Cambie el tipo de servicio de extremo entre S3 y Swift.
- Cambie el modo de enlace de punto final. Para un extremo protegido (HTTPS), puede:
- Cambie el tipo de servicio de extremo entre S3 y Swift.
- Cambie el modo de enlace de punto final.
- Vea el certificado de seguridad.
- Cargue o genere un nuevo certificado de seguridad cuando el certificado actual haya caducado o esté a punto de caducar.

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

> Para cambiar el protocolo de un extremo existente, por ejemplo de HTTP a HTTPS, debe crear un extremo nuevo. Siga las instrucciones para crear puntos finales del equilibrador de carga y seleccione el protocolo deseado.

5. Haga clic en **Guardar**.

Información relacionada

Creación de puntos finales del equilibrador de carga

Retirada de los extremos del equilibrador de carga

Si ya no necesita un extremo de equilibrador de carga, puede eliminarlo.

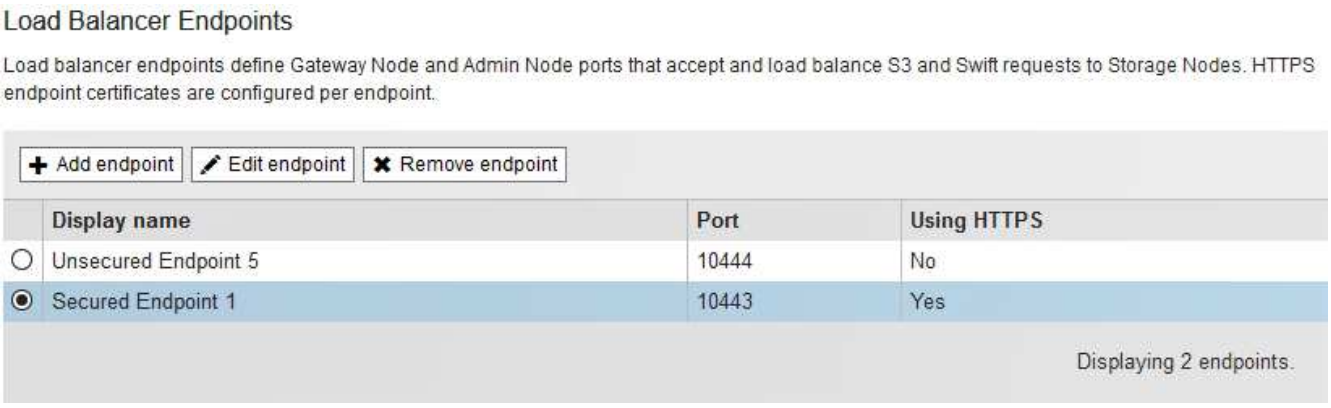
Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**.

   Aparece la página Load Balancer Endpoints. Los extremos existentes se muestran en la tabla.



2. Seleccione el botón de opción situado a la izquierda del extremo que desea eliminar.
3. Haga clic en **Quitar punto final**.

   Se muestra un cuadro de diálogo de confirmación.

4. Haga clic en **Aceptar**.

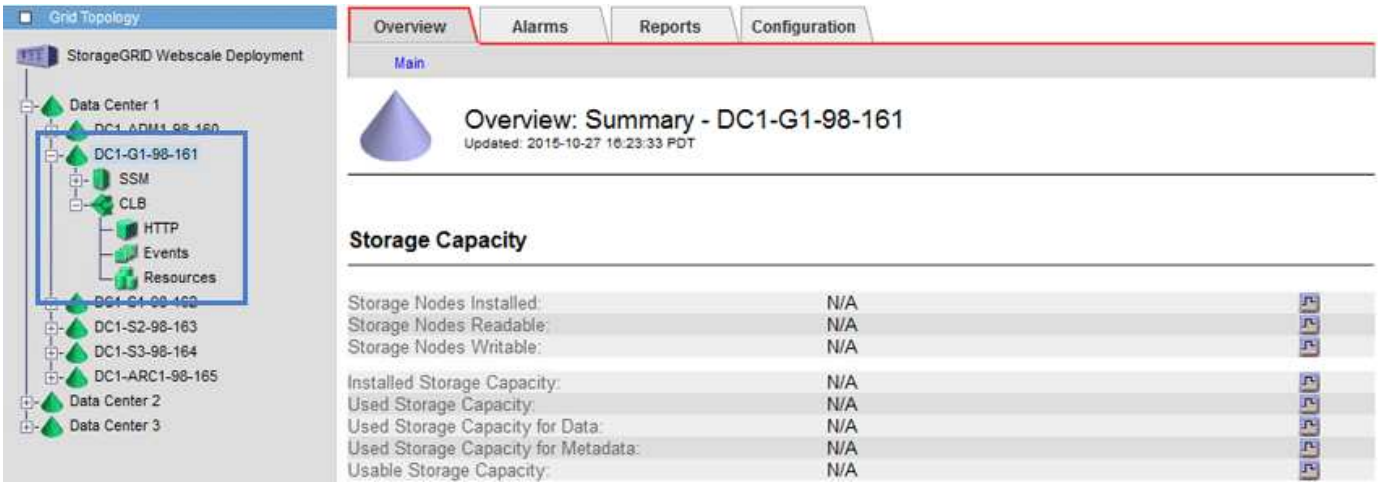
   El punto final se elimina.

Cómo funciona el equilibrio de carga: Servicio CLB

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 acerca del servicio CLB, seleccione **Soporte** > **Herramientas** > **Topología de cuadrícula** y, a continuación, expanda un nodo de puerta de enlace hasta que pueda seleccionar **CLB** y las opciones que aparecen debajo de él.



Si decide utilizar el servicio CLB, debe considerar la configuración de los costes de enlace para su sistema StorageGRID.

Información relacionada

"¿Cuáles son los costes de enlace"

"Actualizando costes de enlace"

Administración de redes de clientes que no son de confianza

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 las directrices de red).

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.

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.

Información relacionada

"Directrices de red"

"Configuración de los extremos del equilibrador de carga"

La especificación de la red de cliente de un 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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.

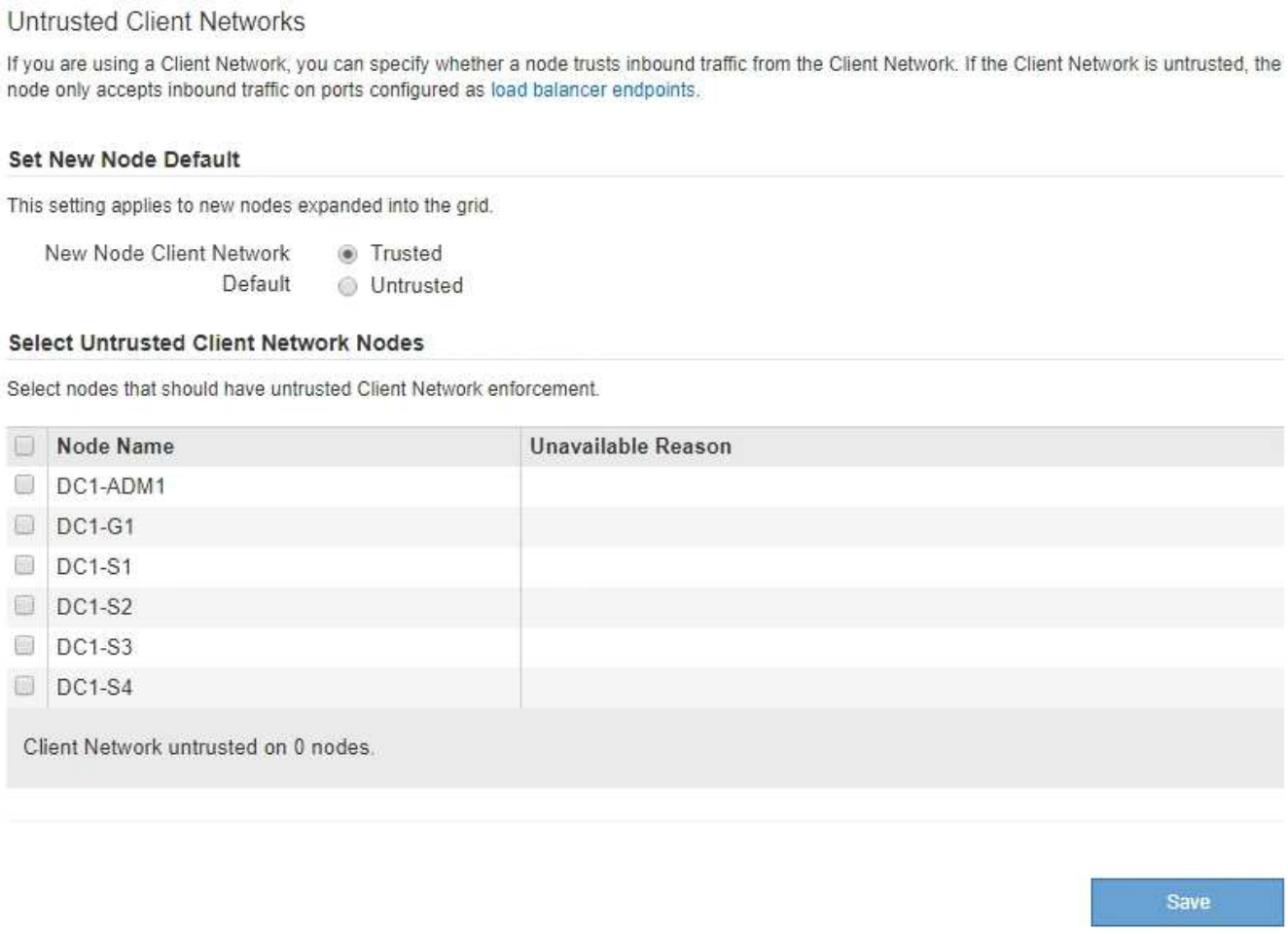
> Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **Red de cliente no confiable**.

   Aparece la página redes de cliente no fiables.

   Esta página muestra 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. Haga clic en **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.

Información relacionada

"Configuración de los extremos del equilibrador de carga"

Gestionar grupos de alta disponibilidad

Los grupos de alta disponibilidad pueden usarse para proporcionar conexiones de datos altamente disponibles para clientes S3 y Swift. Los grupos DE ALTA DISPONIBILIDAD también se pueden utilizar para proporcionar conexiones de alta disponibilidad al administrador de grid y al administrador de inquilinos.

- "Qué es un grupo de alta disponibilidad"
- "Cómo se utilizan los grupos de alta disponibilidad"
- "Opciones de configuración para grupos de alta disponibilidad"
- "Crear un grupo de alta disponibilidad"
- "Edición de un grupo de alta disponibilidad"
- "Eliminar un grupo de alta disponibilidad"

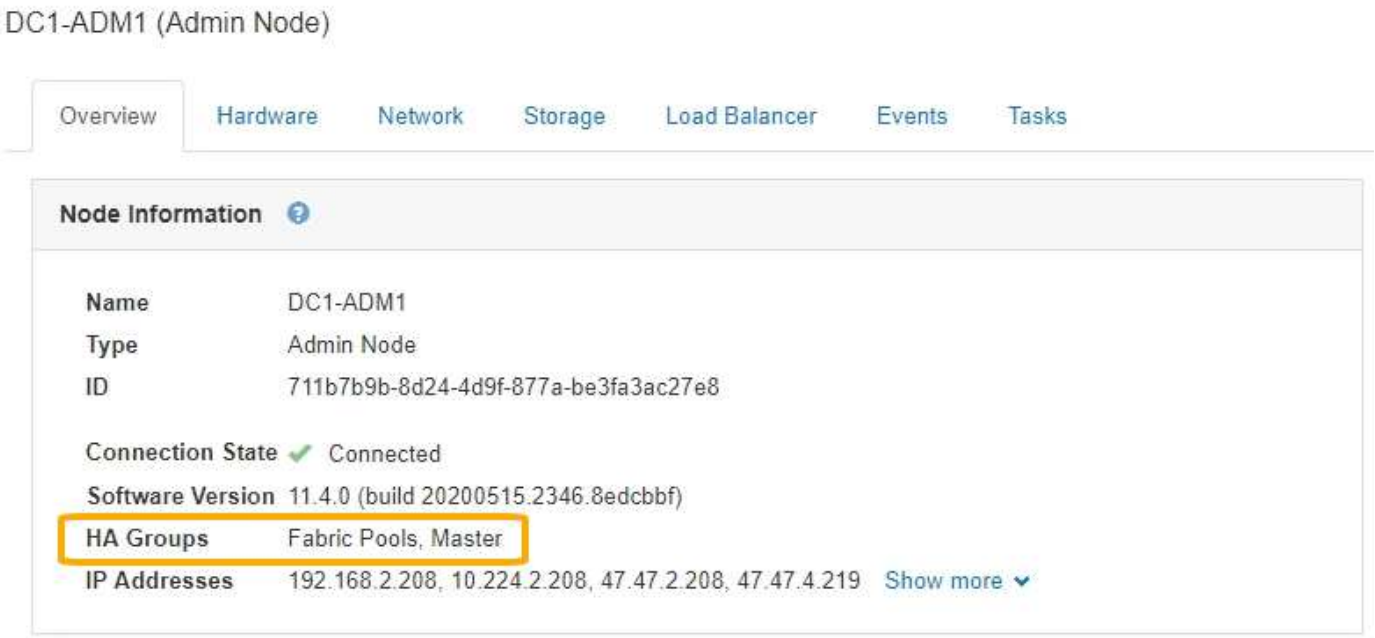
Qué es un grupo de alta disponibilidad

Los grupos de alta disponibilidad usan direcciones IP virtuales (VIP) para proporcionar acceso de backup activo a los servicios Gateway Node o Admin Node.

Un grupo de alta disponibilidad consta de una o varias interfaces de red en los nodos de administración y de pasarela. Al crear un grupo ha, se seleccionan las interfaces de red que pertenecen a la red de cuadrícula (eth0) o a la red de cliente (eth2). Todas las interfaces de un grupo de alta disponibilidad deben estar en la misma subred de red.

Un grupo de alta disponibilidad mantiene una o varias direcciones IP virtuales que se han añadido a la interfaz activa en el grupo. Si la interfaz activa deja de estar disponible, las direcciones IP virtuales se mueven a otra interfaz. Por lo general, este proceso de conmutación por error solo 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.

La interfaz activa de un grupo de alta disponibilidad se designa como maestro. El resto de las interfaces se designan como copia de seguridad. Para ver estas designaciones, seleccione **Nodes** > ***node*** > **Descripción general**.



Al crear un grupo de alta disponibilidad, se especifica una interfaz para que sea el maestro preferido. El principal preferido es la interfaz activa a menos que se produzca un fallo que haga que las direcciones VIP se reasignan a una interfaz de copia de seguridad. Cuando se resuelve el fallo, las direcciones VIP se vuelven automáticamente al maestro preferido.

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.

Si el grupo de alta disponibilidad incluye interfaces de más de dos nodos, la interfaz activa podría moverse a la interfaz de cualquier otro nodo durante la conmutación por error.

Cómo se utilizan los grupos de alta disponibilidad

Puede que quiera utilizar grupos de alta disponibilidad por varios motivos.

- 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 (**Master** preferido) • Nodos de administrador no primario **Nota:** el nodo de administración principal debe ser el Master preferido. 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 • Nodos de puerta de enlace
Acceso al cliente S3 o Swift: Servicio CLB **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

El fallo de los servicios del administrador de grid o del administrador de inquilinos no activa la conmutación por error dentro 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.

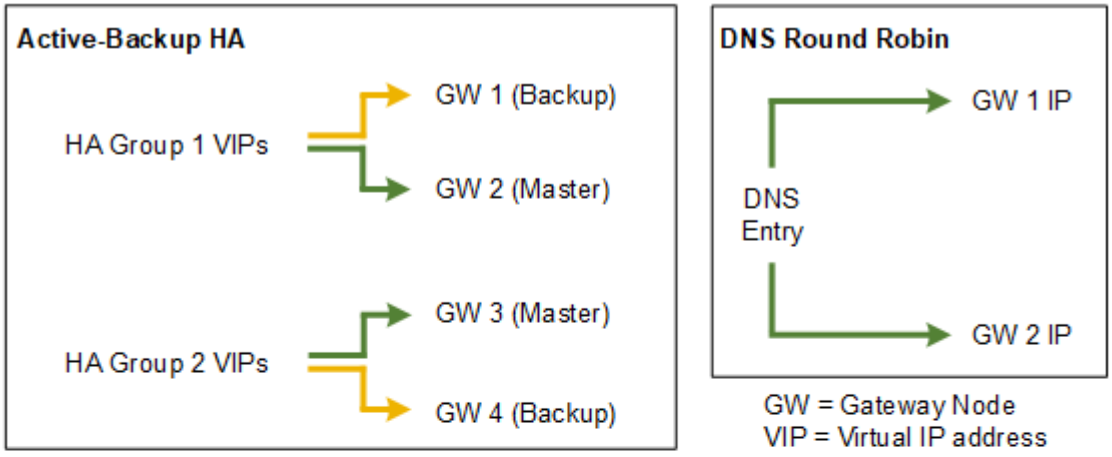
Limitaciones del uso de grupos de alta disponibilidad con el servicio CLB

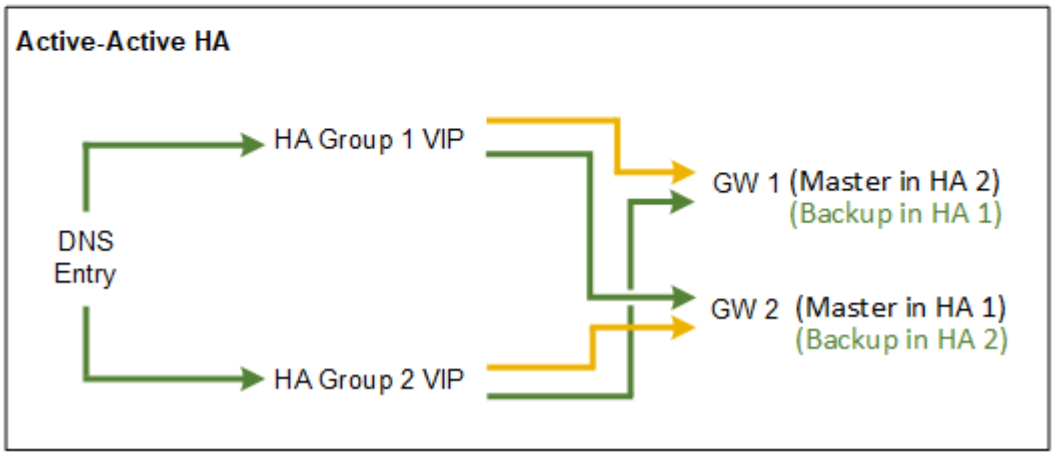
El error del servicio CLB no activa la conmutación por error dentro del grupo ha.

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.





Al crear varios grupos de alta disponibilidad solapados como se muestra en el ejemplo de alta disponibilidad activo-activo, el rendimiento total se escala con el número de nodos y grupos de alta disponibilidad. Con tres o más nodos y tres o más grupos de alta disponibilidad, también tiene la capacidad de continuar con las operaciones utilizando cualquiera de los VIP incluso durante los procedimientos de mantenimiento, lo que requiere que desconecte un nodo.

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. • 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.

Configuración	Ventajas	Desventajas
Operación por turnos DNS	• Mayor rendimiento total. • Sin hosts inactivos.	• Conmutación al respaldo lenta, que puede depender del comportamiento del cliente. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.
Activa-activa	• El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento de agregado escalable con el número de grupos de alta disponibilidad. • Rápida recuperación tras fallos.	• Más complejo de configurar. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.

Crear un grupo de alta disponibilidad

Puede crear uno o varios grupos de alta disponibilidad para proporcionar acceso de alta disponibilidad a los servicios en nodos de administración o nodos de puerta de enlace.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

Una interfaz debe cumplir las siguientes condiciones para incluirse en un grupo de alta disponibilidad:

- La interfaz debe ser para un nodo de puerta de enlace o un nodo de administrador.
- La interfaz debe pertenecer a la red de cuadrícula (eth0) o a la red de cliente (eth2).
- La interfaz debe configurarse con dirección IP fija o estática, no con DHCP.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **grupos de alta disponibilidad**.

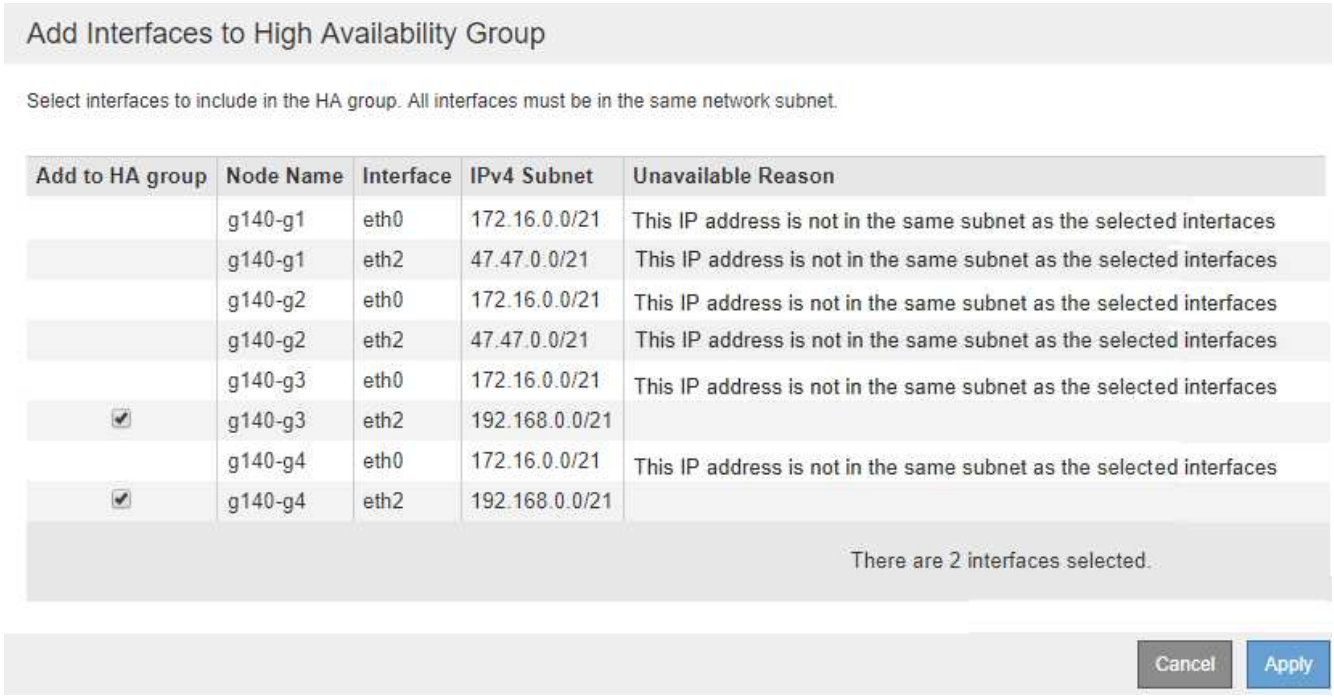
   Aparece la página grupos de alta disponibilidad.

2. Haga clic en **Crear**.

   Se muestra el cuadro de diálogo Crear grupo de alta disponibilidad.

3. Escriba un nombre y, si lo desea, una descripción del grupo de alta disponibilidad.
4. Haga clic en **Seleccionar interfaces**.

   Se muestra el cuadro de diálogo Add interfaces to High Availability Group. En la tabla se enumeran los nodos elegibles, las interfaces y las subredes IPv4.



   Una interfaz no aparece en la lista si DHCP asigna su dirección IP.

5. En la columna **Agregar al grupo ha** , active la casilla de verificación de la interfaz que desee agregar al grupo ha.

   Tenga en cuenta las siguientes directrices para seleccionar interfaces:

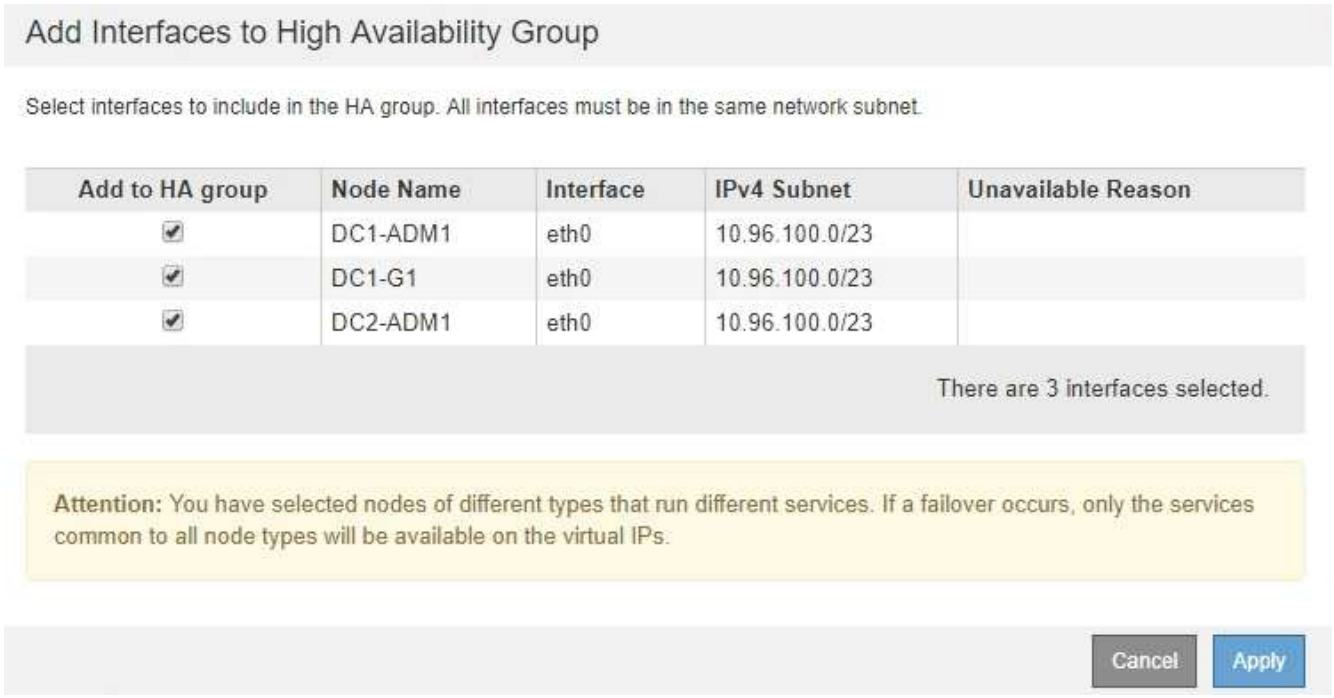
   - Debe seleccionar al menos una interfaz.
   - Si selecciona más de una interfaz, todas las interfaces deben estar en la red de cuadrícula (eth0) o en la red de cliente (eth2).
   - Todas las interfaces deben estar en la misma subred o en subredes con un prefijo común.

     Las direcciones IP se restringirán a la subred más pequeña (la que tenga el prefijo más grande).

   - Si selecciona interfaces en diferentes tipos de nodos y se produce una conmutación al nodo de respaldo, solo estarán disponibles en las IP virtuales los servicios comunes a los nodos seleccionados.
     - Seleccione dos o más nodos de administrador para la protección de alta disponibilidad de Grid Manager o del inquilino Manager.
     - Seleccione dos o más nodos de administrador, nodos de puerta de enlace o ambos para la protección de alta disponibilidad del servicio Load Balancer.
     - Seleccione dos o más nodos de puerta de enlace para la protección de alta disponibilidad del

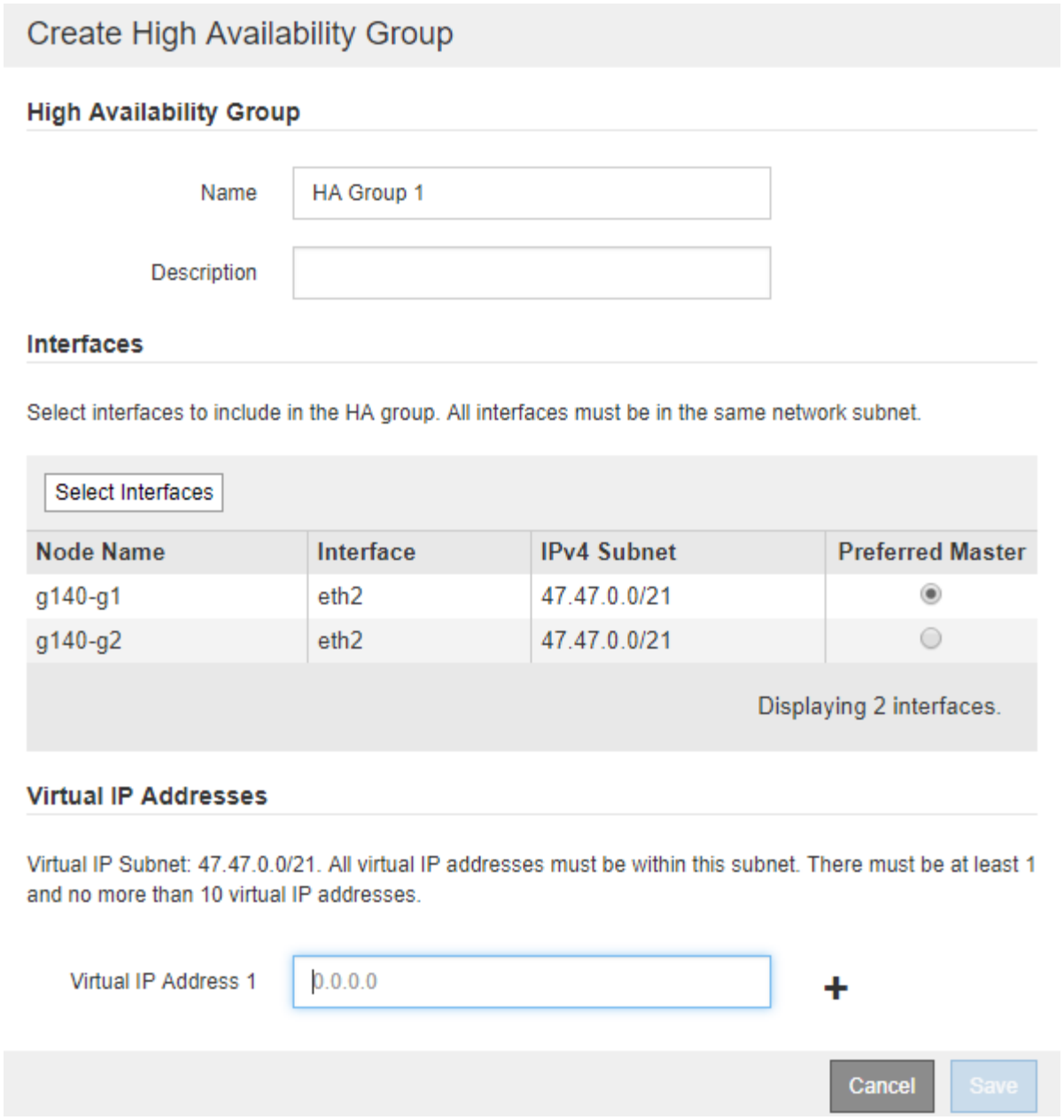
servicio CLB.

El servicio CLB está obsoleto.



6. Haga clic en **aplicar**.

   Las interfaces seleccionadas se muestran en la sección interfaces de la página Create High Availability Group. De forma predeterminada, la primera interfaz de la lista se selecciona como patrón preferido.



7. Si desea que una interfaz diferente sea el Master preferido, seleccione esa interfaz en la columna **Master** preferido.

   El principal preferido es la interfaz activa a menos que se produzca un fallo que haga que las direcciones VIP se reasignan a una interfaz de copia de seguridad.

   > Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea el maestro preferido. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

8. En la sección direcciones IP virtuales de la página, introduzca de una a 10 direcciones IP virtuales para el grupo de alta disponibilidad. Haga clic en el signo más (+) Para agregar varias direcciones IP.

   Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

   Las direcciones IPv4 deben estar en la subred IPv4 compartida por todas las interfaces miembros.

9. Haga clic en **Guardar**.

   El grupo ha se ha creado y ahora puede utilizar las direcciones IP virtuales configuradas.

Información relacionada

"Instale Red Hat Enterprise Linux o CentOS"

"Instale VMware"

"Instalar Ubuntu o Debian"

"Gestión del equilibrio de carga"

Edición de un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, o agregar o actualizar una dirección IP virtual.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

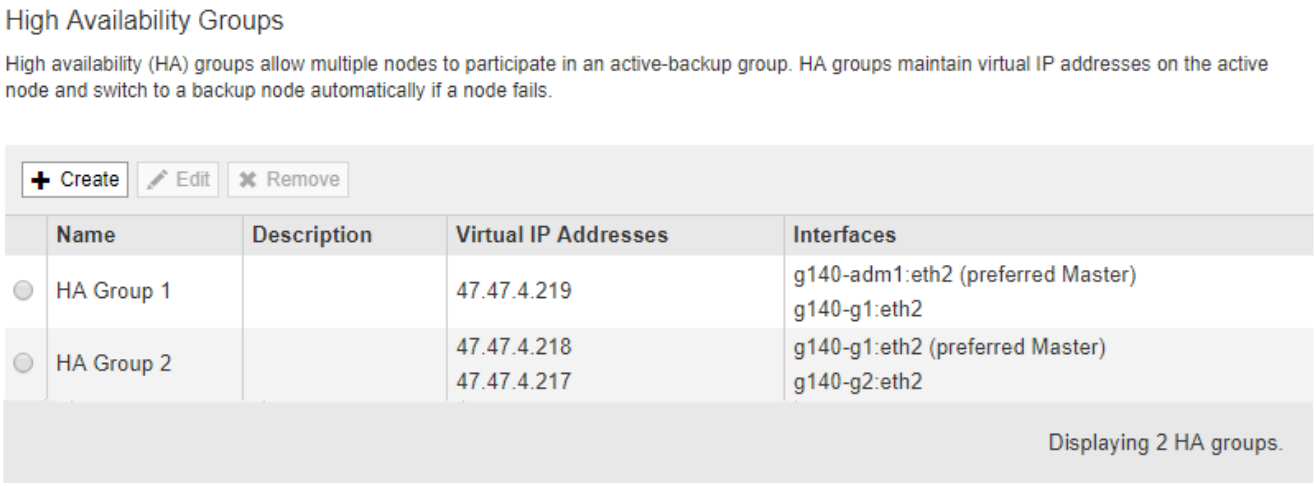
Entre algunos de los motivos para editar un grupo de alta disponibilidad se encuentran los siguientes:

- Agregar una interfaz a un grupo existente. La dirección IP de la interfaz debe estar dentro de la misma subred que otras interfaces ya asignadas al grupo.
- Quitar una interfaz de un grupo de alta disponibilidad. Por ejemplo, no puede iniciar un procedimiento de retirada de sitio o nodo si se utiliza la interfaz de un nodo para la red de cuadrícula o la red de cliente en un grupo ha.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **grupos de alta disponibilidad**.

   Aparece la página grupos de alta disponibilidad.

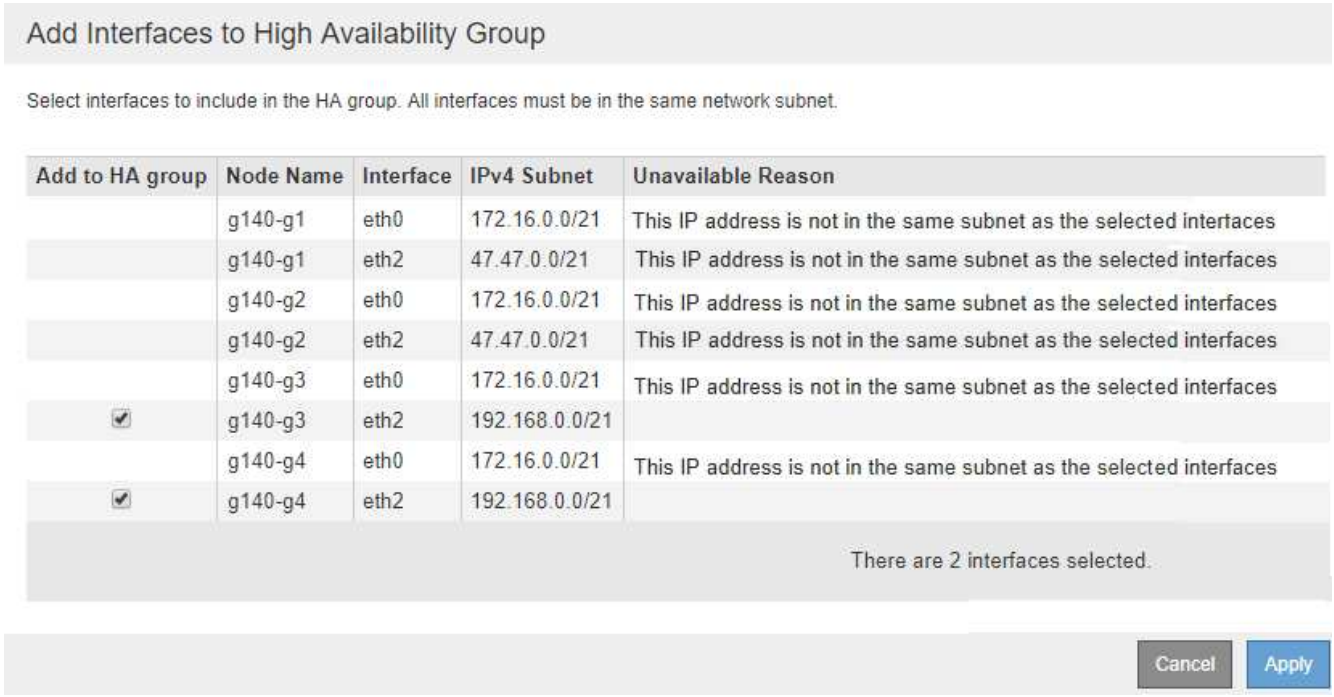


2. Seleccione el grupo ha que desea editar y haga clic en **Editar**.

Se muestra el cuadro de diálogo Editar grupo de alta disponibilidad.

3. Si lo desea, actualice el nombre o la descripción del grupo.
4. Opcionalmente, haga clic en **Seleccionar interfaces** para cambiar las interfaces del grupo ha.

   Se muestra el cuadro de diálogo Add interfaces to High Availability Group.



   Una interfaz no aparece en la lista si DHCP asigna su dirección IP.

5. Active o anule la selección de las casillas de verificación para agregar o quitar interfaces.

   Tenga en cuenta las siguientes directrices para seleccionar interfaces:

   - Debe seleccionar al menos una interfaz.
   - Si selecciona más de una interfaz, todas las interfaces deben estar en la red de cuadrícula (eth0) o en la red de cliente (eth2).
   - Todas las interfaces deben estar en la misma subred o en subredes con un prefijo común.

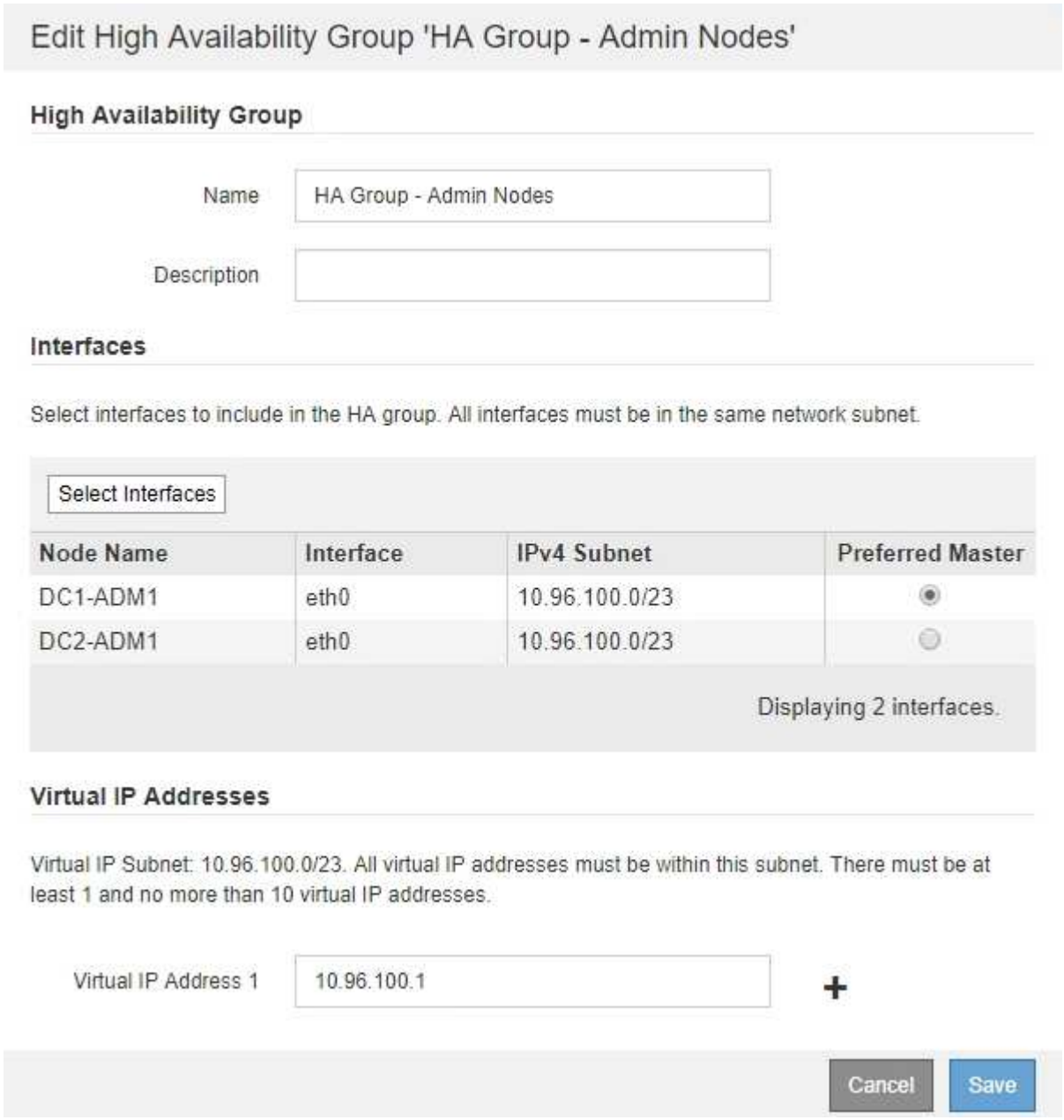
     Las direcciones IP se restringirán a la subred más pequeña (la que tenga el prefijo más grande).

   - Si selecciona interfaces en diferentes tipos de nodos y se produce una conmutación al nodo de respaldo, solo estarán disponibles en las IP virtuales los servicios comunes a los nodos seleccionados.
     - Seleccione dos o más nodos de administrador para la protección de alta disponibilidad de Grid Manager o del inquilino Manager.
     - Seleccione dos o más nodos de administrador, nodos de puerta de enlace o ambos para la protección de alta disponibilidad del servicio Load Balancer.
     - Seleccione dos o más nodos de puerta de enlace para la protección de alta disponibilidad del servicio CLB.

       El servicio CLB está obsoleto.

6. Haga clic en **aplicar**.

   Las interfaces seleccionadas se muestran en la sección interfaces de la página. De forma predeterminada, la primera interfaz de la lista se selecciona como patrón preferido.



7. Si desea que una interfaz diferente sea el Master preferido, seleccione esa interfaz en la columna **Master** preferido.

   El principal preferido es la interfaz activa a menos que se produzca un fallo que haga que las direcciones VIP se reasignan a una interfaz de copia de seguridad.

   > Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea el maestro preferido. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

8. De manera opcional, actualice las direcciones IP virtuales del grupo de alta disponibilidad.

Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

Las direcciones IPv4 deben estar en la subred IPv4 compartida por todas las interfaces miembros.

9. Haga clic en **Guardar**.

   El grupo de alta disponibilidad se ha actualizado.

Eliminar un grupo de alta disponibilidad

Puede eliminar un grupo de alta disponibilidad que ya no utilice.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

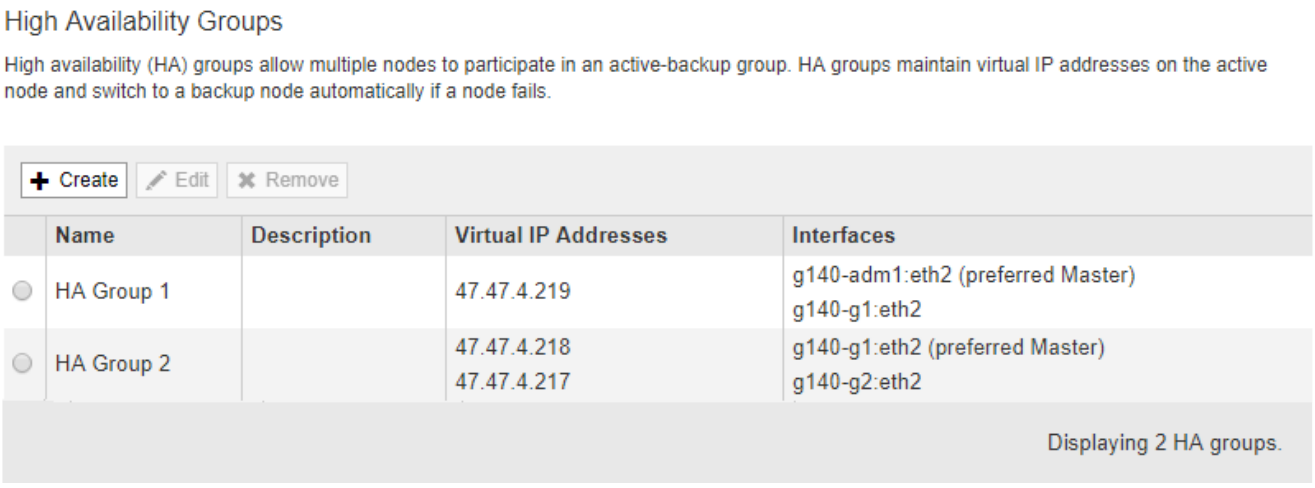
Aboque por esta tarea

Si quita un grupo de alta disponibilidad, todos los clientes S3 o Swift que se hayan configurado para usar una de las direcciones IP virtuales del grupo ya no podrán conectarse a StorageGRID. Para evitar que se produzcan interrupciones en el cliente, debe actualizar todas 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 o mediante DHCP.

Pasos

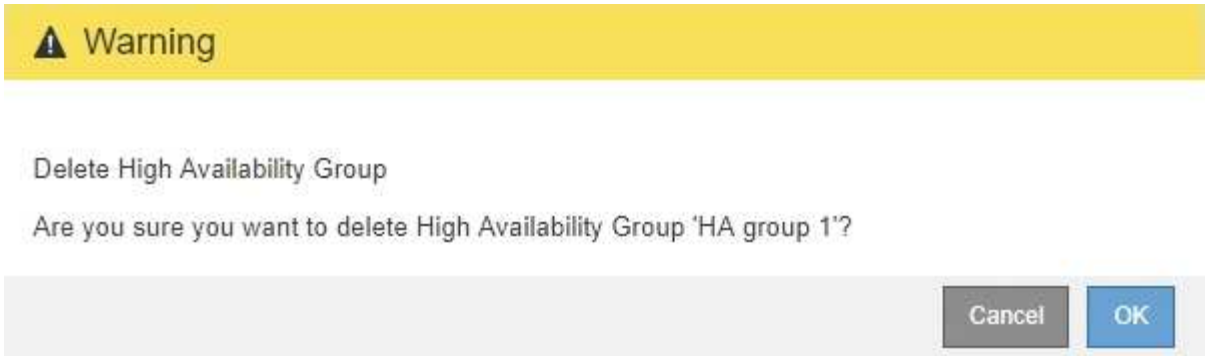
1. Seleccione **Configuración** > **Configuración de red** > **grupos de alta disponibilidad**.

   Aparece la página grupos de alta disponibilidad.



2. Seleccione el grupo ha que desea quitar y haga clic en **Quitar**.

   Aparece la advertencia Eliminar grupo de alta disponibilidad.



3. Haga clic en **Aceptar**.

   El grupo de alta disponibilidad se ha eliminado.

Configurar nombres de dominio de extremo de 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe haber 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 que los clientes usen nombres de dominio extremo de S3, debe realizar todas las tareas siguientes:

- 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.

El certificado que un cliente utiliza para las conexiones HTTPS depende de cómo se conecta el cliente al grid:

- Si un cliente se conecta mediante el servicio Load Balancer, utiliza el certificado para un extremo de equilibrio de carga específico.

  Cada extremo de equilibrador de carga tiene su propio certificado y cada extremo se puede configurar para reconocer diferentes nombres de dominio de extremo.

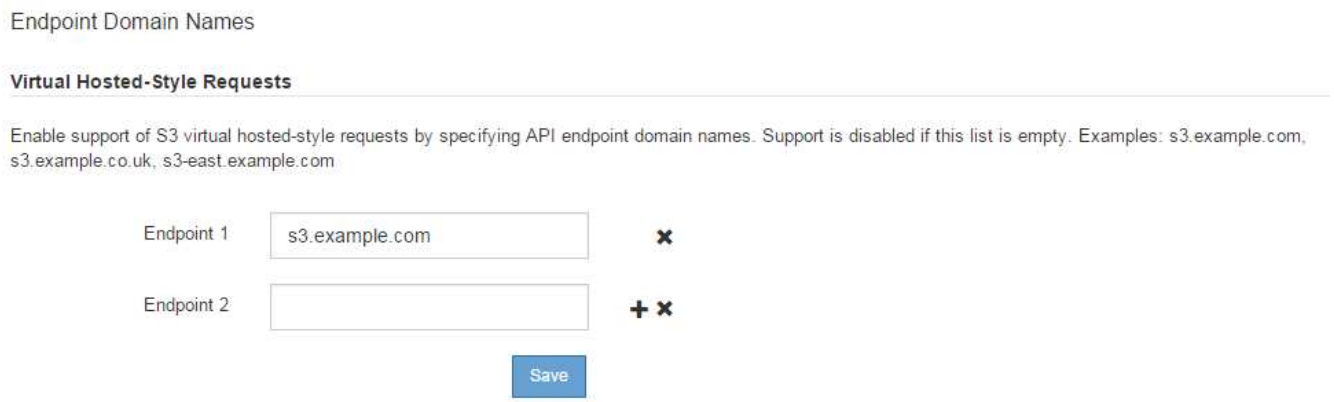
- Si el cliente se conecta a un nodo de almacenamiento o al servicio CLB en un nodo de puerta de enlace, el cliente utiliza un certificado de servidor personalizado de cuadrícula que se ha actualizado para incluir todos los nombres de dominio de extremo requeridos.

  El servicio CLB está obsoleto.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **nombres de dominio**.

   Aparece la página Endpoint Domain Names.



2. Con el icono (+) para añadir campos adicionales, introduzca la lista de nombres de dominio de extremo API de S3 en los campos **Endpoint**.

   Si esta lista está vacía, se deshabilita la compatibilidad con las solicitudes de estilo alojado virtuales de S3.

3. Haga clic en **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de extremo requeridos.
   - Para los clientes que utilizan el servicio Load Balancer, actualice el certificado asociado con el extremo de equilibrio de carga al que se conecta el cliente.
   - Para los clientes que se conectan directamente a nodos de almacenamiento o que usan el servicio CLB en nodos de puerta de enlace, actualice el certificado de servidor personalizado para la cuadrícula.

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"

"Visualización de direcciones IP"

"Crear un grupo de alta disponibilidad"

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

"Configuración de los extremos del equilibrador de carga"

Habilitar 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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** > **Configuración del sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red , active la casilla de verificación **Activar conexión HTTP** .

3. Haga clic en **Guardar**.

Información relacionada

"Configuración de los extremos 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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:

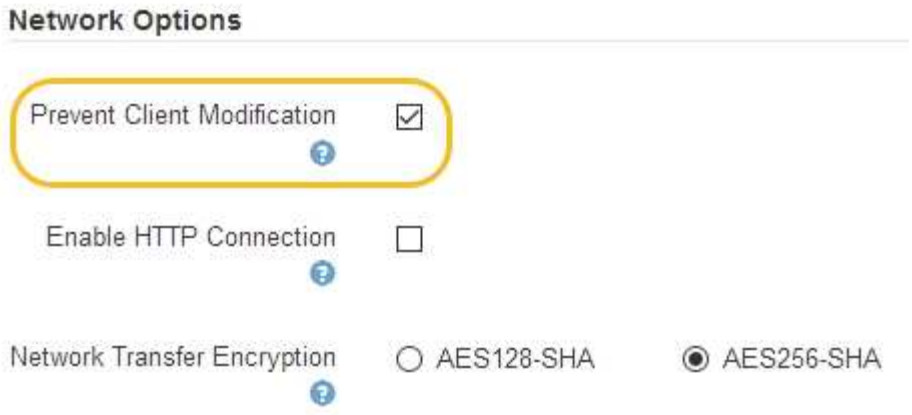
- **API REST S3**
  - Eliminar solicitudes de bloques
  - Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

> 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** > **Configuración del sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red, active la casilla de verificación **evitar modificación de cliente**.



3. Haga clic en **Guardar**.

Gestionar redes y conexiones StorageGRID

Puede utilizar Grid Manager para configurar y administrar redes y conexiones StorageGRID.

Consulte "Configurar las conexiones de clientes S3 y Swift" Para aprender a conectar clientes S3 o Swift.

- "Directrices para redes StorageGRID"
- "Visualización de direcciones IP"
- "Cifrados compatibles para conexiones TLS salientes"
- "Cambiando el cifrado de transferencia de red"
- "Configuración de certificados de servidor"
- "Configurando la configuración del proxy de almacenamiento"
- "Configurando los ajustes del proxy de administrador"
- "Gestión de directivas de clasificación de tráfico"
- "¿Cuáles son los costes de enlace"

Directrices para redes StorageGRID

StorageGRID admite hasta tres interfaces de red por nodo de grid, lo que permite configurar la red para cada nodo de grid individual de modo que se ajuste a sus requisitos de seguridad y acceso.

> Para modificar o añadir una red para un nodo de grid, consulte las instrucciones de recuperación y mantenimiento. Para obtener más información acerca de la topología de red, consulte las instrucciones de 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.

Información relacionada

"Mantener recuperar"

"Directrices de red"

Visualización de 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

Debe iniciar sesión en Grid Manager mediante un explorador compatible.

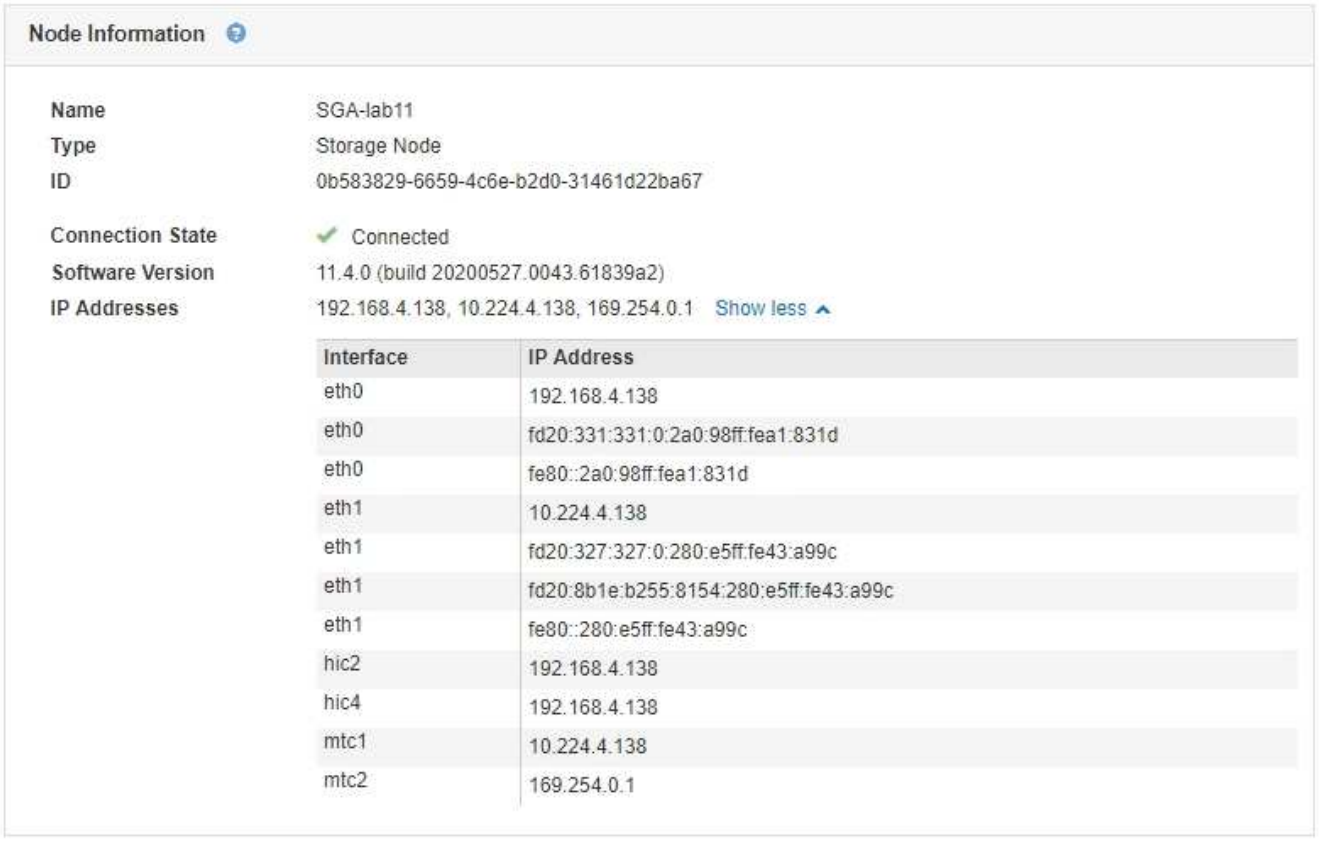
Acerca de esta tarea

Para obtener información acerca de cómo cambiar direcciones IP, consulte las instrucciones de recuperación y mantenimiento.

Pasos

1. Seleccione **Nodes** > ***grid node*** > **Descripción general**.
2. Haga clic en **Mostrar más** a la derecha del título direcciones IP.

   Las direcciones IP de ese nodo de grid se enumeran en una tabla.



Información relacionada

"Mantener recuperar"

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

Cambiando 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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** > **Configuración del 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. Haga clic en **Guardar**.

Configuración de certificados de servidor

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

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

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

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

Tipos admitidos de certificado de servidor personalizado

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

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

Certificados para extremos de equilibrador de carga

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

Información relacionada

"Use S3"

"Use Swift"

"Configuración de los extremos del equilibrador de carga"

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

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

Acerca de esta tarea

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

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

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

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

> Si accede a Grid Manager o a Intenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el explorador mostrará un error de certificado sin una opción para omitir si se produce alguna de las siguientes situaciones:
>
> - El certificado del servidor de la interfaz de gestión personalizada caduca.
> - Se revierte de un certificado del servidor de interfaz de gestión personalizado al certificado de servidor predeterminado.

Pasos

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

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

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

4. Haga clic en **Guardar**.

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

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

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

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

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

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

Pasos

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

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

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

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

Es posible reemplazar el certificado de servidor que se utiliza para las conexiones de clientes S3 o Swift al nodo de almacenamiento o al servicio CLB (obsoleto) en Gateway Node. El certificado de servidor personalizado de reemplazo es específico de su organización.

Acerca de esta tarea

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

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

Después de completar la configuración en el servidor, es posible que los usuarios también deban instalar el certificado de CA raíz en el cliente API S3 o Swift que utilizarán para acceder al sistema, según la entidad de certificación (CA) raíz que use.

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

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

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

Pasos

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

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

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

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

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

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

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

Información relacionada

"Use S3"

"Use Swift"

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

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

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

Pasos

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

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

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

Copia del certificado de CA del sistema StorageGRID

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

Lo que necesitará

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

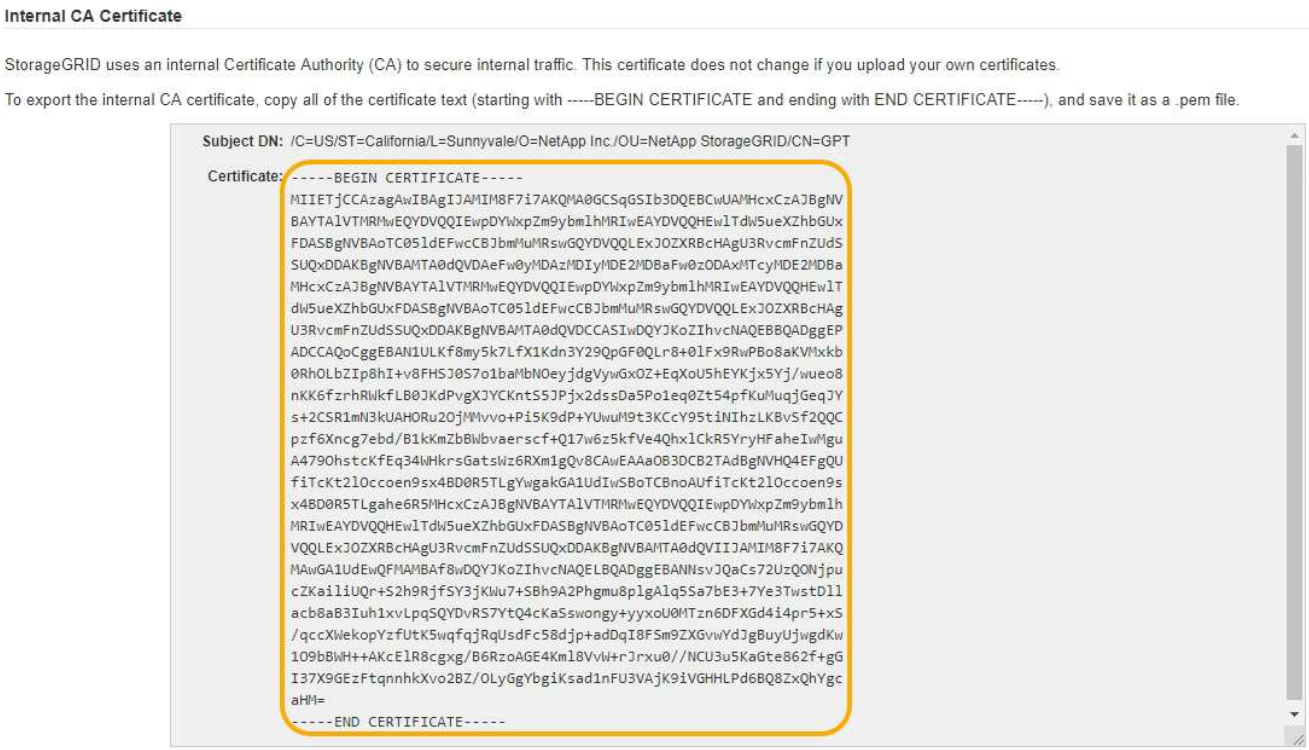
Acerca de esta tarea

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

Pasos

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

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



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

   Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

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

Lo que necesitará

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

Acerca de esta tarea

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

En los siguientes pasos, se ofrecen directrices generales para clientes S3 que usan FabricPool. Para obtener información y procedimientos más detallados, consulte las instrucciones de configuración de StorageGRID para FabricPool.

El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y ya no se recomienda su uso con FabricPool.

Pasos

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

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

3. Adjuntar StorageGRID como nivel de cloud en ONTAP.

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

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

Información relacionada

"Configure StorageGRID para FabricPool"

Generar un certificado de servidor autofirmado para la interfaz de gestión

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

Lo que necesitará

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

Acerca de esta tarea

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

Pasos

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

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

3. Configure StorageGRID con un certificado autofirmado nuevo.

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

- Para `--domains`, Utilice comodines para representar los nombres de dominio completos de todos los nodos Admin. Por ejemplo: `*.ui.storagegrid.example.com` utiliza el comodín * que se va a representar `admin1.ui.storagegrid.example.com` y.. `admin2.ui.storagegrid.example.com`.
- Configurado `--type` para `management` Para configurar el certificado utilizado por el Administrador de grid y el Administrador de inquilinos.
- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede utilizar el `--days` argumento para anular el período de validez predeterminado.

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

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

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

4. Seleccione y copie el certificado.

   Incluya las etiquetas INICIAL Y FINAL en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`
6. Confirme que se configuró el certificado:
   a. Acceda a Grid Manager.
   b. Seleccione **Configuración** > **certificados de servidor** > **Certificado de servidor de interfaz de administración**.
7. Configure el cliente de API de gestión para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Configurando la configuración del 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

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

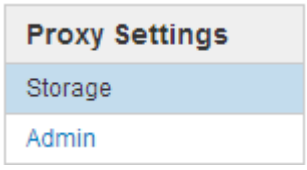
Acerca de esta tarea

Puede configurar los ajustes de un único proxy de almacenamiento.

Pasos

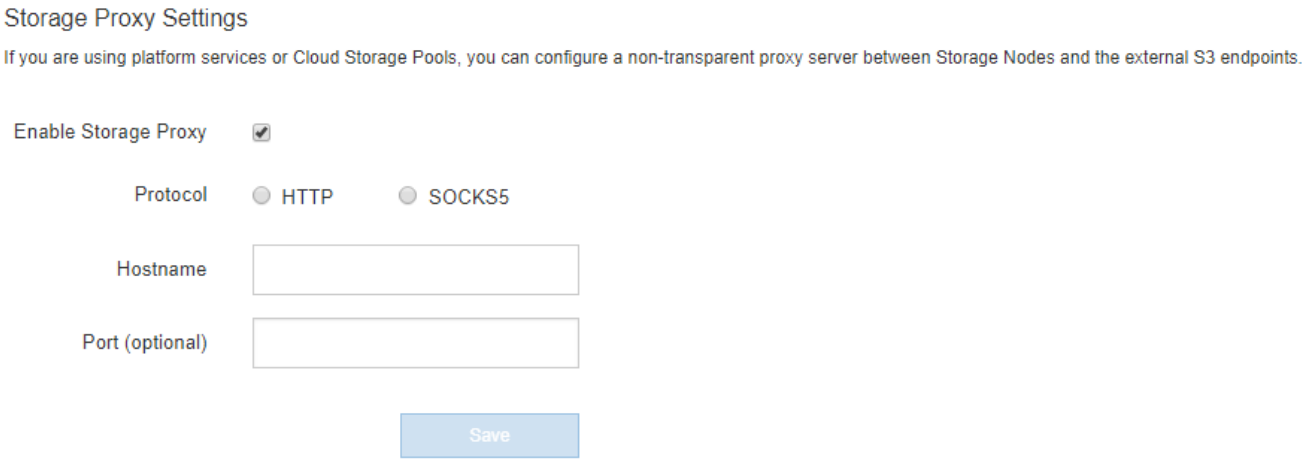
1. Seleccione **Configuración** > **Configuración de red** > **Configuración de proxy**.

   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. Haga clic en **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 haga clic en **Guardar**.

Información relacionada

"Redes y puertos para servicios de plataforma"

"Gestión de objetos con ILM"

Configurando los ajustes del proxy de administrador

Si envía mensajes de AutoSupport mediante HTTP o HTTPS, puede configurar un servidor proxy no transparente entre los nodos de administrador y el soporte técnico (AutoSupport).

Lo que necesitará

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

Acerca de esta tarea

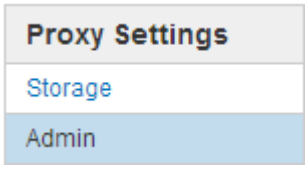
Puede configurar los ajustes de un único proxy de administración.

Pasos

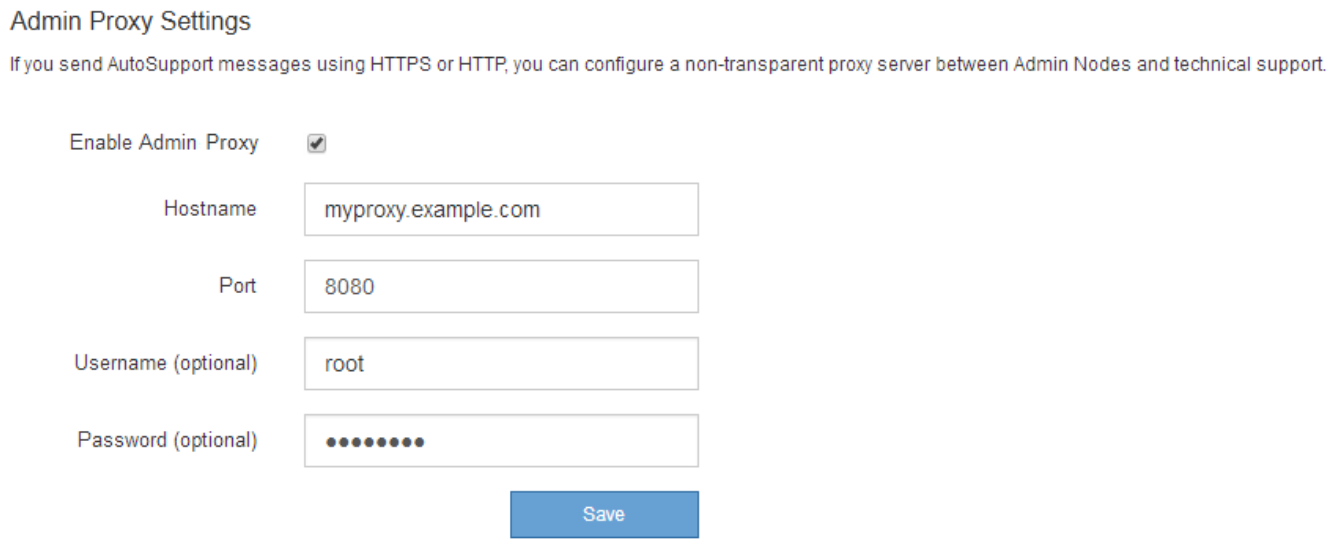
1. Seleccione **Configuración** > **Configuración de red** > **Configuración de proxy**.

   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. Haga clic en **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 haga clic en **Guardar**.

Información relacionada

"Especificar el protocolo para los mensajes de AutoSupport"

Gestión de 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 y límites opcionales

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.

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

> 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.

Limitación del tráfico

Cuando ha creado directivas de clasificación de tráfico, el tráfico se limita según el tipo de reglas y límites establecidos. 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.

Uso de políticas de clasificación del tráfico con 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 Ancho de banda de 5 GB/s (40 Gbps)	por mes
Plata	Capacidad de almacenamiento de 250 TB	2 regla de copia de ILM	10 000 solicitudes/s Ancho de banda de 1.25 GB/s (10 Gbps)	$$ al mes

Nivel de servicio	Capacidad	Protección de datos	Rendimiento	Coste
Bronce	Capacidad de almacenamiento de 100 TB	2 regla de copia de ILM	5 000 solicitudes/s Ancho de banda de 1 GB/s (8 Gbps)	$ al mes

Creación de 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.

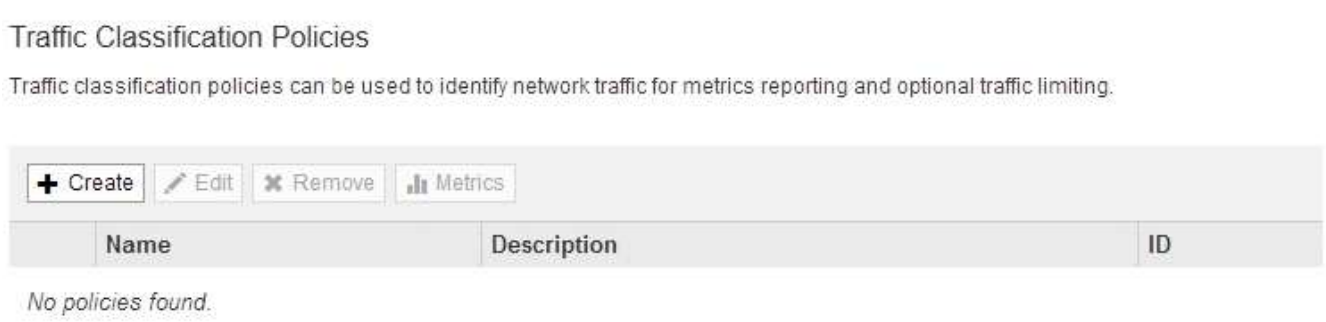
Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.
- Debe haber creado cualquier punto final de equilibrador de carga que desee que coincida.
- Debe haber creado los inquilinos que desee que coincidan.

Pasos

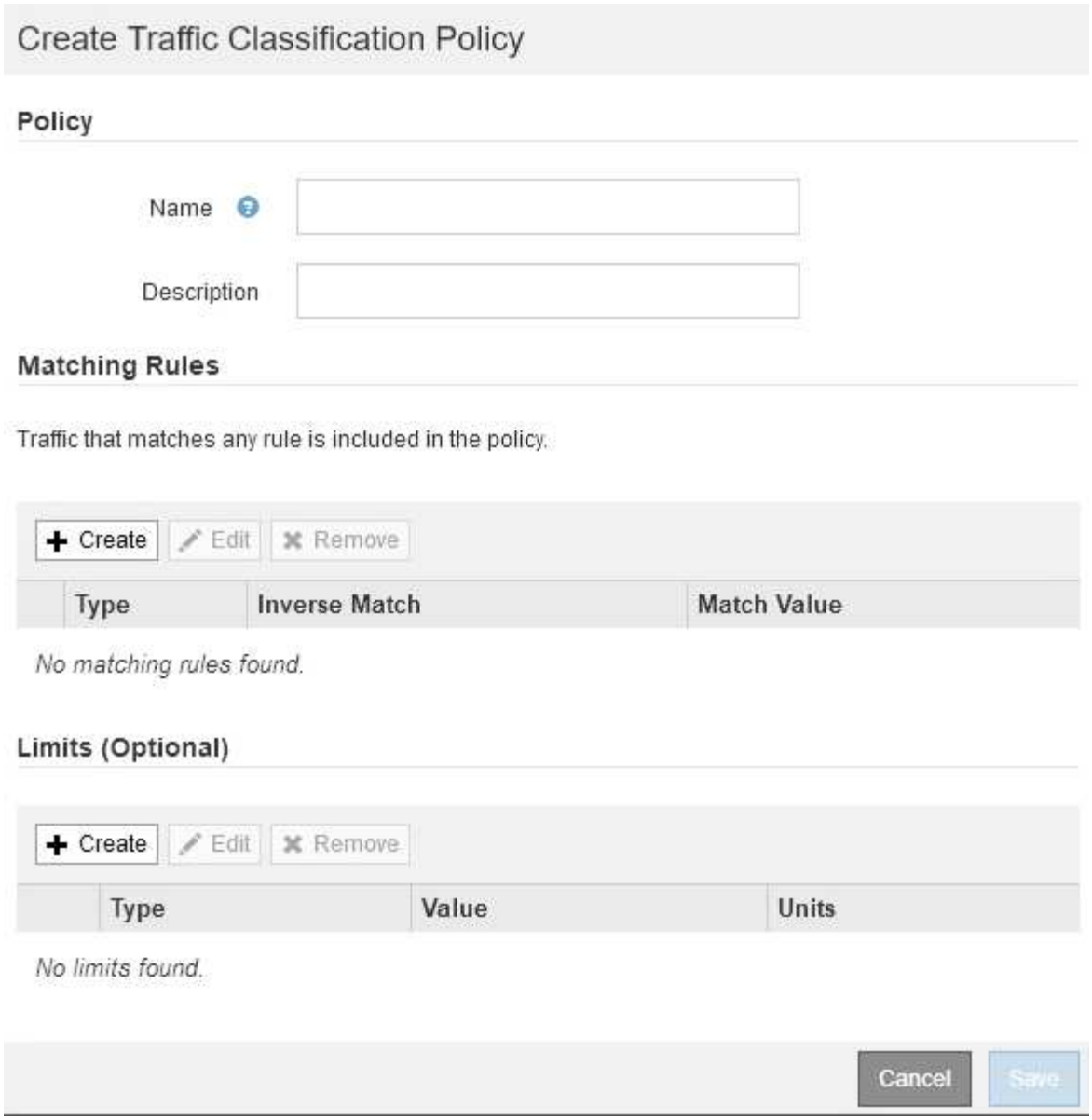
1. Seleccione **Configuración** > **Configuración de red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico.



2. Haga clic en **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**.

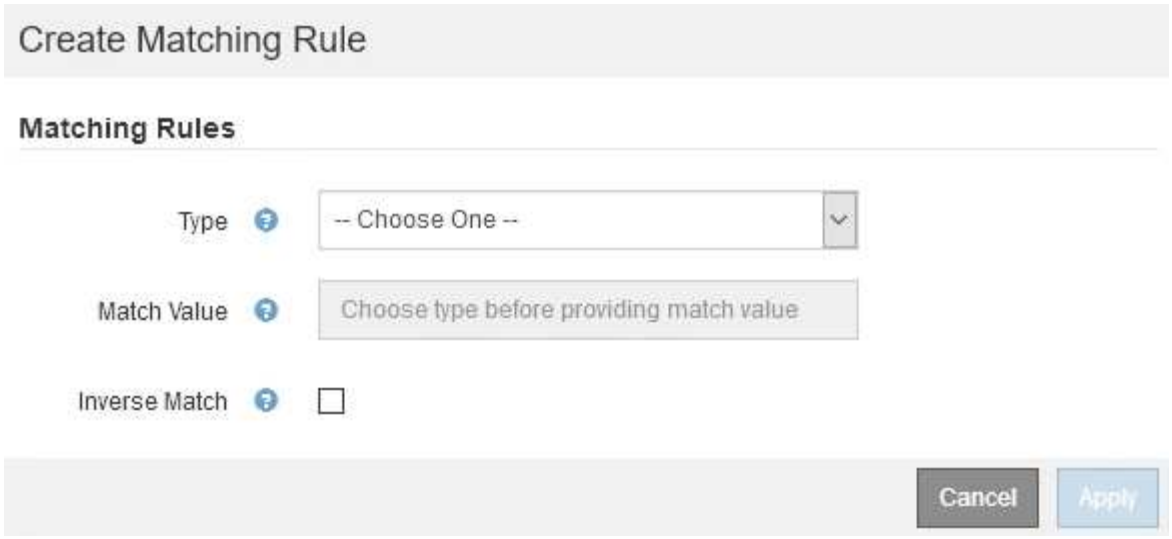
   Por ejemplo, describa a qué se aplica esta política de clasificación del tráfico y a qué se limitará.

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. Haga clic en **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.
   - 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.

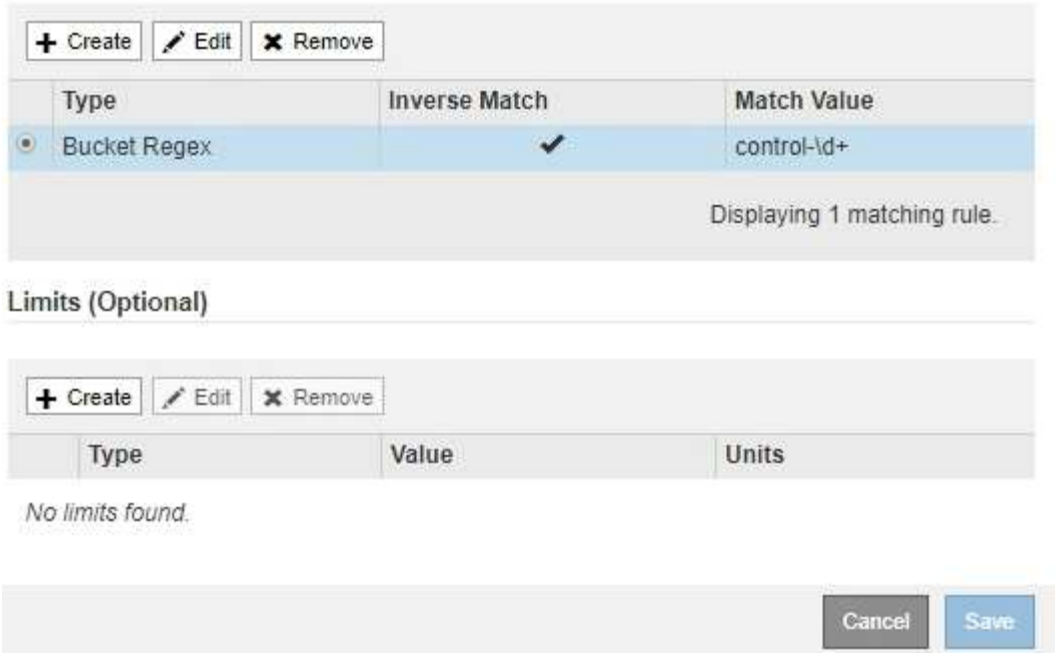
d. Si desea hacer coincidir todo el tráfico de red *excepto* que sea coherente con el valor Type and Match que acaba de definir, active la casilla de verificación **Inverse** . De lo contrario, deje la casilla de verificación sin seleccionar.

   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. Haga clic en **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.

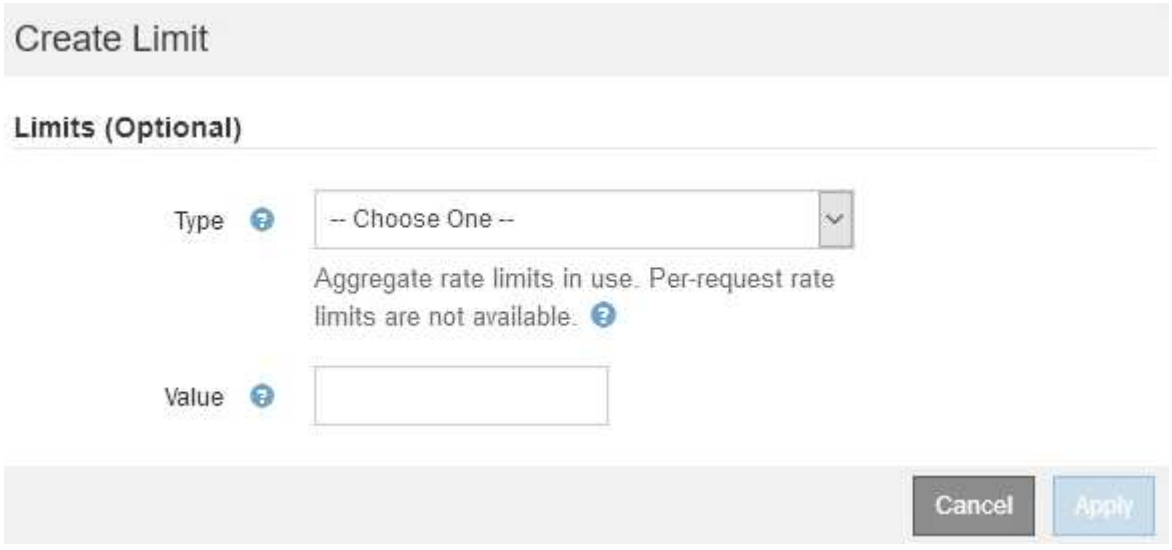
> El tráfico que coincide con cualquier regla se gestiona mediante la directiva.

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. Haga clic en **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:

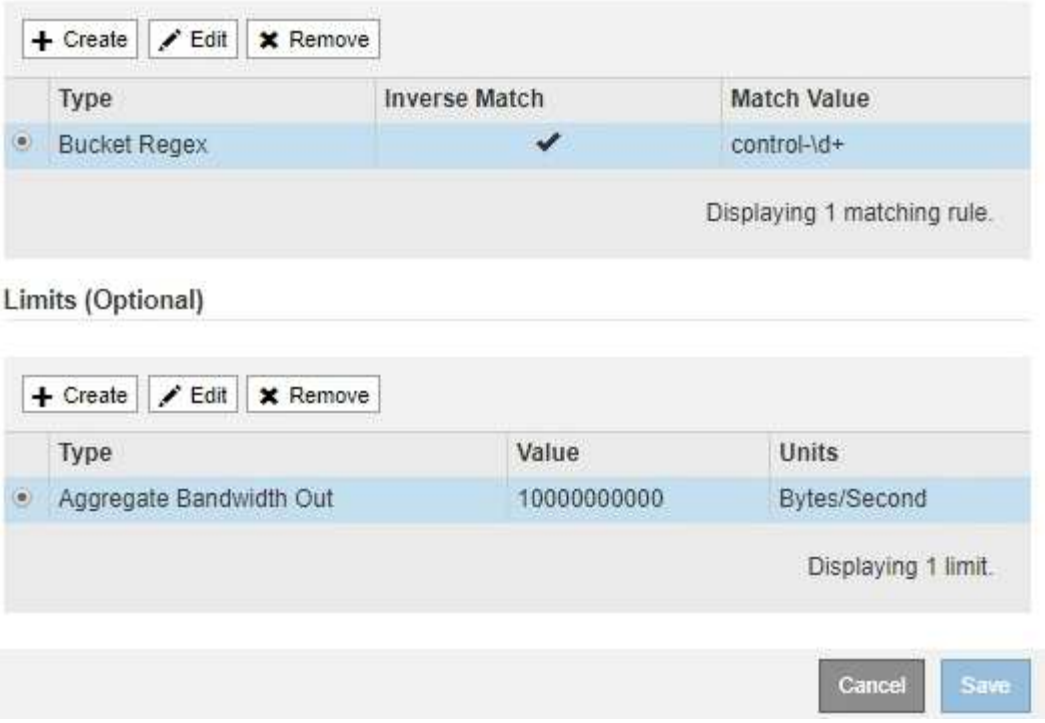
- Dirección IP exacta (/máscara 32)
- Nombre exacto del cucharón
- Regex. Cucharón
- Inquilino
- Extremo
- Coincidencias CIDR no exactas (no /32)
- Coincidencias inversas

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. Haga clic en **aplicar**.

   El límite se crea y se muestra en la tabla límites.



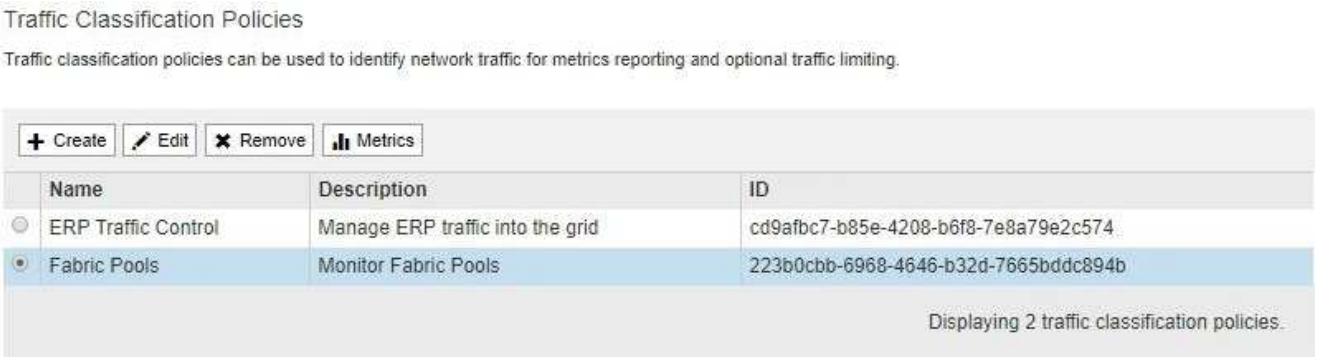
e. Repita estos pasos para cada límite que desee agregar a la directiva.

   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, haga clic en **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.

Información relacionada

"Gestión del equilibrio de carga"

"Ver las métricas de tráfico de red"

Edición de 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.

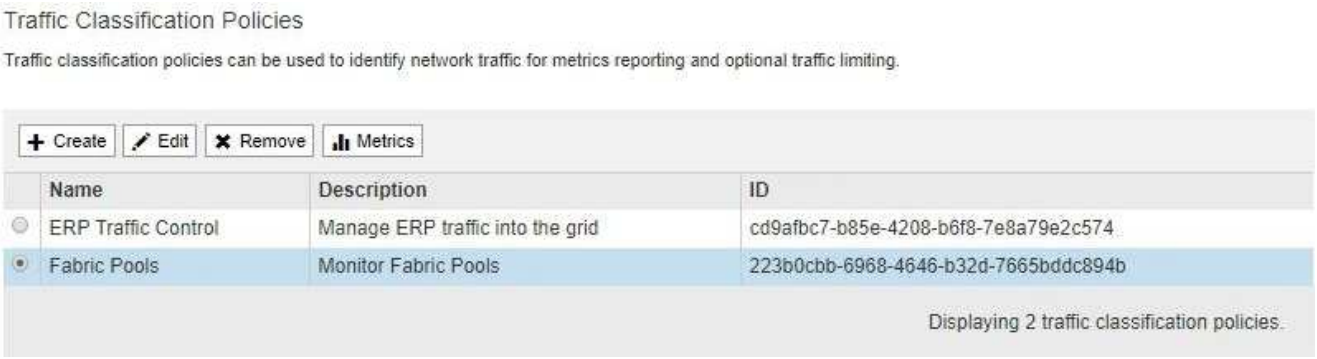
Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Pasos

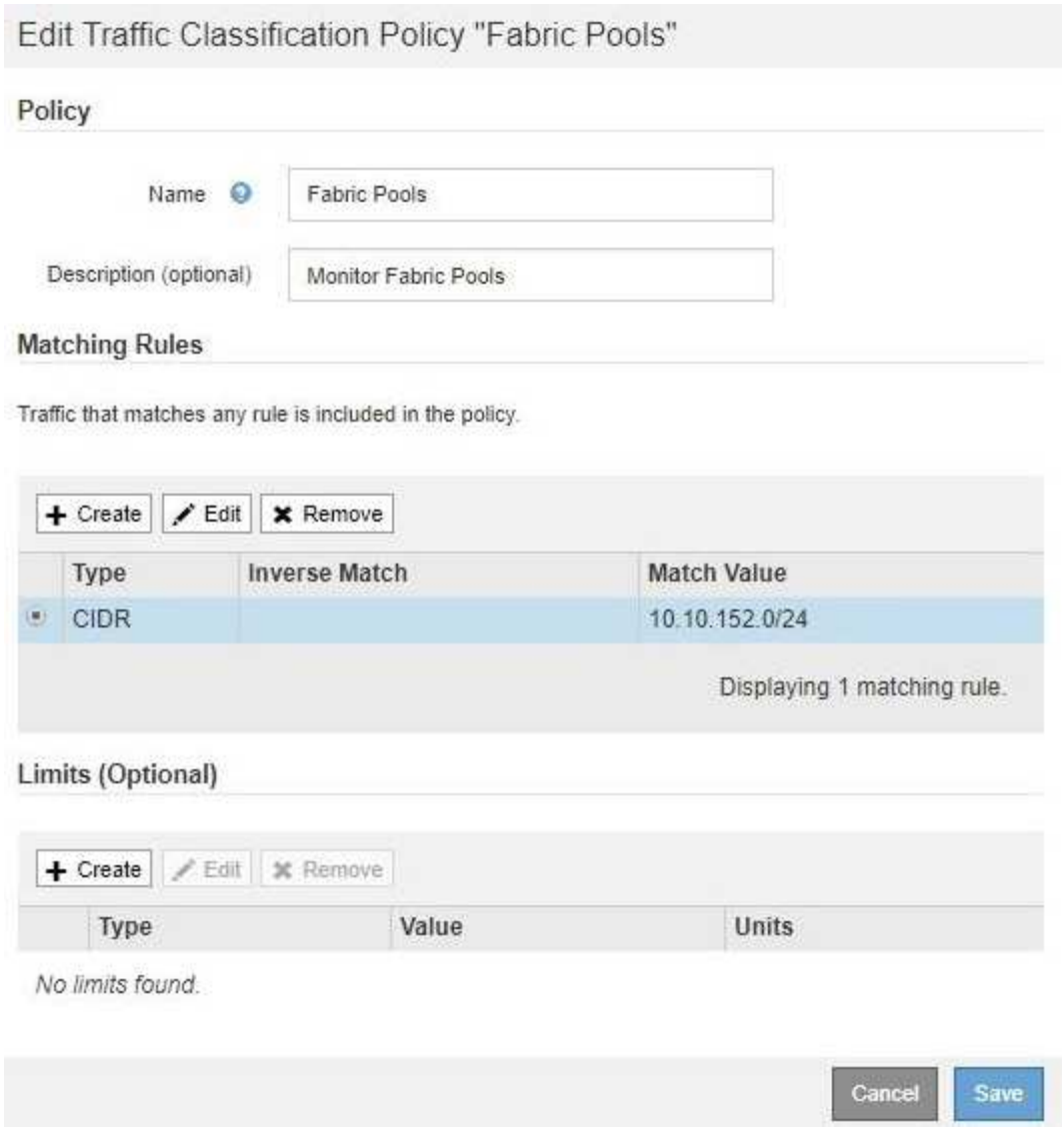
1. Seleccione **Configuración** > **Configuración de red** > **Clasificación de tráfico**.

   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. Haga clic en **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, haga clic en **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 de la regla o límite, haga clic en **Editar** en la sección **Reglas coincidentes** o en 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 haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar la regla o el límite.
5. Cuando haya terminado de crear o editar una regla o un límite, haga clic en **aplicar**.
6. Cuando termine de editar la directiva, haga clic en **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.

Eliminación de una directiva de clasificación de tráfico

Si ya no necesita una directiva de clasificación del tráfico, puede eliminarla.

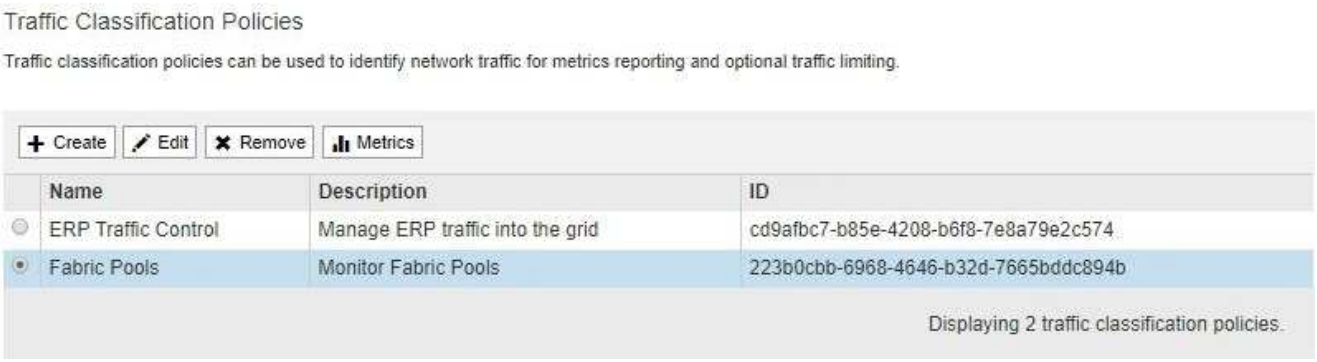
Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Pasos

1. Seleccione **Configuración** > **Configuración de 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. Haga clic en **Quitar**.

   Aparecerá un cuadro de diálogo Advertencia.

4. Haga clic en **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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

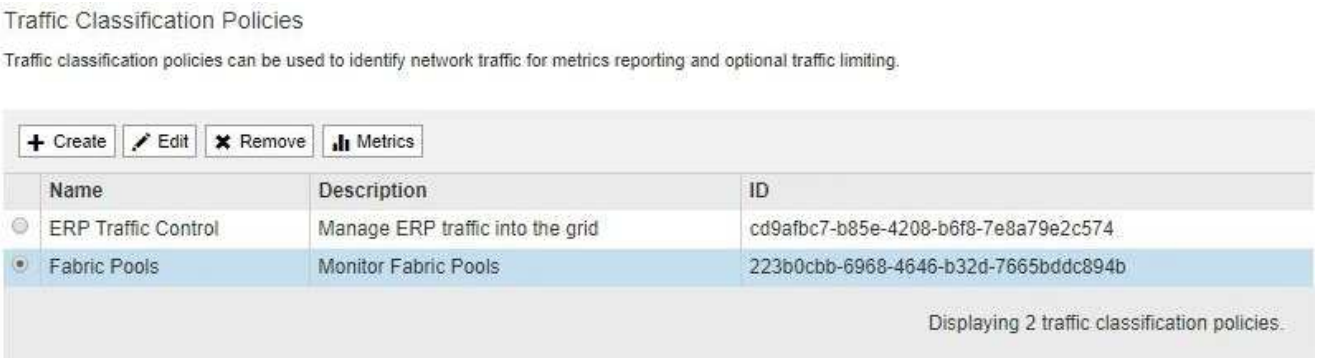
Para cualquier directiva de clasificación de tráfico existente, puede ver las métricas del servicio Load Balancer para determinar si la directiva limita correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si es necesario ajustar la política.

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** > **Configuración de 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 política para la que desea ver las métricas.
3. Haga clic en **métricas**.

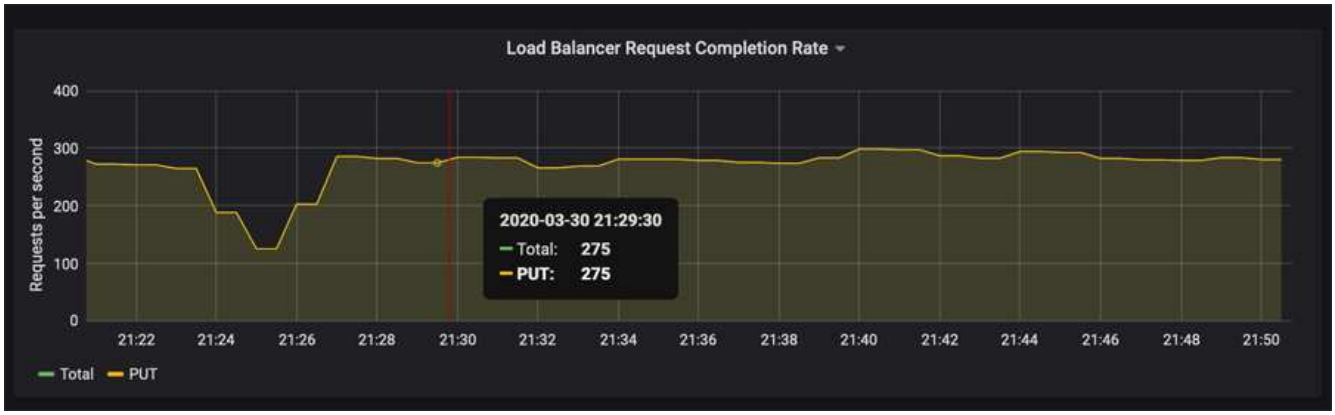
   Se abrirá una nueva ventana del explorador y aparecerán los gráficos de la directiva de clasificación del tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Puede seleccionar otras directivas para visualizarlas mediante el menú desplegable **Policy**.

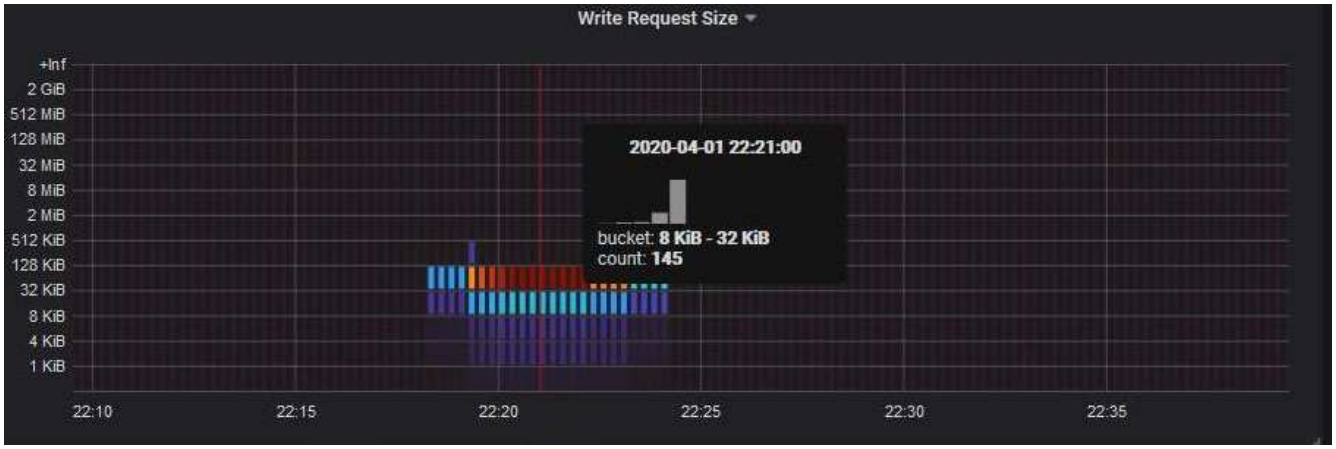
Los siguientes gráficos están incluidos en la página web.

- 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 **Soporte**.
   a. Seleccione **Soporte** > **Herramientas** > **parámetros**.
   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

"Solución de problemas de monitor"

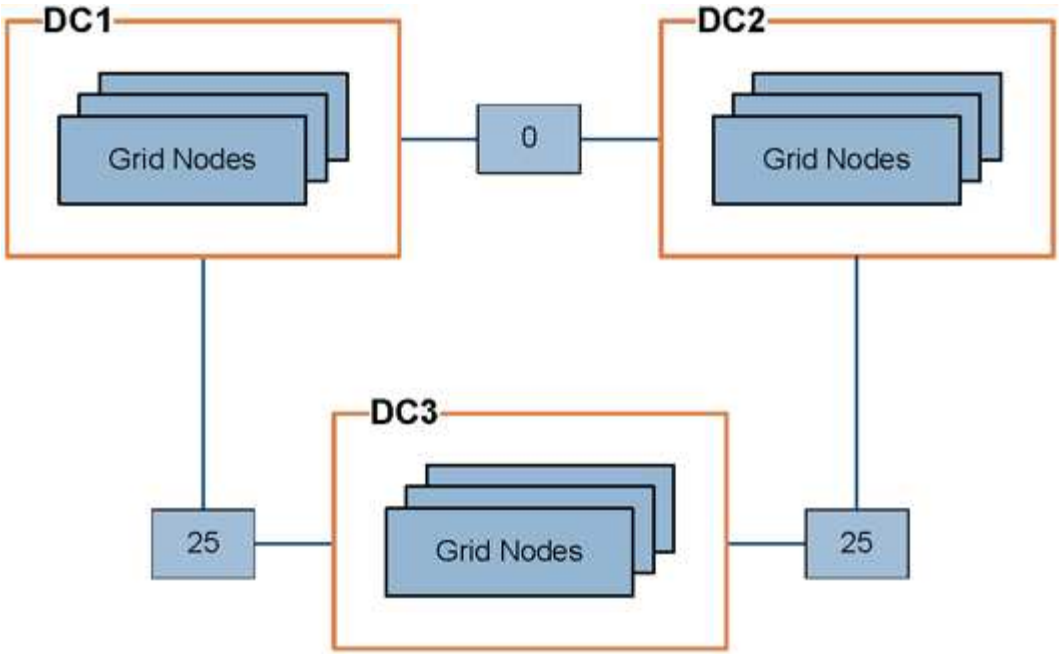
¿Cuáles son los costes de enlace

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 los utiliza el servicio CLB en los nodos de puerta de enlace para dirigir las conexiones del cliente.

  El servicio CLB está obsoleto.

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.

Información relacionada

"Cómo funciona el equilibrio de carga: Servicio CLB"

Actualizando costes de enlace

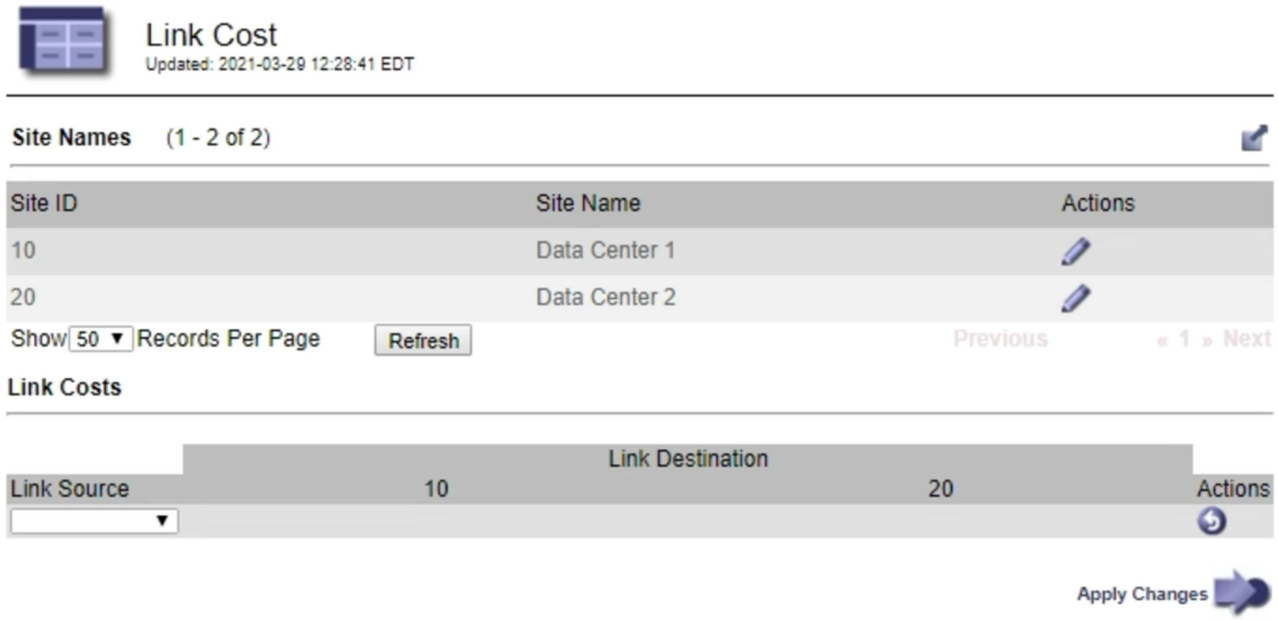
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso Grid Topology Page Configuration.

Pasos

1. Seleccione **Configuración** > **Ajustes de 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, haga clic en **Revert**.

3. Haga clic en **aplicar cambios**.

Configurando 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
- Información de eventos tal como se muestra en la página **Nodes** > ***Grid Node*** > **Eventos**
- 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.

Puede seleccionar el símbolo «'x'» para cerrar el mensaje. El mensaje no volverá a aparecer hasta que se borre la caché del explorador, incluso si AutoSupport queda deshabilitado.

Uso de Active IQ

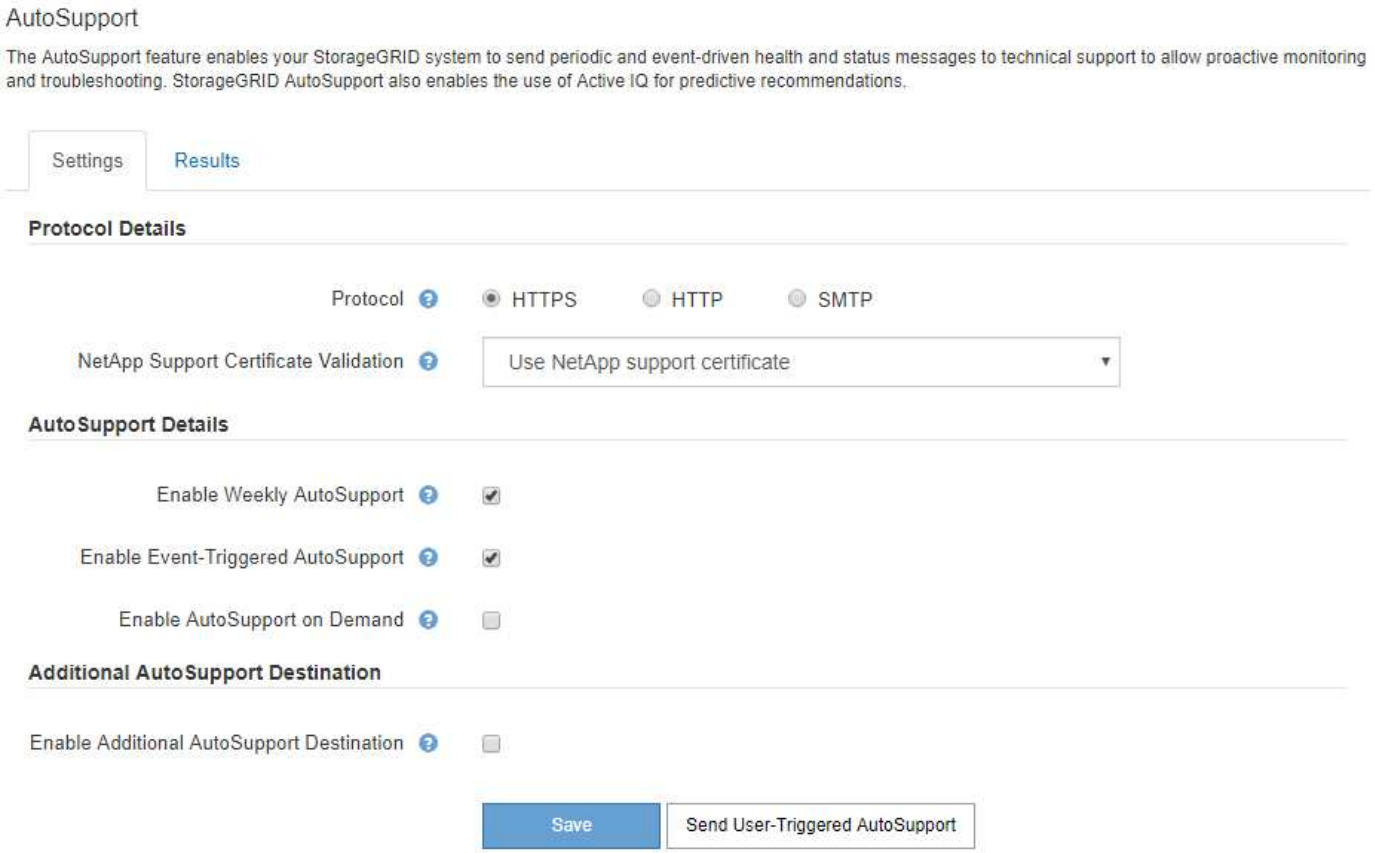
Active IQ es un asesor digital basado en cloud que aprovecha el análisis predictivo y los conocimientos de la comunidad de la base instalada de NetApp. Sus evaluaciones de riesgos continuas, las alertas predictivas, las directrices prescriptivas y las acciones automatizadas le ayudan a evitar problemas 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"

Accediendo a la configuración de AutoSupport

La configuración de AutoSupport se realiza mediante Grid Manager (**asistencia** > **Herramientas** > **AutoSupport**). La página **AutoSupport** tiene dos fichas: **Ajustes** y **resultados**.



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"

Especificar el protocolo para los mensajes de AutoSupport

Puede usar uno de los tres protocolos para enviar mensajes de AutoSupport.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.
- Si va a utilizar el protocolo HTTPS o HTTP para enviar mensajes AutoSupport, debe haber proporcionado acceso saliente a Internet al nodo de administración principal, ya sea directamente o mediante un servidor proxy (no se necesitan conexiones entrantes).
- Si utilizará el protocolo HTTPS o HTTP y desea utilizar un servidor proxy, debe haber configurado un servidor proxy de administrador.
- Si utilizará SMTP como protocolo para mensajes de AutoSupport, debe haber configurado un servidor de correo SMTP. La misma configuración del servidor de correo se utiliza para las notificaciones de correo electrónico de alarma (sistema heredado).

Acerca de esta tarea

Los mensajes de AutoSupport pueden enviarse utilizando cualquiera de los siguientes protocolos:

- **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 (**Soporte** > **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.

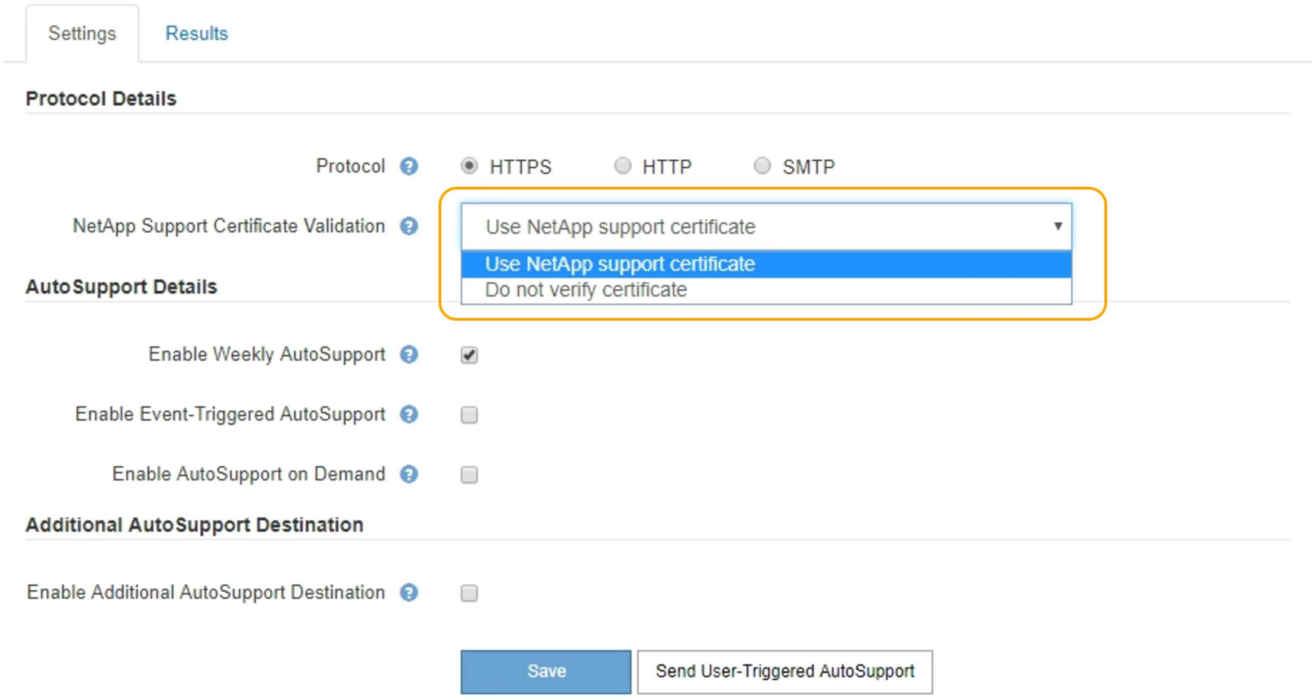
El protocolo configurado se utiliza para enviar todos los tipos de mensajes de AutoSupport.

Pasos

1. Seleccione **Soporte** > **Herramientas** > **AutoSupport**.

   Aparece la página AutoSupport y la ficha **Configuración** está seleccionada.

2. Seleccione el protocolo que desea utilizar para enviar mensajes de AutoSupport.



3. Seleccione su elección para **validación de certificados de soporte de NetApp**.
   - Utilizar certificado de soporte de NetApp (predeterminado): La validación de certificados garantiza la seguridad de la transmisión de mensajes de 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.

Información relacionada

"Configurando los ajustes del proxy de administrador"

Habilitar AutoSupport bajo demanda

AutoSupport On Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente. Al habilitar AutoSupport on Demand, el soporte técnico puede solicitar el envío de mensajes de AutoSupport sin necesidad de intervención del usuario.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.
- Debe haber habilitado los mensajes de AutoSupport semanales.
- Debe haber establecido el protocolo de transporte en HTTPS.

Acerca de esta tarea

Si habilita 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.

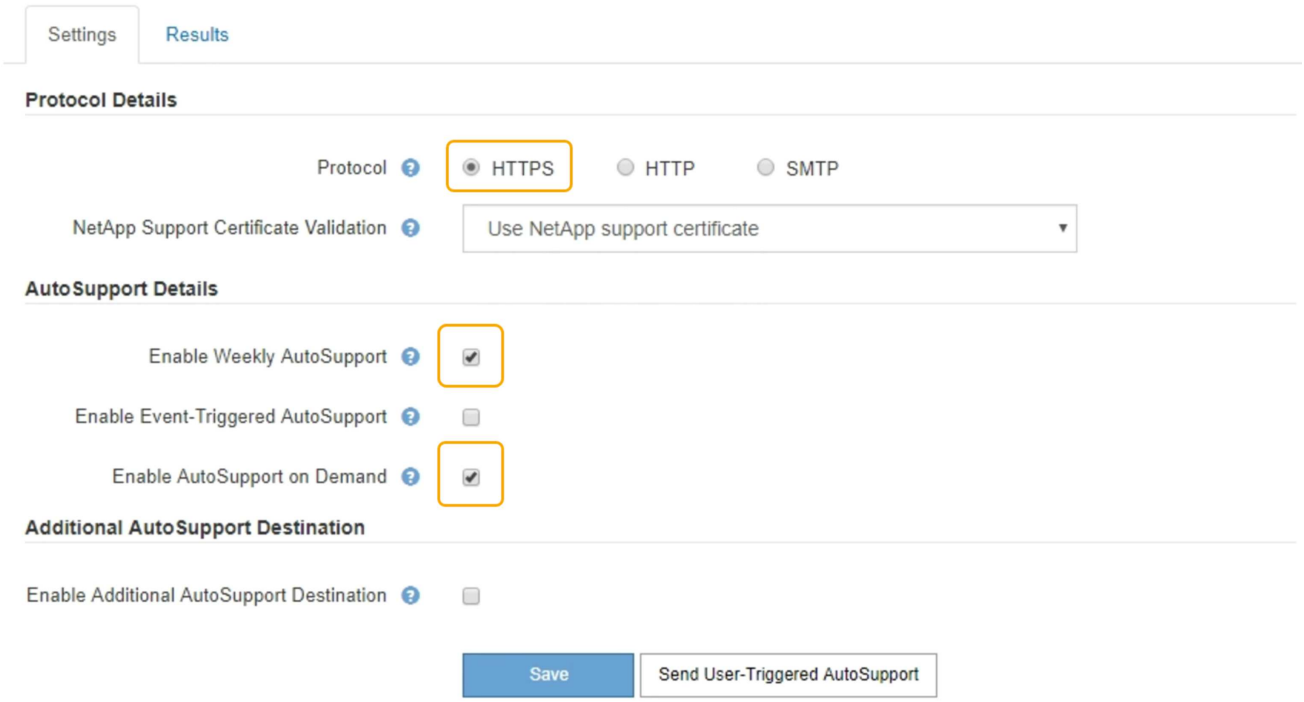
El soporte técnico no puede habilitar o deshabilitar AutoSupport bajo demanda.

Pasos

1. Seleccione **Soporte** > **Herramientas** > **AutoSupport**.

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Seleccione el botón de opción HTTPS en la sección **Detalles del protocolo** de la página.



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.

Deshabilitar los mensajes semanales de AutoSupport

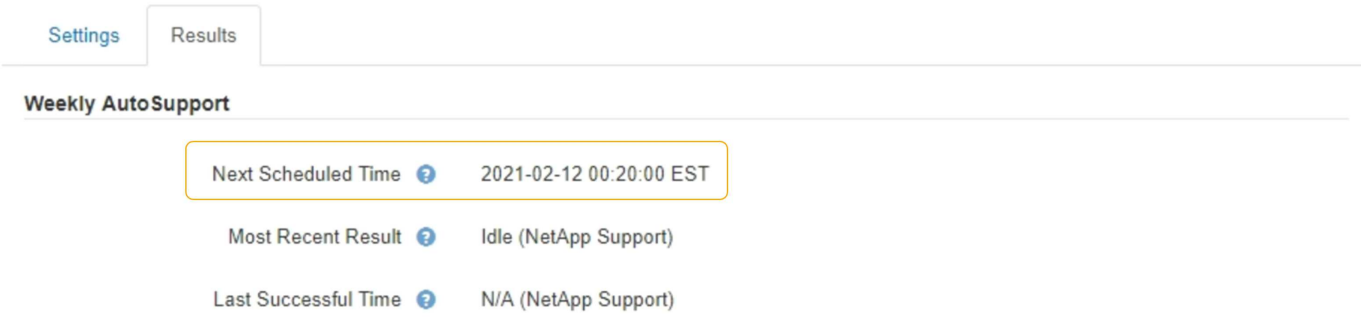
De manera predeterminada, el sistema StorageGRID se configura para que envíe un mensaje de AutoSupport al soporte de NetApp una vez por semana.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.

Acerca de esta tarea

Para determinar cuándo se envía el mensaje semanal de AutoSupport, consulte **la siguiente hora programada** en **AutoSupport semanal** en la página **AutoSupport** > **resultados**.



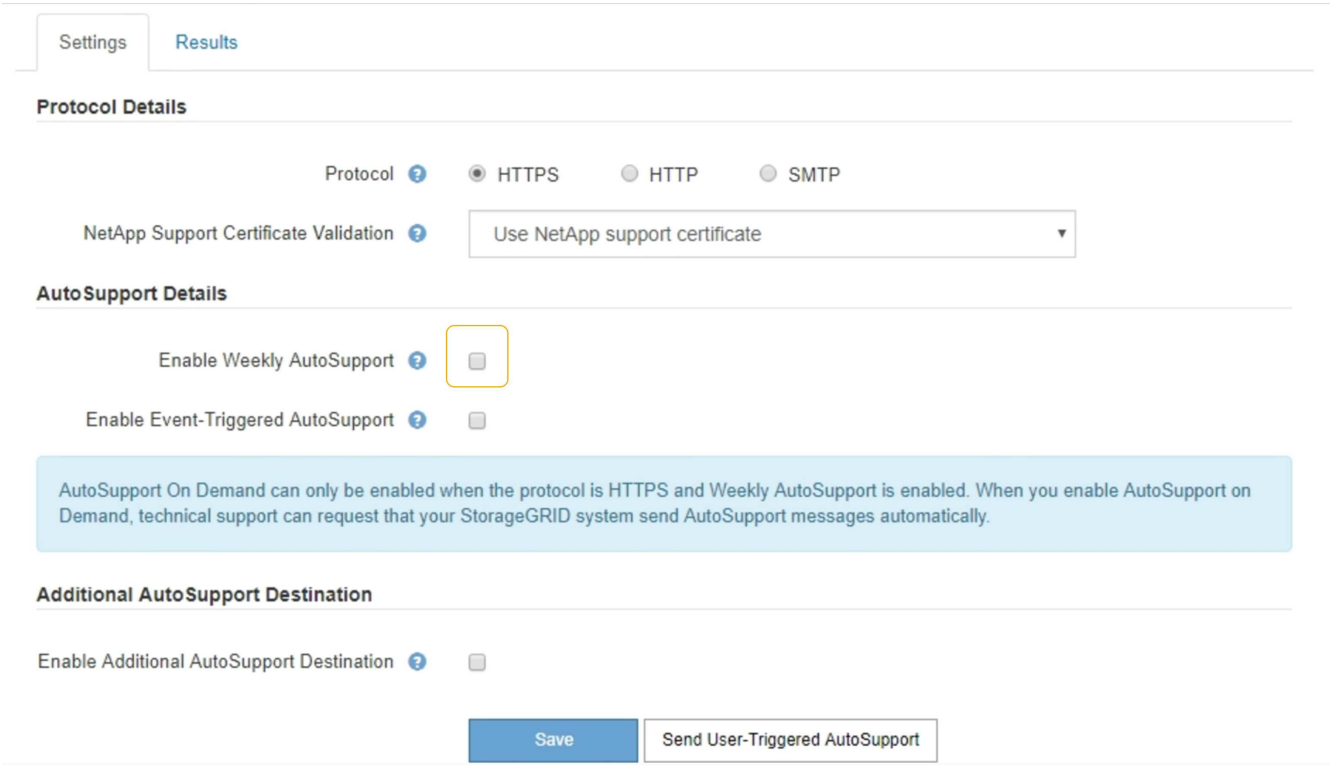
Es posible deshabilitar el envío automático de un mensaje de AutoSupport en cualquier momento.

Pasos

1. Seleccione **Soporte** > **Herramientas** > **AutoSupport**.

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Desactive la casilla de verificación **Activar AutoSupport semanal**.



3. Seleccione **Guardar**.

Deshabilitar 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.

Acerca de esta tarea

Puede deshabilitar los mensajes de AutoSupport activados por eventos en cualquier momento.

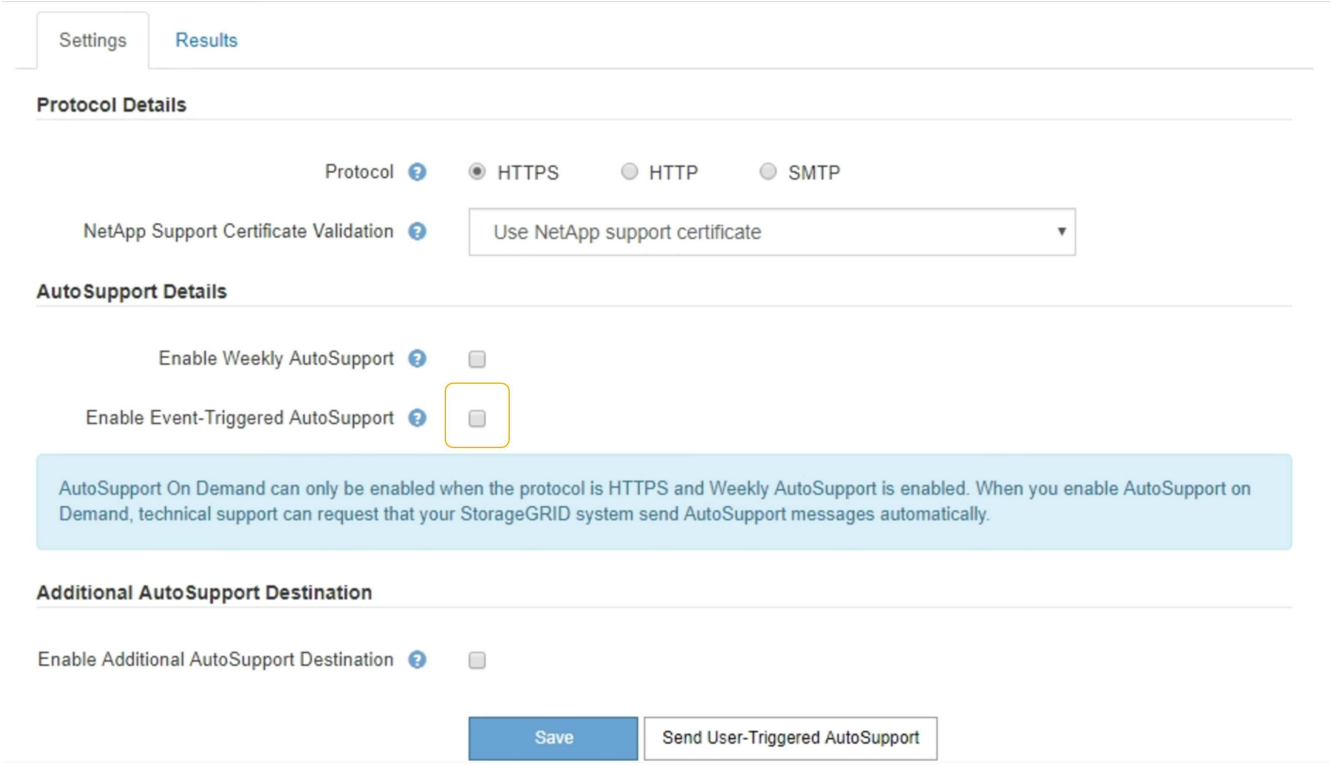
> Los mensajes de AutoSupport activados por los eventos también se suprimen cuando se suprimen las notificaciones de correo electrónico de todo el sistema. (Seleccione **Configuración** > **Configuración del sistema** > **Opciones de pantalla**. A continuación, seleccione **notificación Suprimir todo**.)

Pasos

1. Seleccione **Soporte** > **Herramientas** > **AutoSupport**.

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Desactive la casilla de verificación **Activar AutoSupport** desencadenado por eventos.



3. Seleccione **Guardar**.

Activación manual de 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.

Pasos

1. Seleccione **Soporte** > **Herramientas** > **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.

Adición de un destino 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.

Acerca de esta tarea

Para comprobar o cambiar el protocolo utilizado para enviar mensajes AutoSupport, consulte las instrucciones de especificación de un protocolo AutoSupport.

> No se puede utilizar el protocolo SMTP para enviar mensajes de AutoSupport a un destino adicional.

"Especificar el protocolo para los mensajes de AutoSupport"

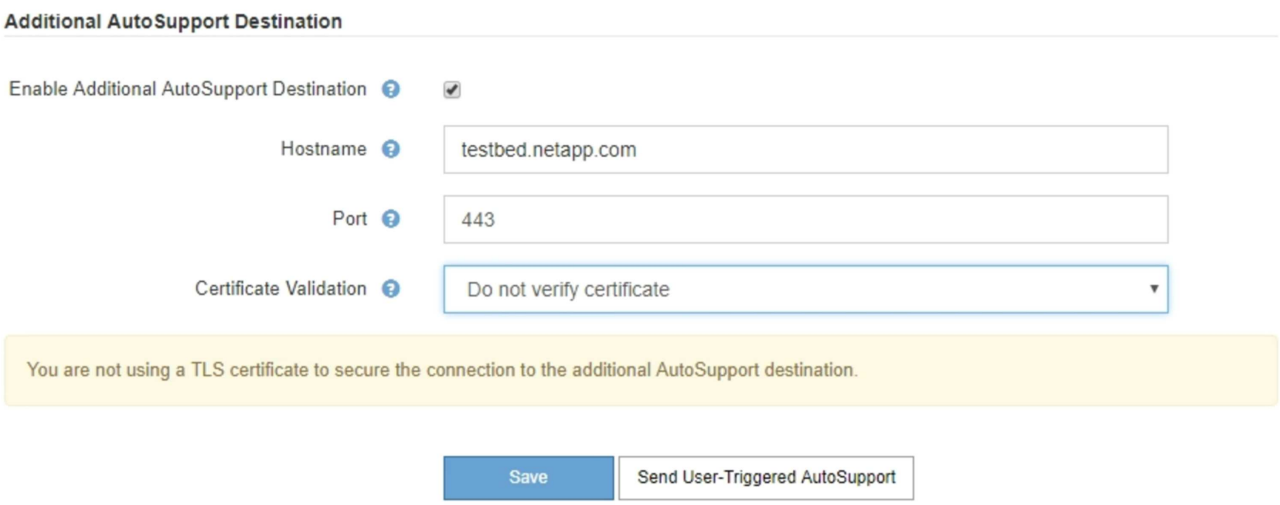
Pasos

1. Seleccione **Soporte** > **Herramientas** > **AutoSupport**.

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Seleccione **Activar destino AutoSupport adicional**.

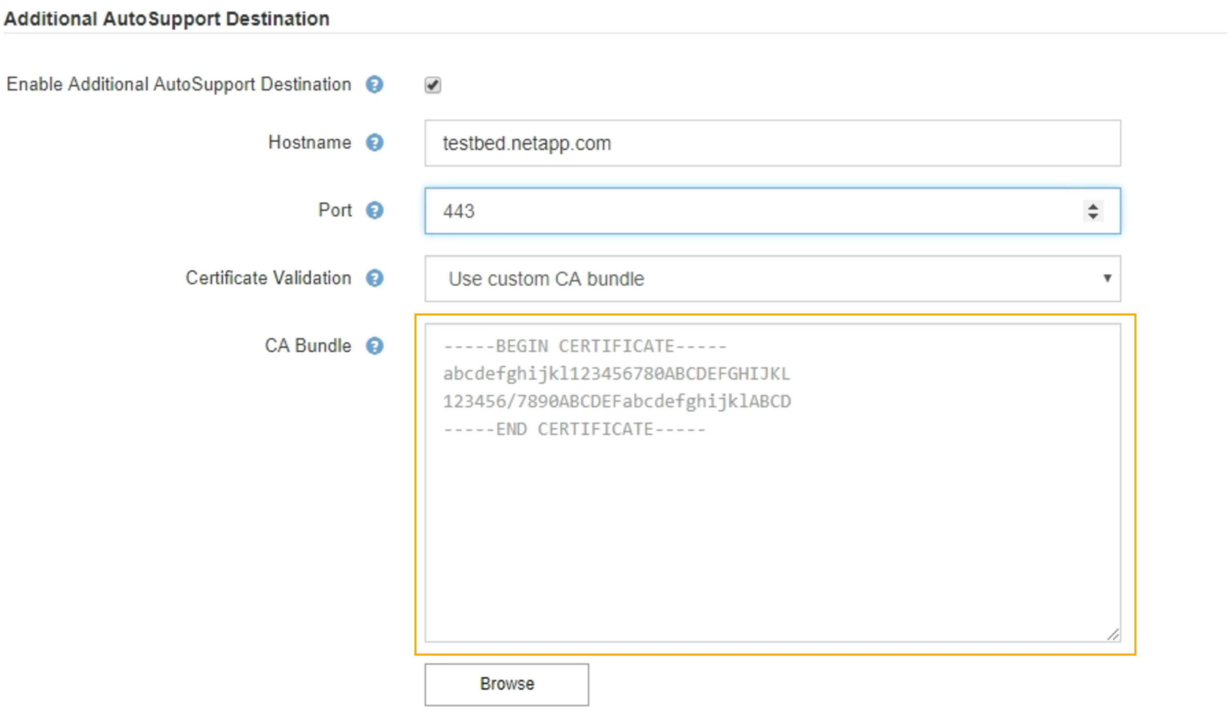
   Aparecerán los campos destino AutoSupport adicional.



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.

Envío de 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 al puerto de gestión del dispositivo de almacenamiento.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un explorador web compatible.
- Tiene el permiso de administrador de Storage Appliance o acceso raíz.

> Debe tener el firmware 8.70 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 las instrucciones para configurar los ajustes del proxy de administración.

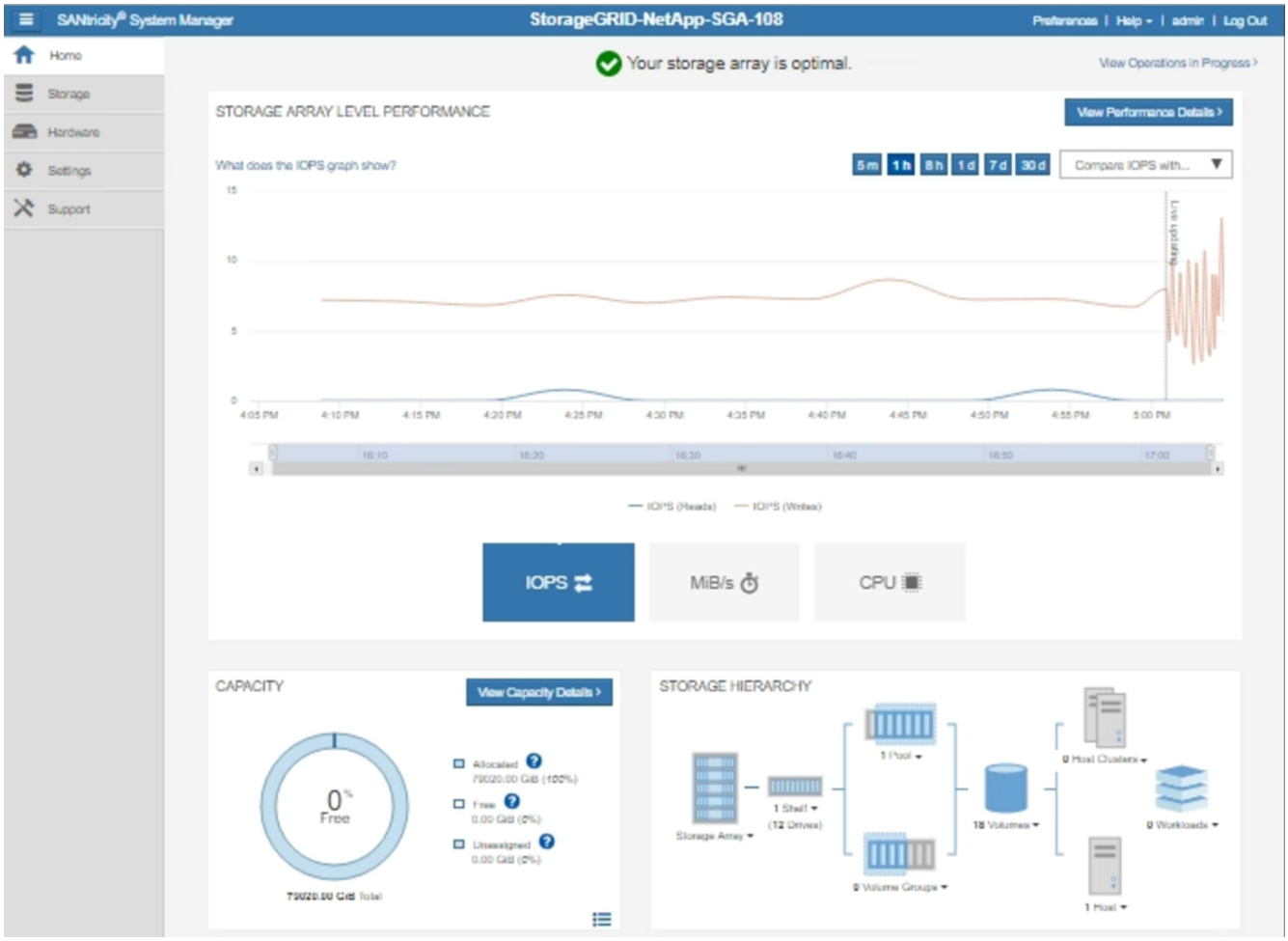
"Configurando los ajustes del proxy de administrador"

> Este procedimiento solo se utiliza para configurar un servidor proxy StorageGRID para los mensajes de AutoSupport E-Series. Para obtener más información sobre la configuración de AutoSupport de E-Series, consulte el centro de documentación de E-Series.
>
> "Centro de documentación para sistemas E-Series y EF-Series de NetApp"

Pasos

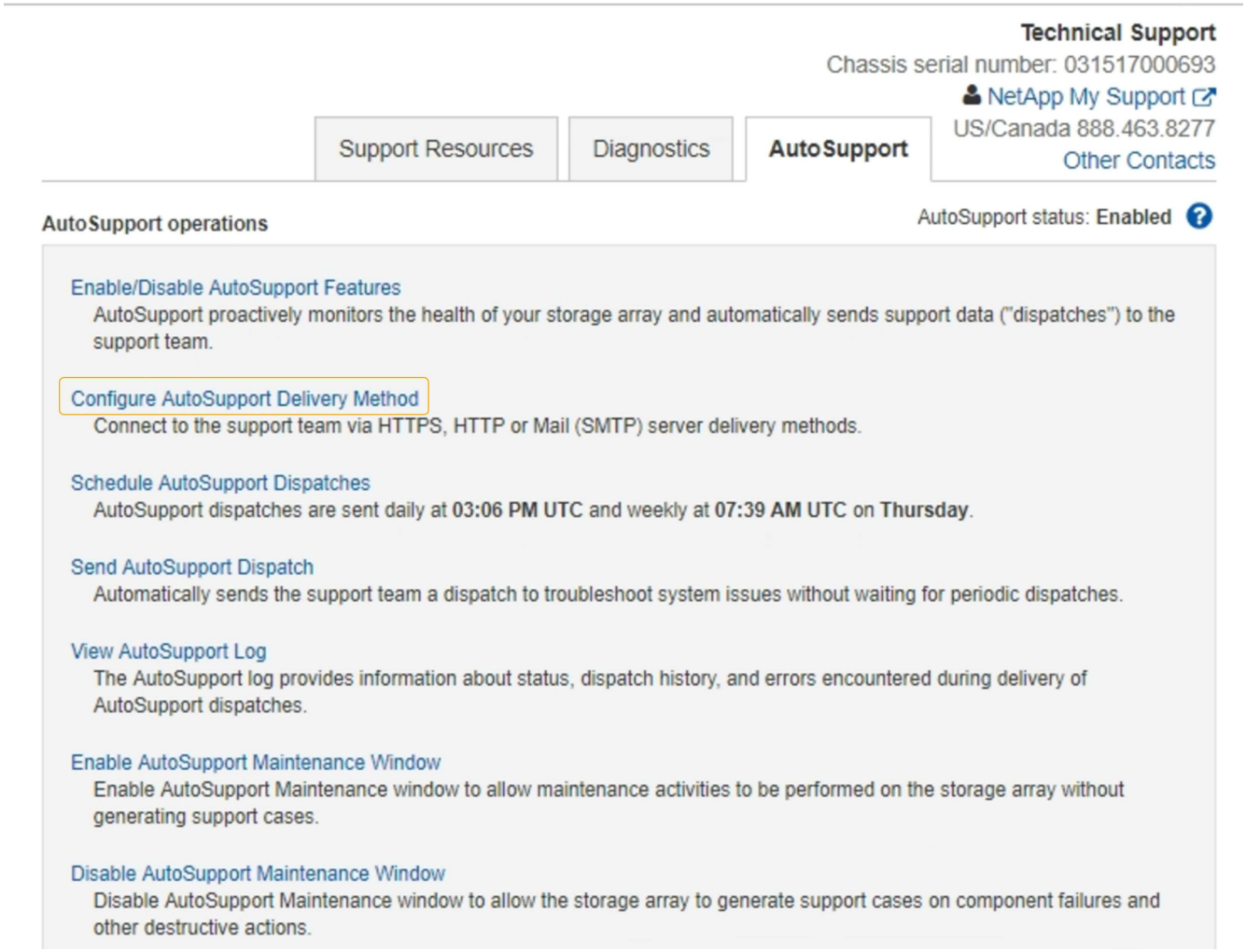
1. En Grid Manager, seleccione **Nodes**.
2. En la lista de nodos que aparece a la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione **Administrador del sistema SANtricity**.

   Se mostrará la página de inicio de SANtricity System Manager.



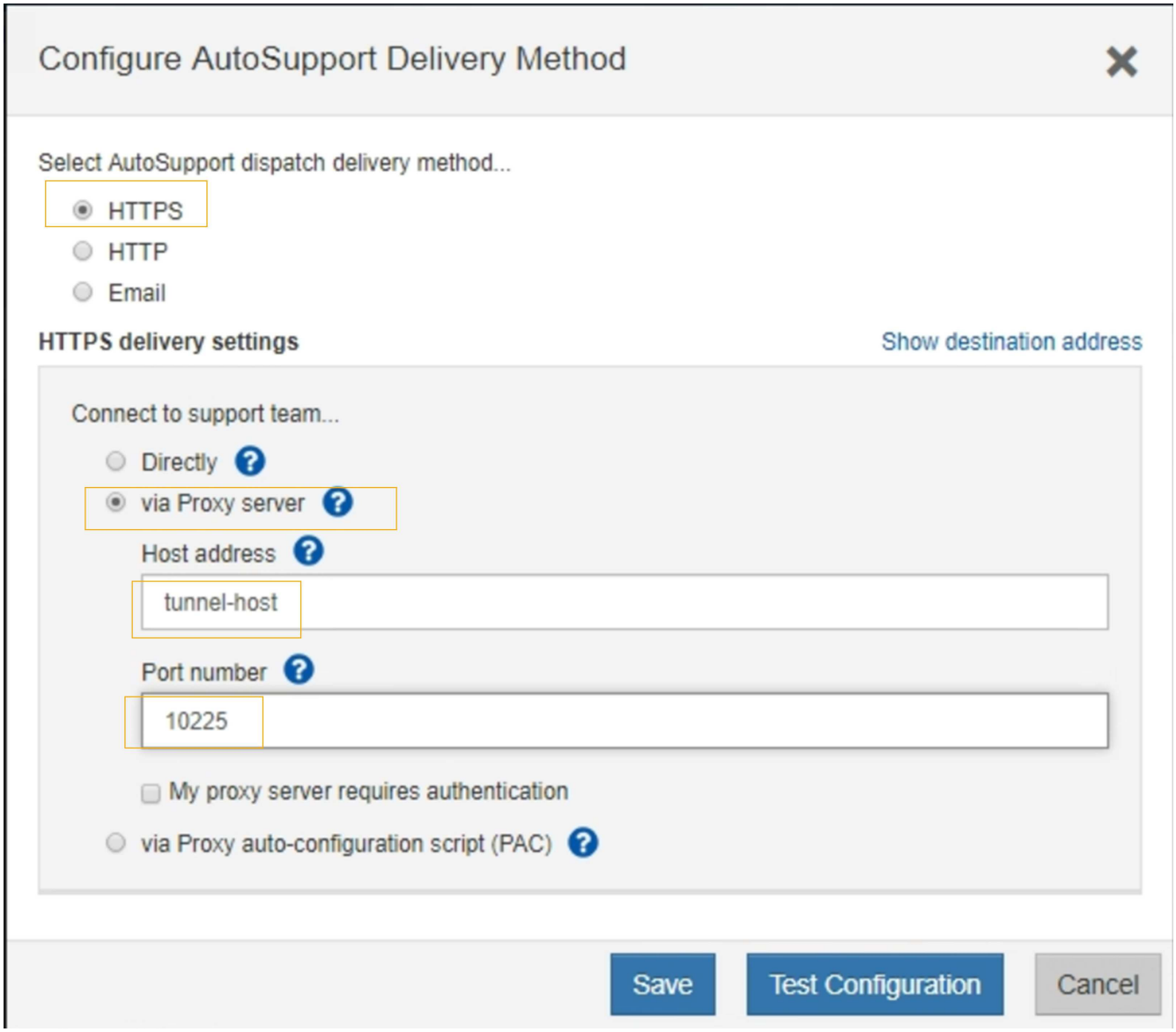
4. Seleccione **Soporte** > **Centro de soporte** > **AutoSupport**.

   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**.

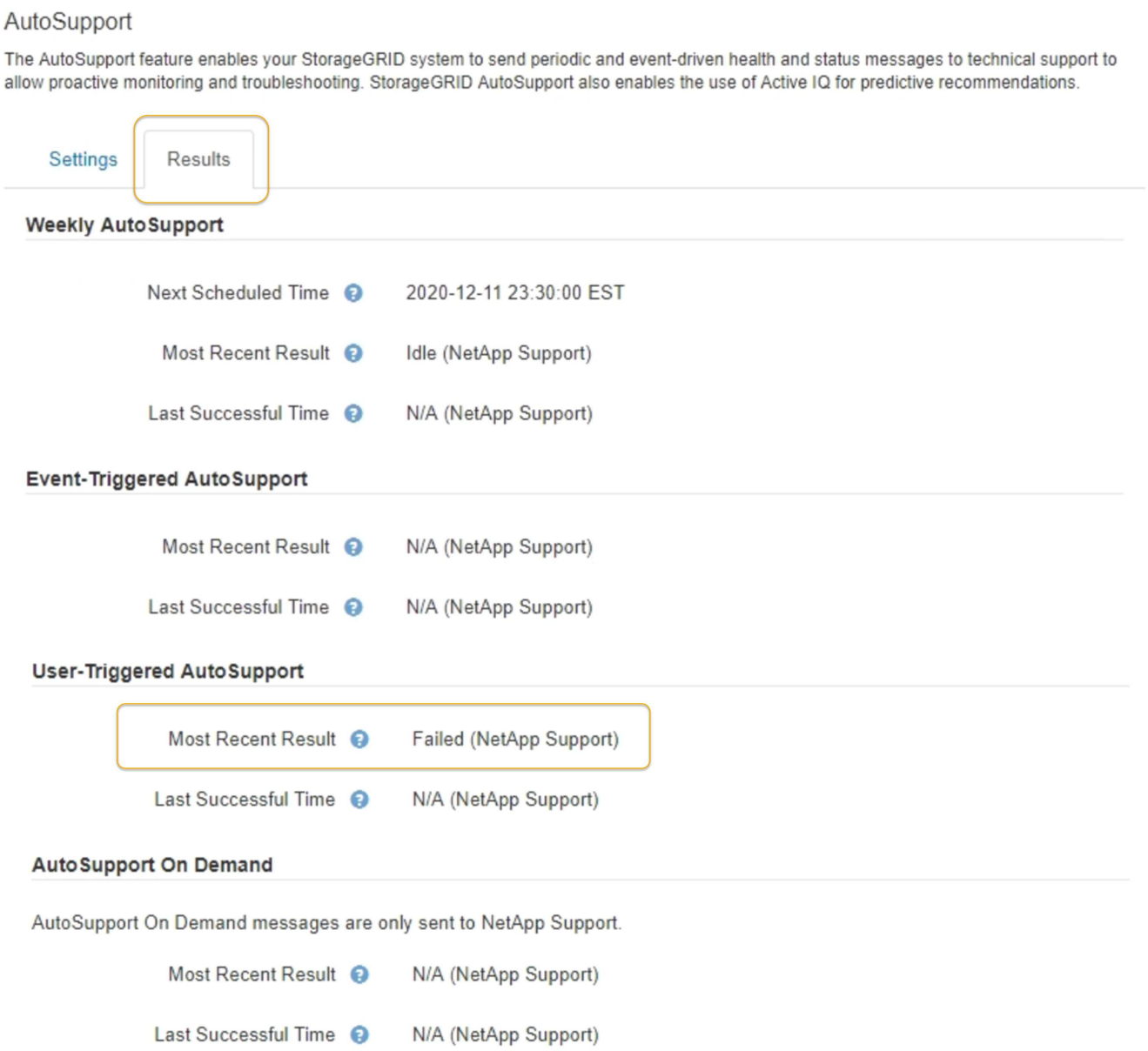
    Se guardará la configuración y aparecerá un mensaje de confirmación: "'se ha configurado el método de entrega de AutoSupport'".

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 **Soporte** > **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** > **Configuración del sistema** > **Opciones de pantalla**. 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 (**Soporte** > **Alarmas (heredadas)** > **> 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 solucionar problemas de instrucciones".

Corrección de un error de 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.`

Información relacionada

"Solución de problemas de monitor"

Gestión de nodos de almacenamiento

Los nodos de almacenamiento proporcionan servicios y capacidad de almacenamiento en disco. La gestión de los nodos de almacenamiento conlleva la supervisión de la cantidad de espacio útil en cada nodo, el uso de la configuración de Marca de agua y la aplicación de los ajustes de configuración del nodo de almacenamiento.

- "Qué es un nodo de almacenamiento"
- "Gestión de opciones de almacenamiento"
- "Gestionar el almacenamiento de metadatos de objetos"
- "Configuración de la configuración global de los objetos almacenados"
- "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 de 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 (**Soporte** > **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.

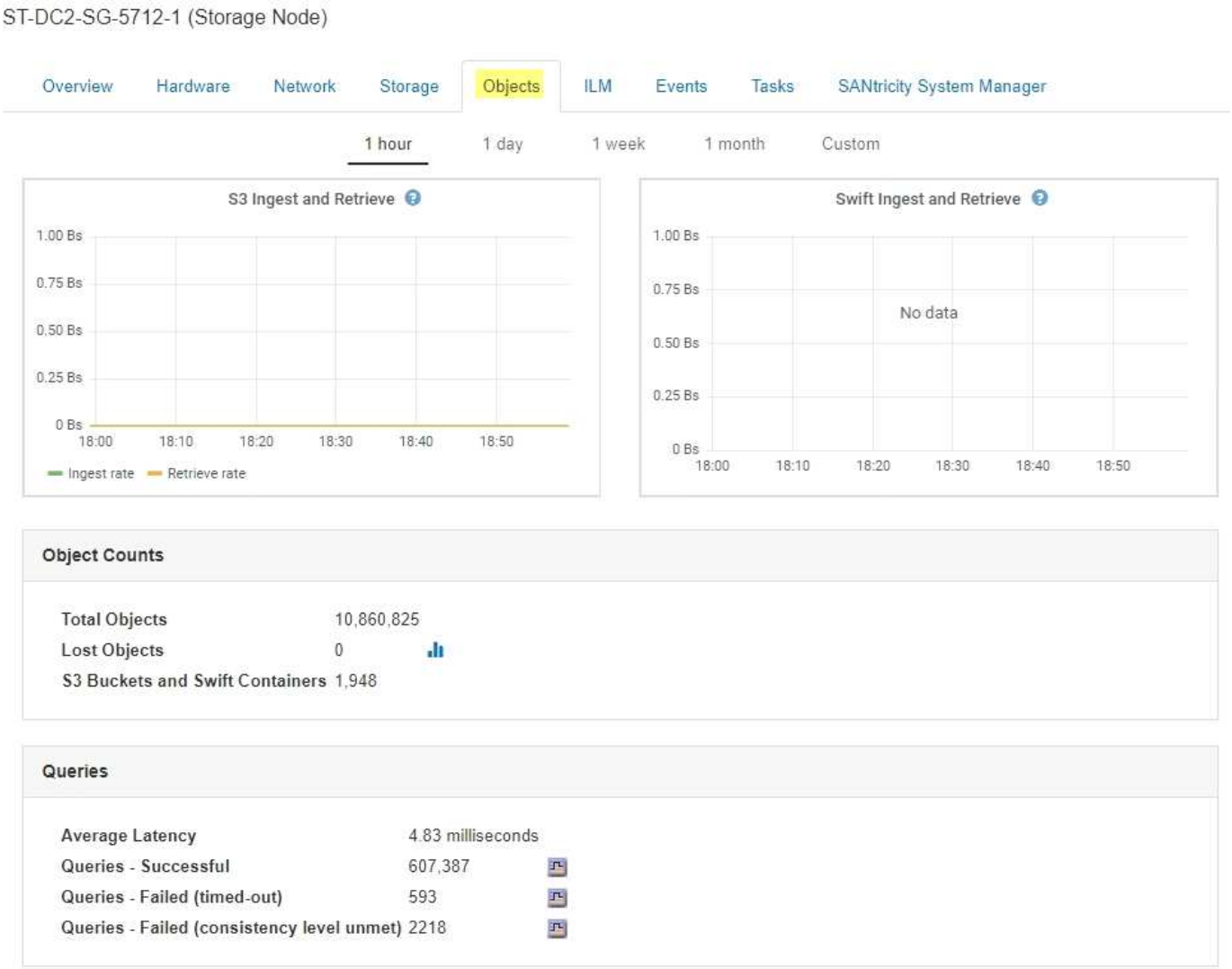
Qué es el servicio DDS

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 "Ejecución de diagnósticos".

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 "Ejecución de diagnósticos".

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 la consola o en la página Nodes > pestaña ILM para cada nodo de almacenamiento.

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	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	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.

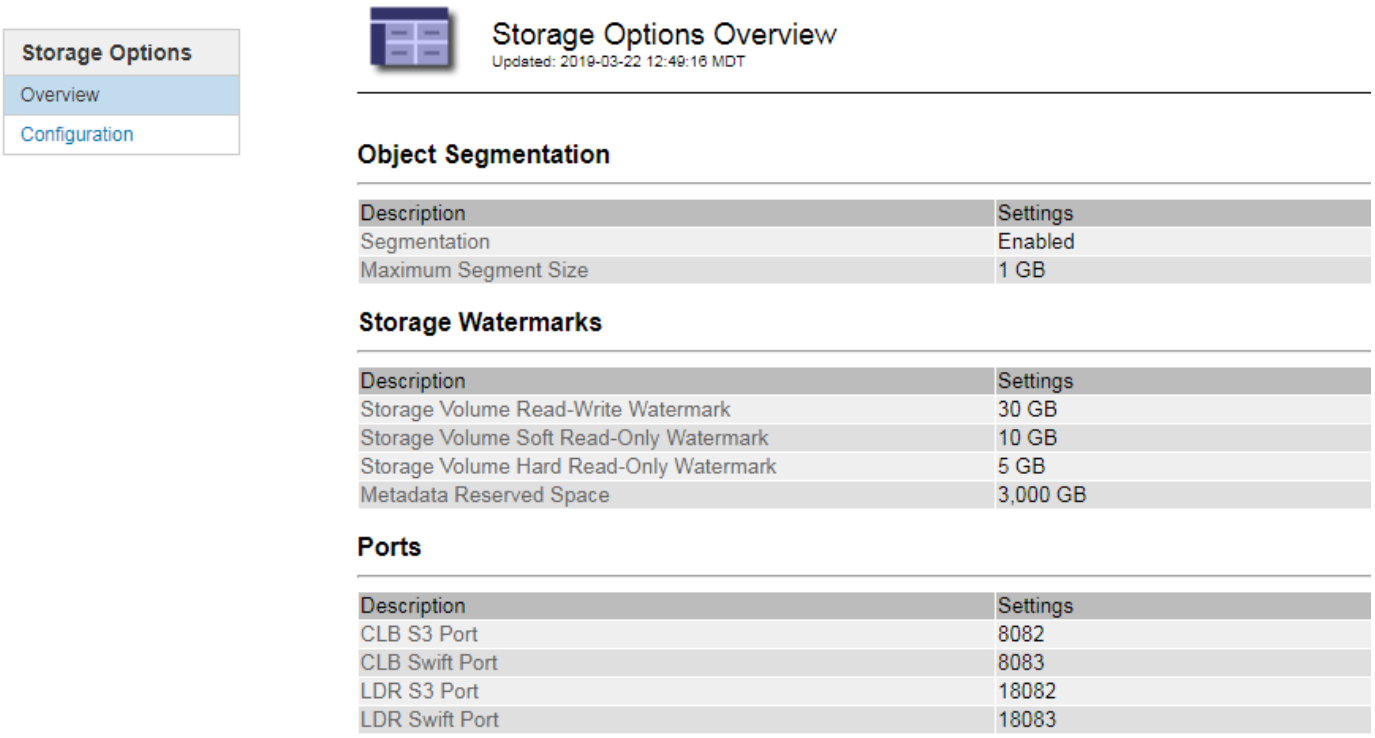
"Gestionar el almacenamiento de metadatos de objetos"

Gestión de opciones de almacenamiento

Puede ver y configurar Opciones de almacenamiento mediante el menú Configuración del Gestor de grid. Opciones de almacenamiento incluyen la configuración de

segmentación de objetos y los valores actuales para las marcas de agua de almacenamiento. 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.

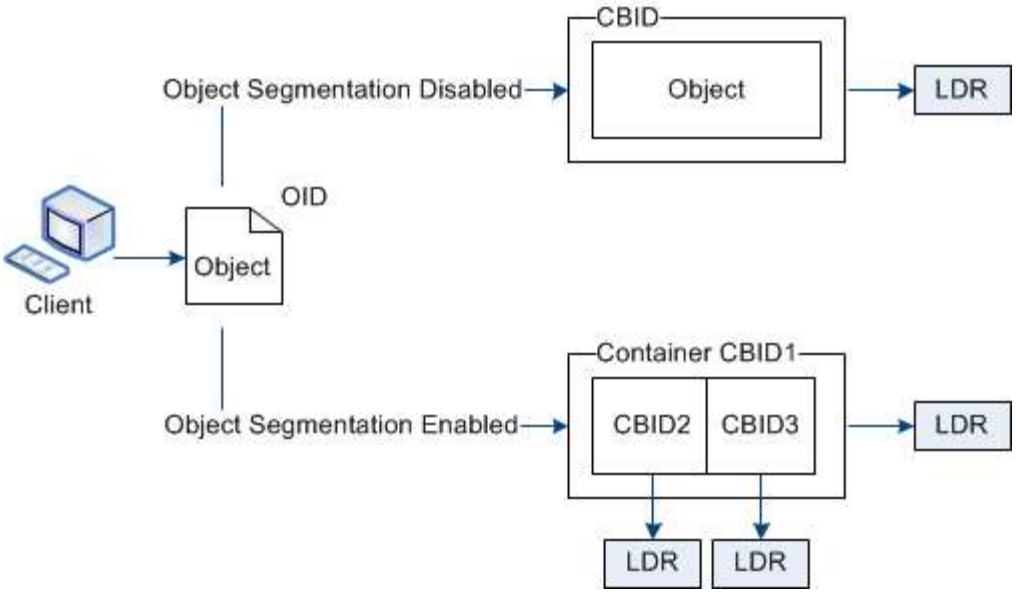
Para obtener información sobre las asignaciones de puertos, consulte "Resumen: Direcciones IP y puertos para conexiones cliente".



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.



Si el sistema StorageGRID incluye un nodo de archivado cuyo tipo de destino es la organización en niveles del cloud. Simple Storage Service y el sistema de almacenamiento de archivado dirigido es Amazon Web Services (AWS), el tamaño máximo de segmento debe ser menor o igual a 4.5 GIB (4,831,838,208 bytes). Este límite superior garantiza que no se supere la limitación DE PUT AWS de cinco GB. Las solicitudes a AWS que superen este valor fallarán.

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 se pueden almacenar en cualquier nodo de almacenamiento.

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

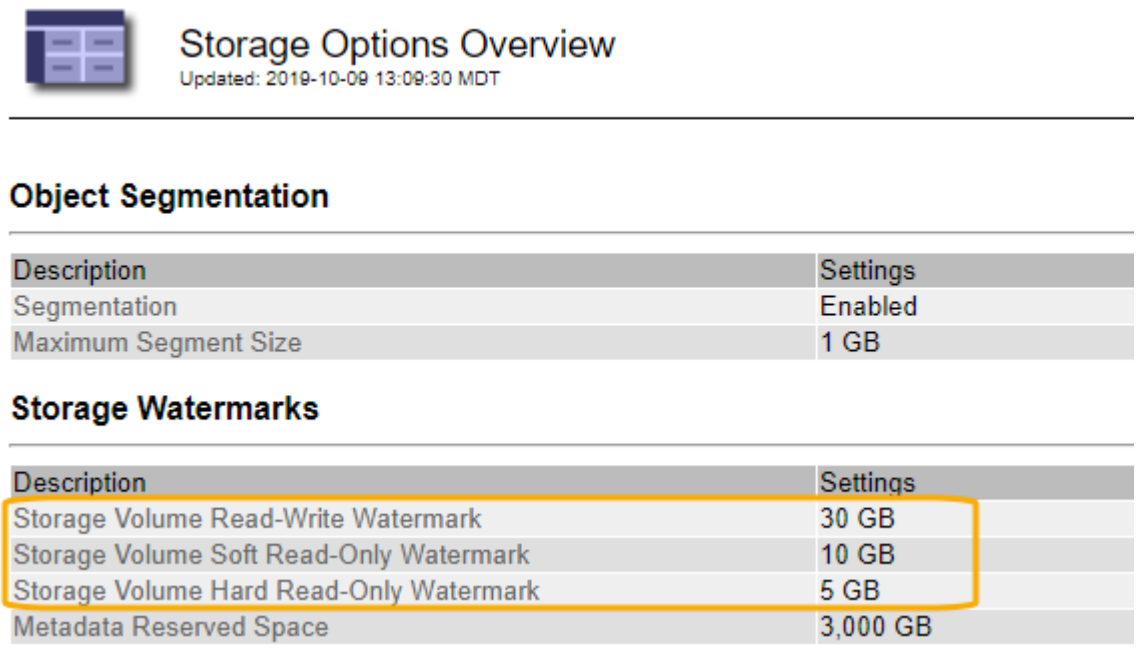
Puede mejorar el rendimiento al manejar objetos grandes asegurándose de que:

- 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 utiliza marcas de agua de volumen de almacenamiento para permitir supervisar la cantidad de espacio útil disponible en los nodos de almacenamiento. Si la cantidad de espacio disponible en un nodo es menor que la configuración de Marca de agua configurada, se activa la alarma Estado de almacenamiento (SSTS) para poder determinar si necesita agregar nodos de almacenamiento.

Para ver la configuración actual de las marcas de agua del volumen de almacenamiento, seleccione **Configuración** > **Opciones de almacenamiento** > **Descripción general**.



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

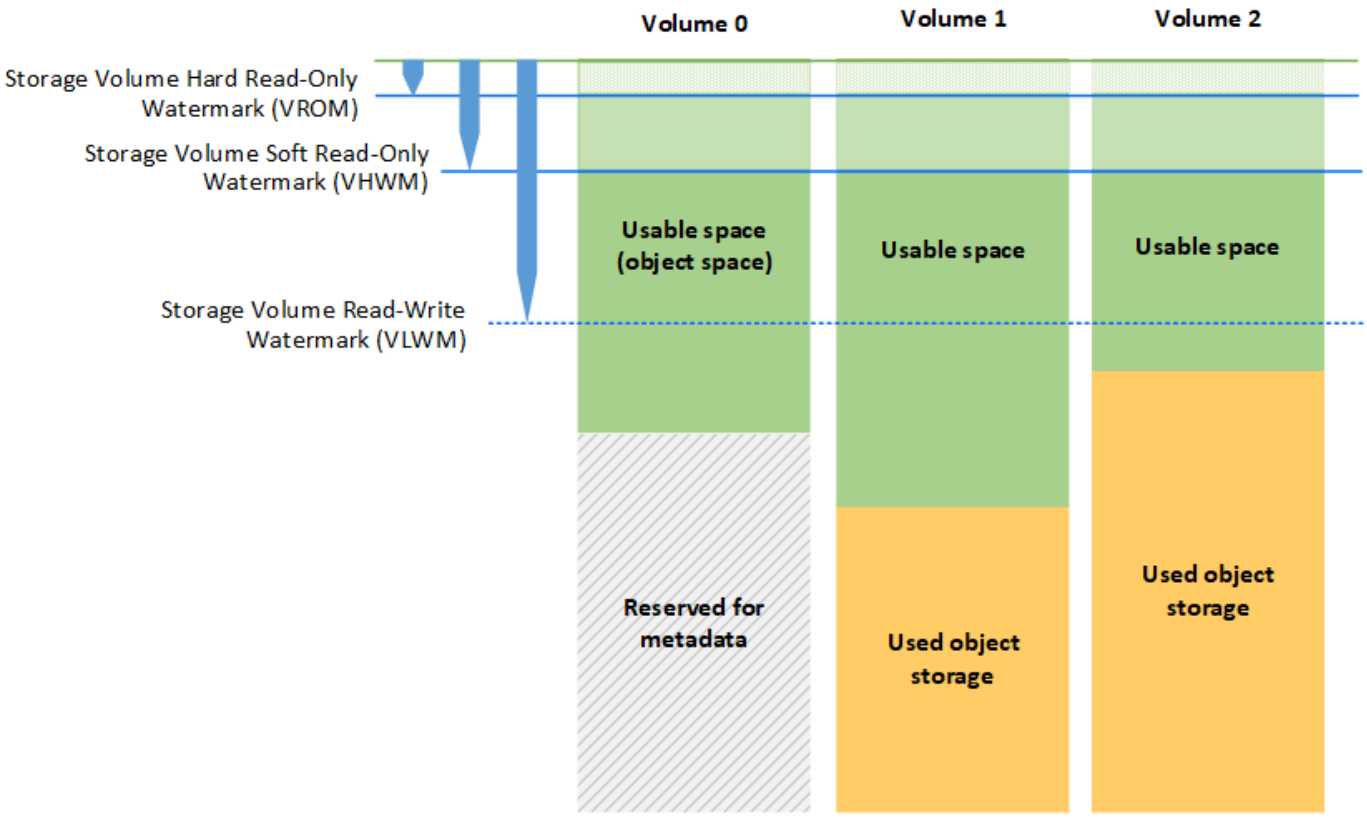
Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

La siguiente figura representa un nodo de almacenamiento con tres volúmenes y muestra la posición relativa de las tres marcas de agua de volumen de almacenamiento. En cada nodo de almacenamiento, StorageGRID reserva espacio en el volumen 0 para los metadatos de objetos; cualquier espacio restante en ese volumen se usa para los datos de objetos. Todos los demás volúmenes se utilizan exclusivamente para datos de objetos, lo que incluye copias replicadas y fragmentos codificados para borrado.



Las marcas de agua del volumen de almacenamiento son valores predeterminados en todo el sistema que indican la cantidad mínima de espacio libre requerida en cada volumen del nodo de almacenamiento para evitar que StorageGRID cambie el comportamiento de lectura/escritura del nodo o active una alarma. Tenga en cuenta que todos los volúmenes deben alcanzar la Marca de agua antes de que StorageGRID actúe. Si algunos volúmenes tienen más de la cantidad mínima requerida de espacio libre, la alarma no se activa y el comportamiento de lectura y escritura del nodo no cambia.

Marca de agua de sólo lectura suave del volumen de almacenamiento (VHWM)

La 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 para los datos de objeto se está llenando. Esta Marca de agua representa la cantidad de espacio libre que debe existir en cada volumen de un nodo de almacenamiento para evitar que el nodo entre en «el modo de sólo lectura». El modo de solo lectura suave significa que el nodo de almacenamiento anuncia servicios de solo lectura al resto del sistema StorageGRID, pero completa todas las solicitudes de escritura pendientes.

Si la cantidad de espacio libre en cada volumen es menor que el valor de esta Marca de agua, la alarma Estado de almacenamiento (SST) se activa en el nivel de aviso y el nodo de almacenamiento pasa al modo de sólo lectura suave.

Por ejemplo, supongamos que la Marca de agua de sólo lectura suave del volumen de almacenamiento se establece en 10 GB, que es su valor predeterminado. Si queda menos de 10 GB de espacio libre en cada volumen en el nodo de almacenamiento, la alarma SSTS se activa en el nivel de aviso y el nodo de almacenamiento pasa al modo de solo lectura suave.

Marca de agua de solo lectura (VROM) de volumen de almacenamiento

La Marca de agua de sólo lectura dura del 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. Esta Marca de agua representa la cantidad de espacio libre que debe existir en cada volumen de un nodo de almacenamiento para evitar que el nodo entre en el modo "'modo de sólo lectura'". El modo de solo lectura estricta significa que el nodo de almacenamiento es de solo lectura y ya no acepta solicitudes de escritura.

Si la cantidad de espacio libre en cada volumen de un nodo de almacenamiento es menor que la configuración de esta Marca de agua, la alarma Estado de almacenamiento (SST) se activa en el nivel principal y el nodo de almacenamiento pasa al modo de sólo lectura.

Por ejemplo, supongamos que la Marca de agua de sólo lectura del disco duro del volumen de almacenamiento está establecida en 5 GB, que es su valor predeterminado. Si queda menos de 5 GB de espacio libre en cada volumen de almacenamiento en el nodo de almacenamiento, la alarma DE SSTS se activa en el nivel principal y el nodo de almacenamiento pasa al modo de solo lectura fija.

El valor de la Marca de agua de sólo lectura rígida del volumen de almacenamiento debe ser menor que el valor de la Marca de agua de sólo lectura suave del volumen de almacenamiento.

Marca de agua de lectura y escritura de volumen de almacenamiento (VLWM)

La Marca de agua de lectura-escritura del volumen de almacenamiento solo se aplica a los nodos de almacenamiento que hayan cambiado al modo de solo lectura. Esta Marca de agua determina cuándo se permite que el nodo de almacenamiento vuelva a ser de lectura y escritura.

Por ejemplo, supongamos que un nodo de almacenamiento ha pasado al modo de solo lectura estricta. Si la Marca de agua de lectura y escritura del volumen de almacenamiento se establece en 30 GB (predeterminado), el espacio libre en cada volumen de almacenamiento del nodo de almacenamiento debe aumentar de 5 GB a 30 GB antes de que el nodo pueda volver a ser de lectura y escritura.

El valor de la Marca de agua de lectura y escritura de volumen de almacenamiento debe ser mayor que el valor de la Marca de agua de solo lectura suave de volumen de almacenamiento.

Información relacionada

"Gestión de nodos de almacenamiento completos"

Gestionar 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

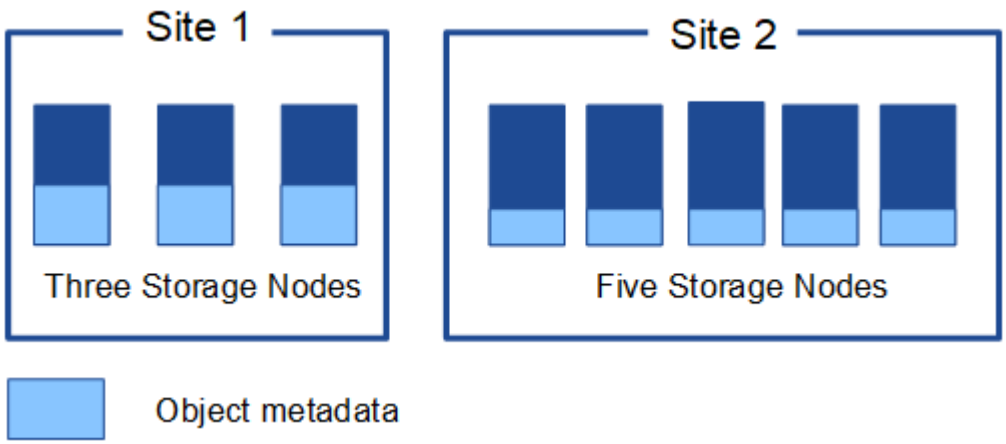
objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y hora en que se modificó por última vez el objeto.

- 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?

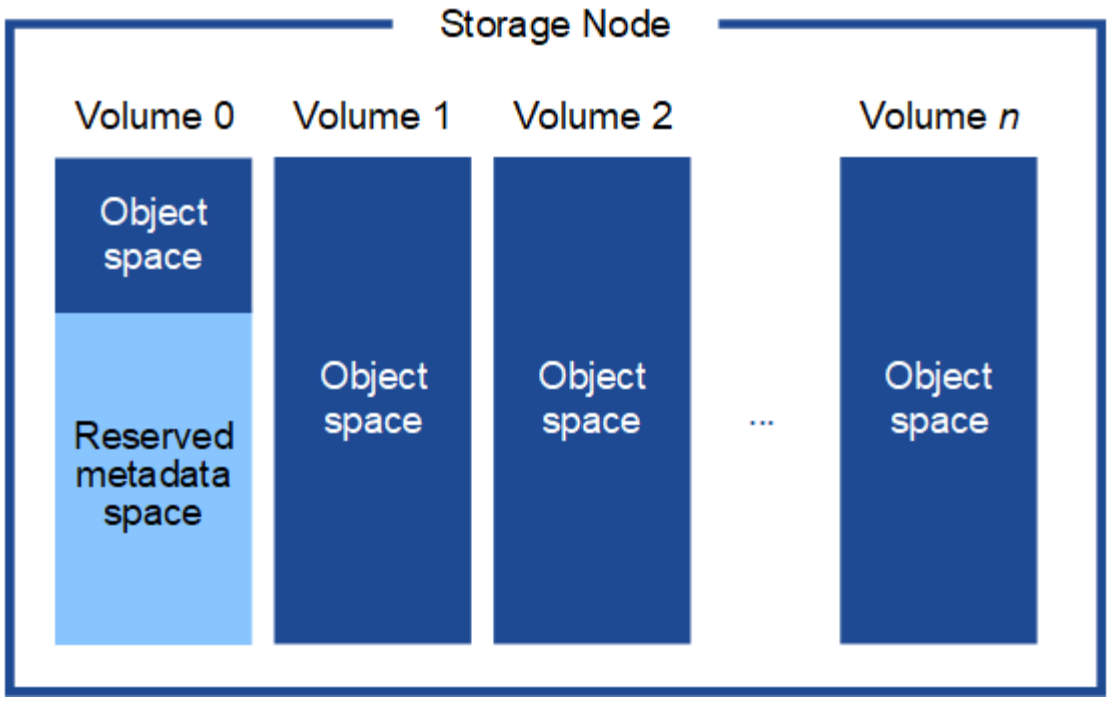
StorageGRID mantiene los metadatos de objetos en una base de datos de Cassandra, que se almacena independientemente de los datos de objetos. Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema 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 11.5 se basa en lo siguiente:

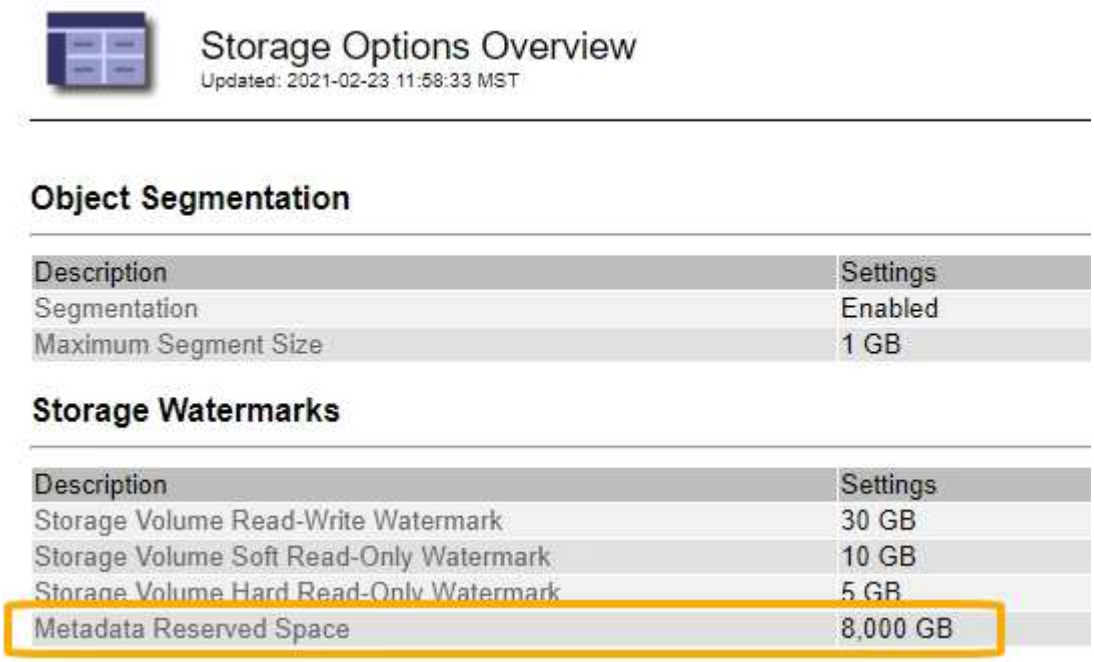
- La versión de software que estaba utilizando cuando instaló inicialmente StorageGRID.
- La cantidad de RAM en cada nodo de almacenamiento.

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 11.5
11.5	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)

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 11.5
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** > **Configuración del 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 11.5 en la que cada nodo de almacenamiento tiene 128 GB o más de RAM.

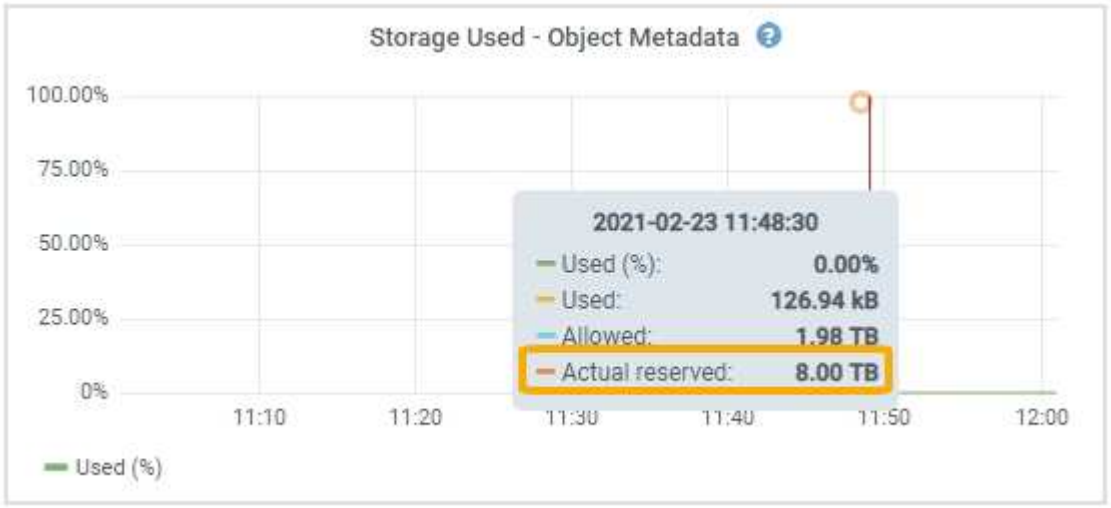
Espacio reservado real para los metadatos

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: • Volumen 0 • 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 11.5. 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.

El valor **Real reservado** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

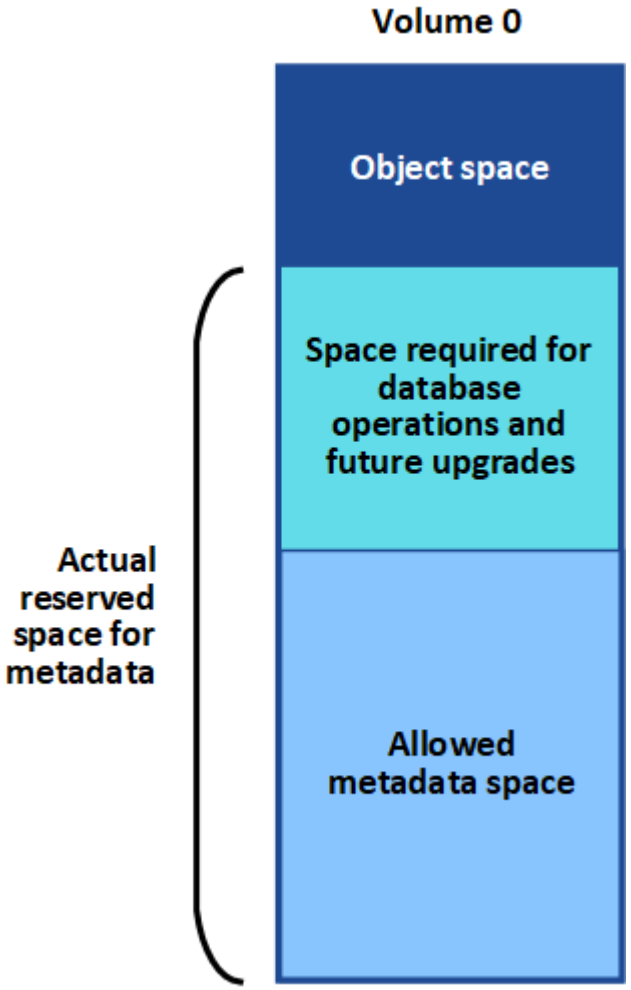
Ejemplo de espacio de metadatos reservado real

Suponga que instala un nuevo sistema StorageGRID mediante la versión 11.5. 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 11.5 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.



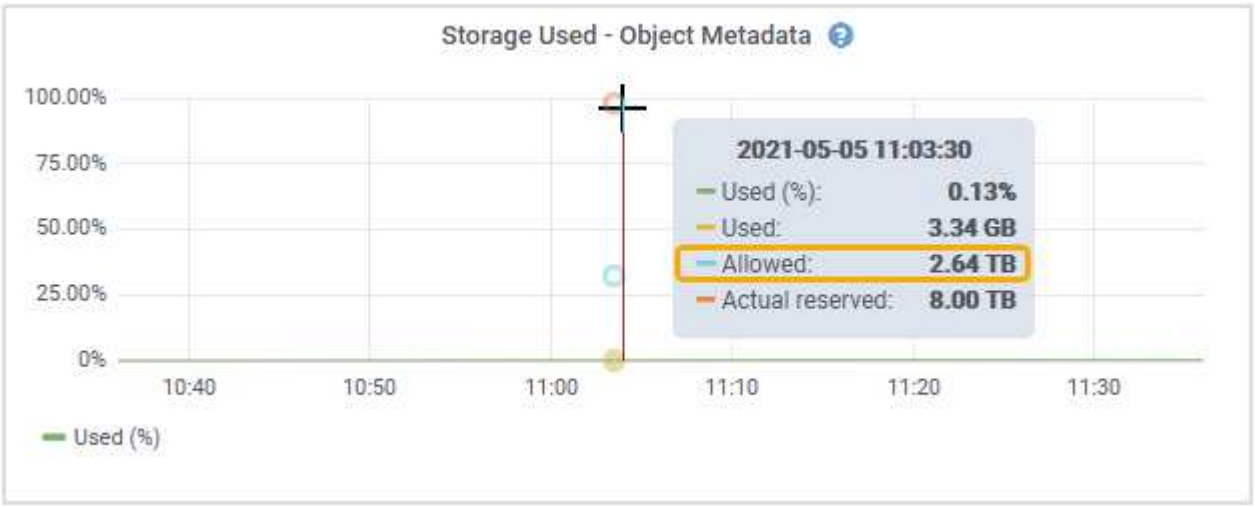
En la tabla siguiente se resume cómo StorageGRID determina el valor de espacio de metadatos permitido para un nodo de almacenamiento.

Espacio reservado real para los metadatos	Espacio de metadatos permitido
4 TB o menos	60 % del espacio reservado real para metadatos, hasta un máximo de 1.98 TB
Más de 4 TB	(Espacio reservado real para metadatos − 1 TB) × 60 %, hasta un máximo de 2.64 TB

En algunos casos, si el sistema de StorageGRID almacena (o se espera que almacene) más de 2.64 TB de metadatos en cualquier nodo de almacenamiento, se puede aumentar el espacio de metadatos permitido. Si cada uno de sus nodos de almacenamiento tiene más de 128 GB de RAM y espacio libre disponible en el volumen de almacenamiento 0, póngase en contacto con su representante de cuentas de NetApp. NetApp revisará sus requisitos y aumentará el espacio de metadatos permitido para cada nodo de almacenamiento, si es posible.

Para ver el espacio de metadatos permitido para un nodo de almacenamiento:

1. En Grid Manager, seleccione **Node** > ***Storage Node***.
2. Seleccione la ficha **almacenamiento**.
3. 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 2.64 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 11.5. 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 11.5 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 2.64 TB. (Este es el valor máximo del espacio

reservado real.)

Cómo afectan los nodos de almacenamiento de diferentes tamaños a la capacidad de objetos

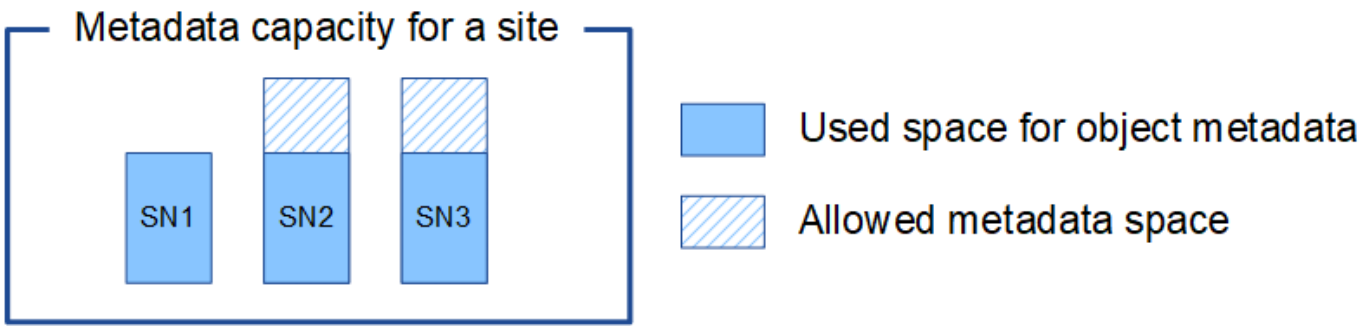
Como se ha descrito anteriormente, StorageGRID distribuye uniformemente los metadatos de objetos de los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

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 aprender a supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento:

  "Solución de problemas de monitor"

- Para aumentar la capacidad de metadatos de los objetos del sistema, debe añadir nodos de

almacenamiento nuevos:

"Amplíe su grid"

Configuración de la configuración global de los objetos almacenados

Puede utilizar Opciones de cuadrícula para configurar los valores de todos los objetos almacenados en el sistema StorageGRID, incluida la compresión de objetos almacenados, el cifrado de objetos almacenados. y hash de objetos almacenados.

- "Configurar la compresión de objetos almacenados"
- "Configurar el cifrado de objetos almacenados"
- "Configuración de hash de 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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:

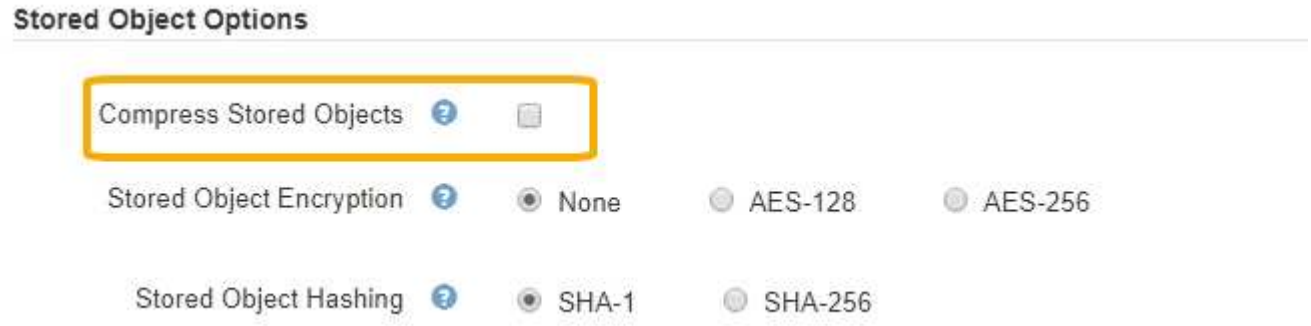
- No debe activar la compresión a menos que sepa que los datos almacenados son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimir objetos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, la activación de comprimir 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** > **Configuración del sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado , active la casilla de verificación **comprimir objetos almacenados** .



3. Haga clic en **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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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** > **Configuración del 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. Haga clic en **Guardar**.

Configuración de 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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** > **Configuración del 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. Haga clic en **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 **Soporte** > **Herramientas** > **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: • 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. • 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. • 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. 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. El atributo puede tomar uno de los siguientes valores: • Sin conexión: Cuando el estado deseado es sin conexión, el servicio LDR desconecta el componente **LDR** > **almacenamiento**. • 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. • 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 verificación en primer plano. El sistema StorageGRID restaura automáticamente los datos de objetos replicados que faltan.
Verificación	FVOV	Seleccione los almacenes de objetos en los que se realizará la verificación en primer plano.
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. 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.

Nombre de atributo	Codificación	Descripción
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.
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 verificación en primer plano.

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. 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.

Nombre de atributo	Codificación	Descripción
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. 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

"Solución de problemas de monitor"

Gestión de 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.

Adición de 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 ampliar un sistema StorageGRID.

Añadiendo bandejas de ampliación de 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 ampliar un sistema StorageGRID.

Añadir 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 ampliar un sistema StorageGRID.

Información relacionada

"Amplíe su grid"

Gestión de los nodos de administrador

Cada sitio de una implementación de StorageGRID puede tener uno o varios nodos de

administrador.

- "Qué es un nodo de administrador"
- "El uso de varios nodos de administrador"
- "Identificar el nodo de administrador principal"
- "Seleccionar un remitente preferido"
- "Ver el estado de notificación y las colas"
- "Cómo muestran los nodos de administración alarmas confirmadas (sistema heredado)"
- "Configuración del acceso de clientes de auditoría"

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.

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.

Información relacionada

"Uso de la API de gestión de grid"

"Usar una cuenta de inquilino"

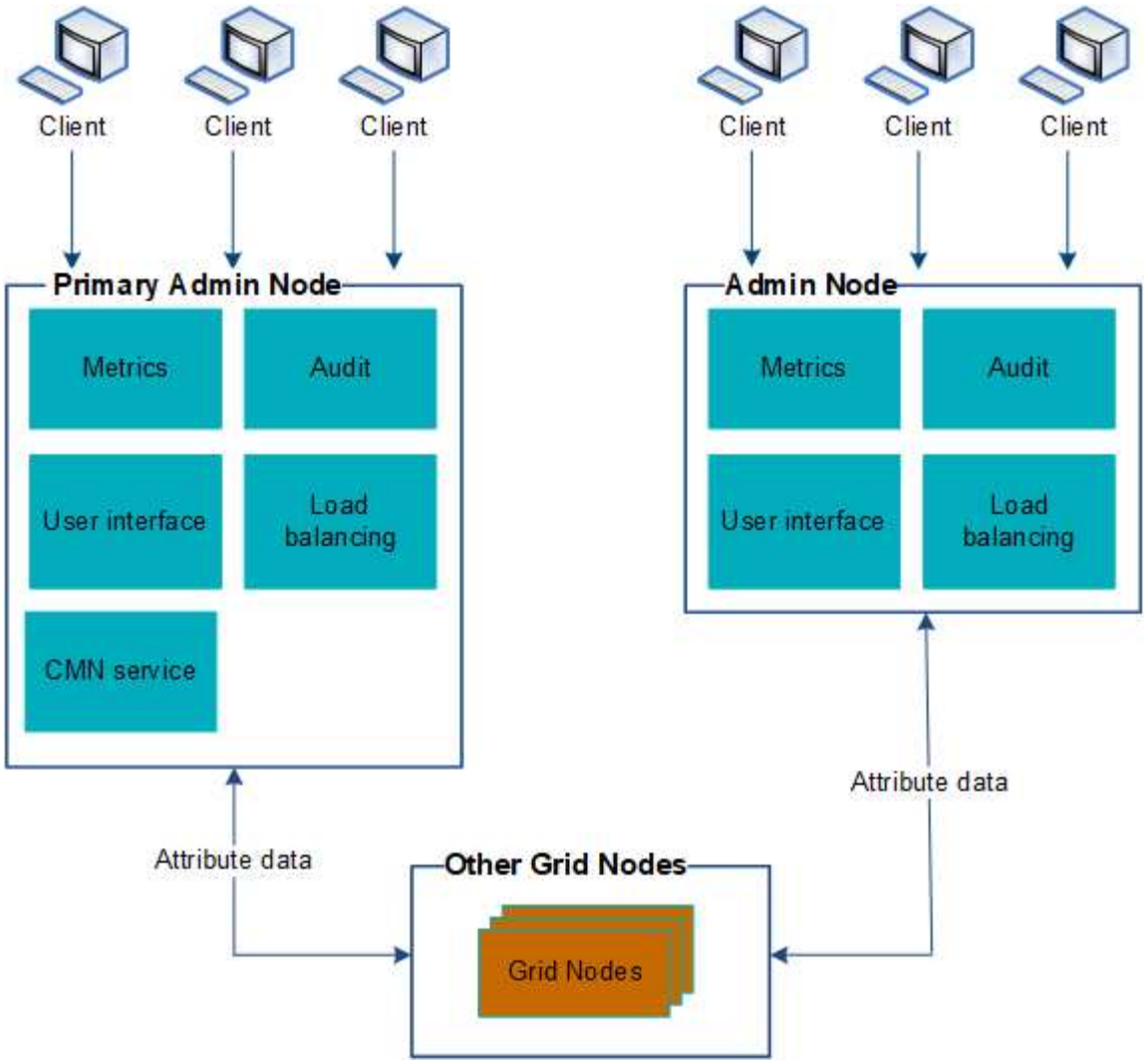
"Gestión del equilibrio de carga"

"Gestionar grupos de alta disponibilidad"

El uso de 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.

> 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.

Información relacionada

"Gestionar grupos de alta disponibilidad"

Identificar el nodo de administrador 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

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

Pasos

1. Seleccione **Soporte** > **Herramientas** > **Topología de cuadrícula**.
2. Seleccione ***site*** > **Admin Node** y, a continuación, haga clic en ➕ 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.

Seleccionar 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

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

Acerca de esta tarea

La página **Configuración** > **Configuración del sistema** > **Opciones de pantalla** 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:

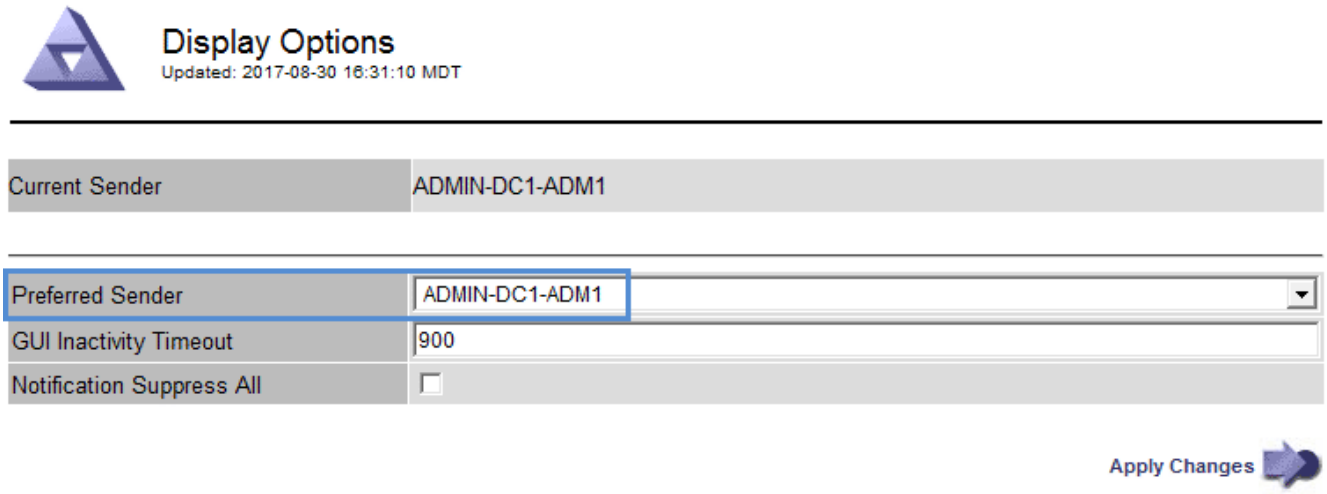
- Si los nodos de administración se convierten en "'desembarcados'" entre sí, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones, y pueden recibirse varias copias de las notificaciones.

- 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** > **Configuración del 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.



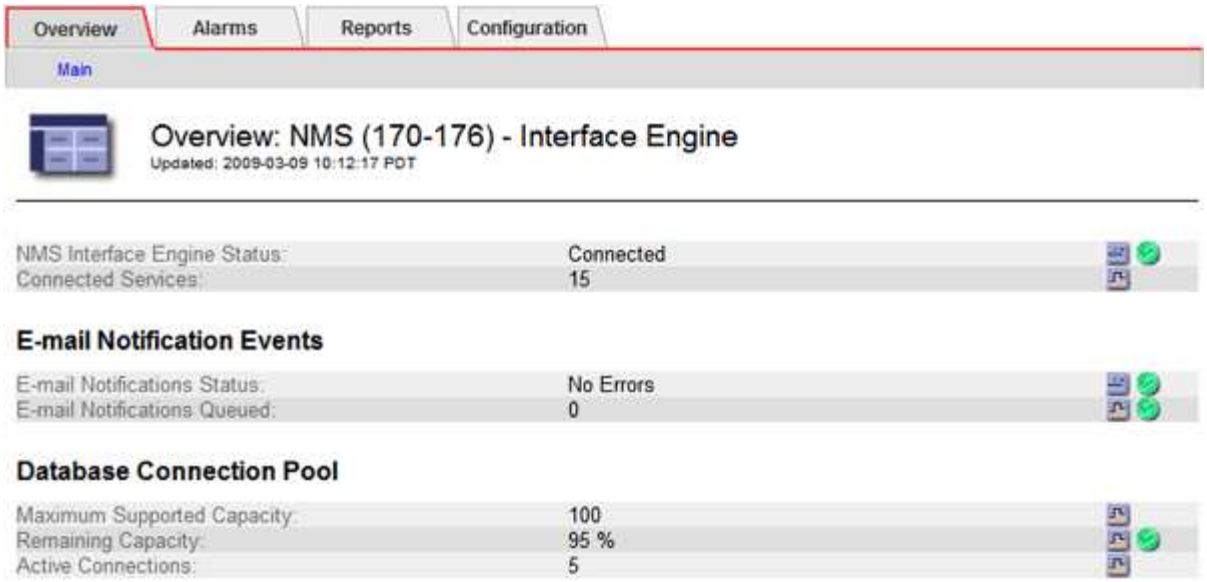
4. Haga clic en **aplicar cambios**.

   El nodo de administrador se establece como el remitente preferido de notificaciones.

Ver el estado de notificación y las colas

El servicio NMS de los nodos Admin 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 Interface Engine, seleccione **Support** > **Tools** > **Grid Topology**. Por último, seleccione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.

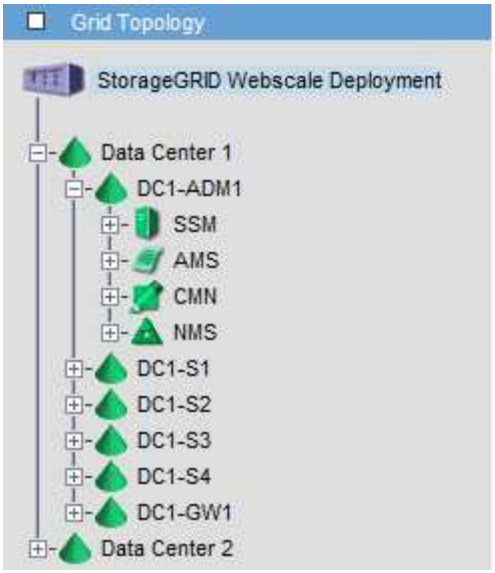


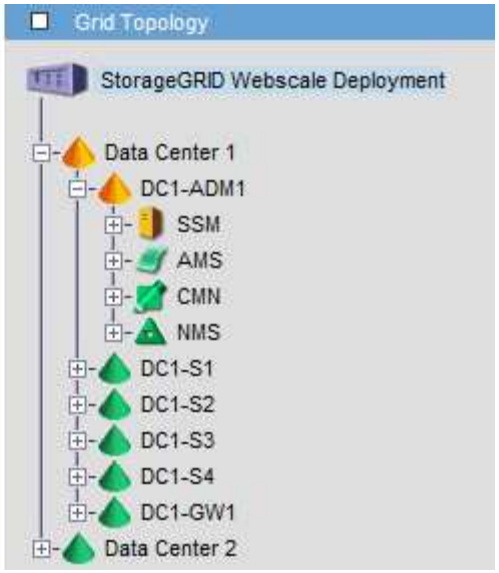
Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la 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.

Configuración del acceso de 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 las instrucciones para comprender los mensajes de auditoría.

Si dispone de la opción de utilizar CIFS o NFS, elija NFS.

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Información relacionada

"Qué es un nodo de administrador"

"Revisar los registros de auditoría"

"Actualizar el software de"

Configuración de 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.

Información relacionada

"Actualizar el software de"

Configuración de 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

- Debe tener la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Debe tener 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`

Información relacionada

"Actualizar el software de"

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

- Debe tener la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Debe tener el nombre de usuario y la contraseña de CIFS Active Directory.
- Debe tener 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`

Información relacionada

"Actualizar el software de"

Adición de 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

- Debe tener la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Debe tener 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`

Eliminar 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

- Debe tener la `Passwords.txt` Archivo con las contraseñas de la cuenta raíz (disponible en DICHO paquete).

- Debe tener 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`

Información relacionada

"Actualizar el software de"

Cambiar un nombre de usuario o de grupo de recursos compartidos de auditoría de 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

"Actualizar el software de"

"Adición de un usuario o un grupo a un recurso compartido de auditoría CIFS"

"Eliminar un usuario o un grupo de un recurso compartido de auditoría CIFS"

Verificación de la integración de la auditoría 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.

Configuración del cliente de auditoría para NFS

El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

Lo que necesitará

- Debe tener la `Passwords.txt` Archivo con la contraseña root/admin (disponible en DICHO paquete).
- Debe tener la `Configuration.txt` Archivo (disponible en DICHO paquete).
- El cliente de auditoría debe utilizar 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.

Adición de 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

- Debe tener la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Debe tener la `Configuration.txt` Archivo (disponible en DICHO paquete).
- El cliente de auditoría debe utilizar 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`

Verificación de la integración de la 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.

Eliminación de 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

- Debe tener la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Debe tener 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 NFS

1. Agregue una nueva dirección IP a un recurso compartido de auditoría NFS existente.
2. Elimine la dirección IP original.

Información relacionada

"Adición de un cliente de auditoría NFS a un recurso compartido de auditoría"

"Eliminación de un cliente de auditoría NFS del recurso compartido de auditoría"

Gestión de los nodos de archivado

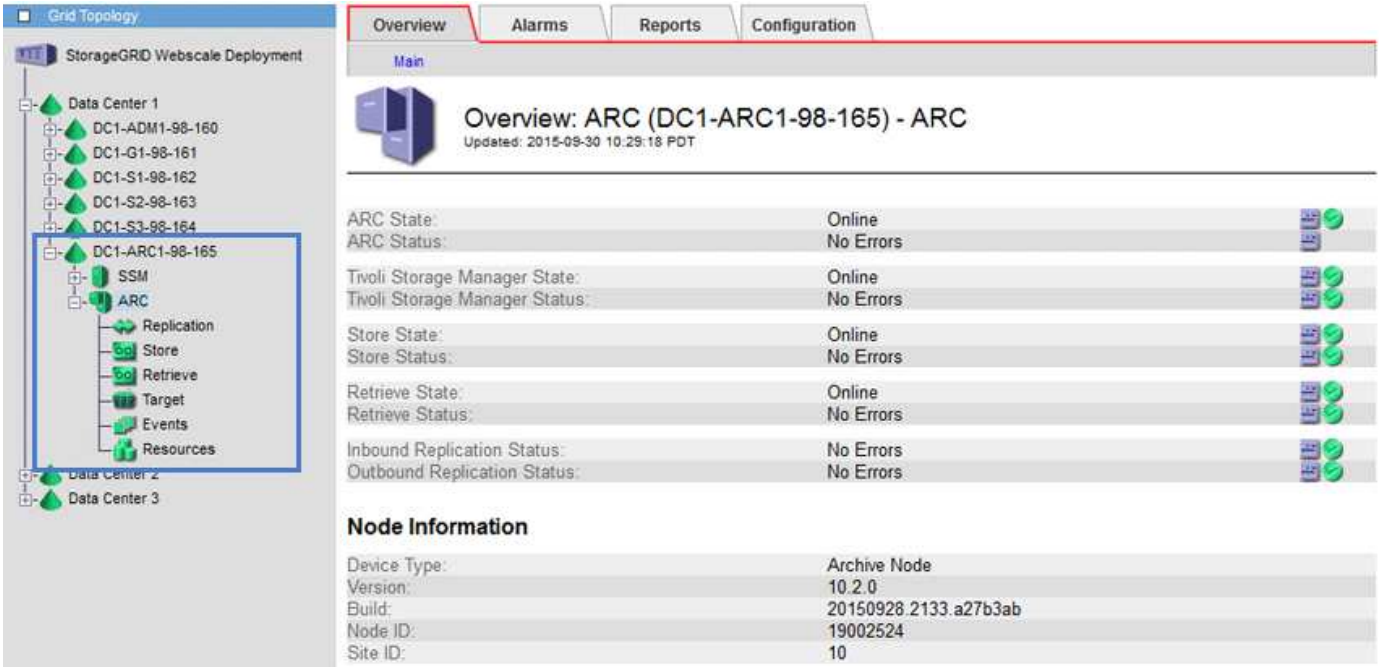
Opcionalmente, cada una de las ubicaciones de los centros de datos del sistema StorageGRID se puede implementar con un nodo de archivado, que permite conectarse a un sistema de almacenamiento de archivado externo específico, como Tivoli Storage Manager (TSM).

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.

- "Qué es un nodo de archivado"
- "Configurar las conexiones del nodo de archivado con el almacenamiento de archivado"
- "Establecer alarmas personalizadas para el nodo de archivado"
- "Integración de Tivoli Storage Manager"

Qué es un nodo de archivado

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.



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 del nodo de archivado (ARC) proporciona 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.

Configurar las conexiones del nodo de archivado con el almacenamiento de archivado

Al configurar un nodo de archivado para conectarse con un archivo externo, debe seleccionar el tipo de destino.

El sistema StorageGRID es compatible con el archivado de datos de objetos en el cloud a través de una interfaz S3 o a cinta mediante el middleware Tivoli Storage Manager (TSM).

> Una vez configurado el tipo de destino de archivado para un nodo de archivado, el tipo de destino no se puede cambiar.

- "Archivado en el cloud mediante la API de S3"
- "Archivar en cinta a través de TSM middleware"
- "Configurar los ajustes de recuperación del nodo de archivado"
- "Configurar la replicación de nodos de archivado"

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 gestionar objetos con gestión del ciclo de vida de la información.

Información relacionada

"Gestión de objetos con ILM"

Configurar 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.

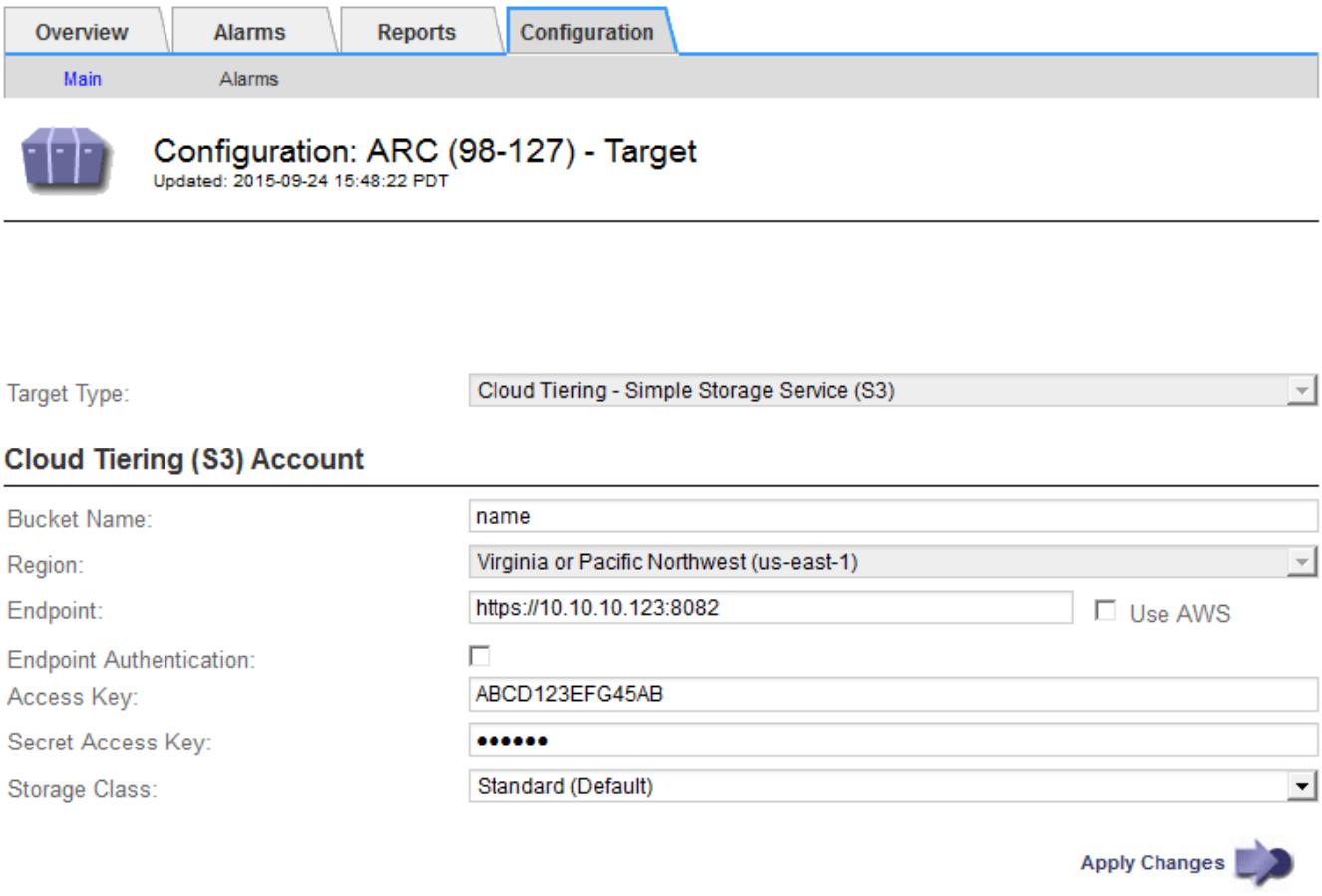
> El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades. La opción **Cloud Tiering - simple Storage Service (S3)** sigue siendo compatible, 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 las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe haber creado un bloque en el sistema de almacenamiento de archivado de destino:
  - El bloque debe estar dedicado a un único nodo de archivado. No puede utilizarlo otros nodos de archivado ni otras aplicaciones.
  - El cucharón debe tener la región adecuada seleccionada para su ubicación.
  - El bloque debe configurarse con el control de versiones suspendido.
- La segmentación de objetos debe estar activada y el tamaño máximo de segmento debe ser inferior 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 **Soporte** > **Herramientas** > **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. Haga clic en **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.

Información relacionada

"Gestión de objetos con ILM"

Modificación de 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

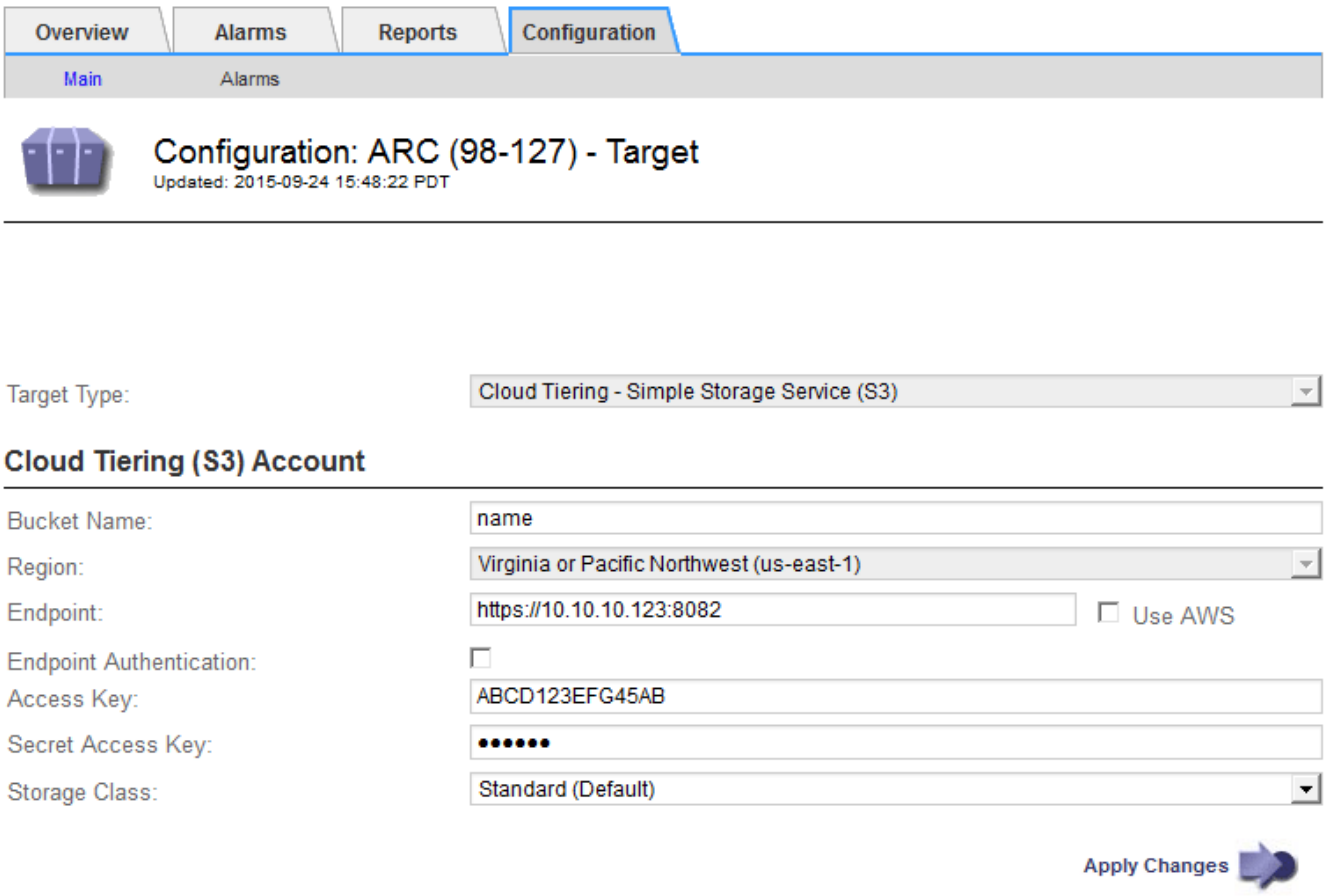
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

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 **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Modificación del 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

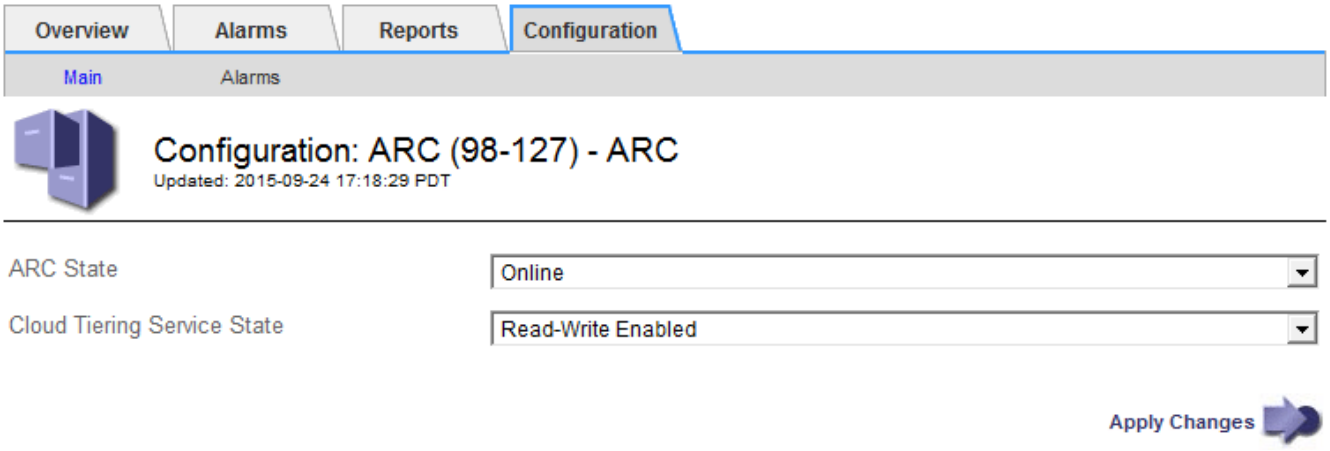
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe configurarse el nodo de archivado.

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 **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Restablecer el número de errores de almacén para la conexión API de S3

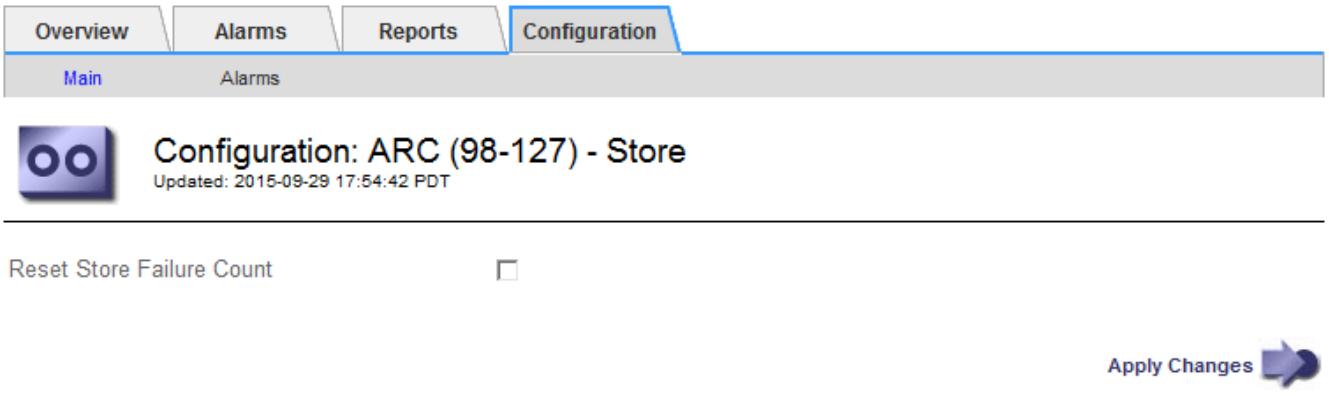
Si el nodo de archivado se conecta a un sistema de almacenamiento de archivado a través de la API de S3, puede restablecer el recuento de fallos de almacenamiento, que se puede utilizar para borrar la alarma de ARVF (fallos de almacenamiento).

Lo que necesitará

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

Pasos

1. Seleccione **Soporte** > **Herramientas** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione **Restablecer recuento de fallos de tienda**.

5. Haga clic en **aplicar cambios**.

   El atributo fallos de almacén se restablece a cero.

Migrar objetos de 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

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener 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).

Configuración de conexiones con TSM middleware

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

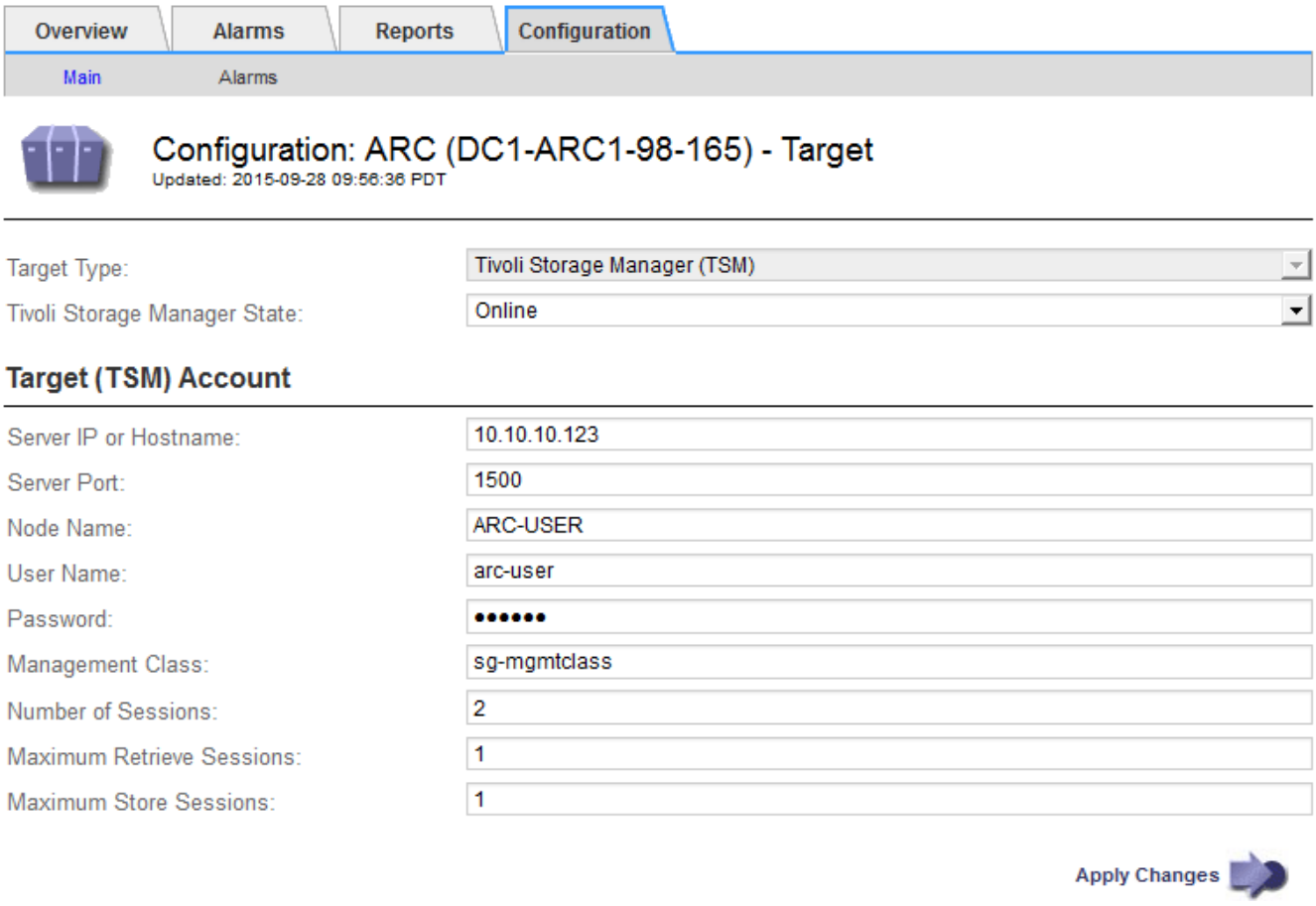
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

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 **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Optimización de 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

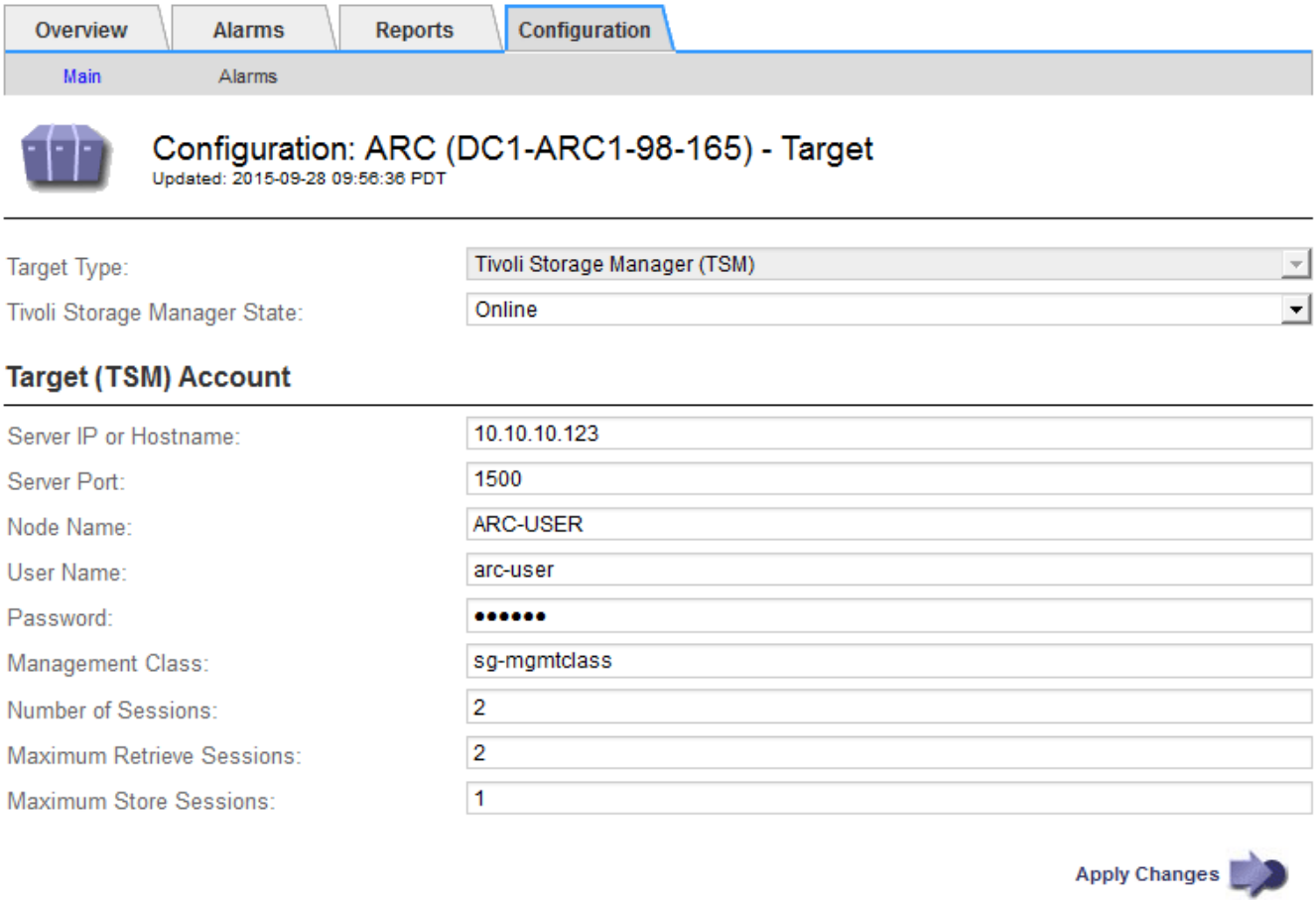
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

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 **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Configuración del 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.

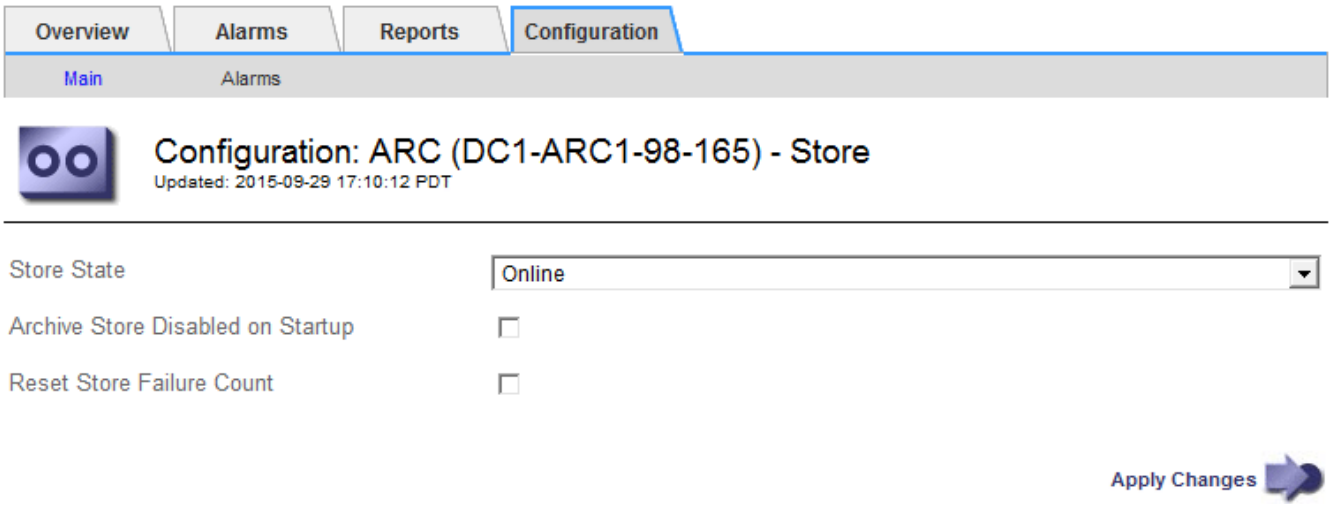
Lo que necesitará

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

Pasos

1. Seleccione **Soporte** > **Herramientas** > **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 objetivo el sistema de almacenamiento de archivado 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. Haga clic en **aplicar cambios**.

Información relacionada

"Gestión de un nodo de archivado cuando el servidor TSM alcanza la capacidad"

Gestión de un nodo de archivado cuando el servidor TSM alcanza 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. 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. Esta situación se puede evitar gracias a la supervisión proactiva del servidor TSM.

Lo que necesitará

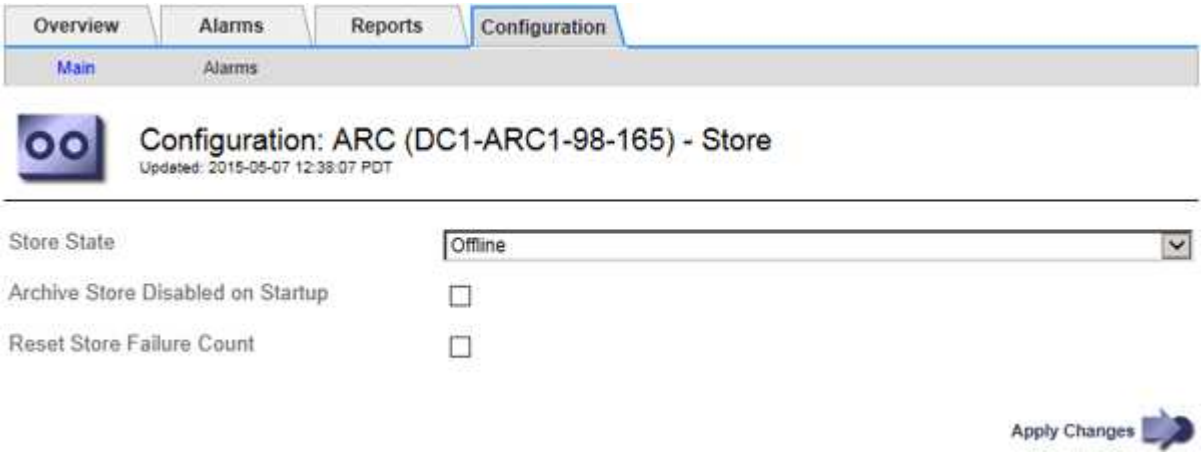
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

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 **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Configurar el nodo de archivado como de sólo 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.

Lo que necesitará

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

Pasos

1. Seleccione **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Configurar los ajustes de recuperación del nodo de archivado

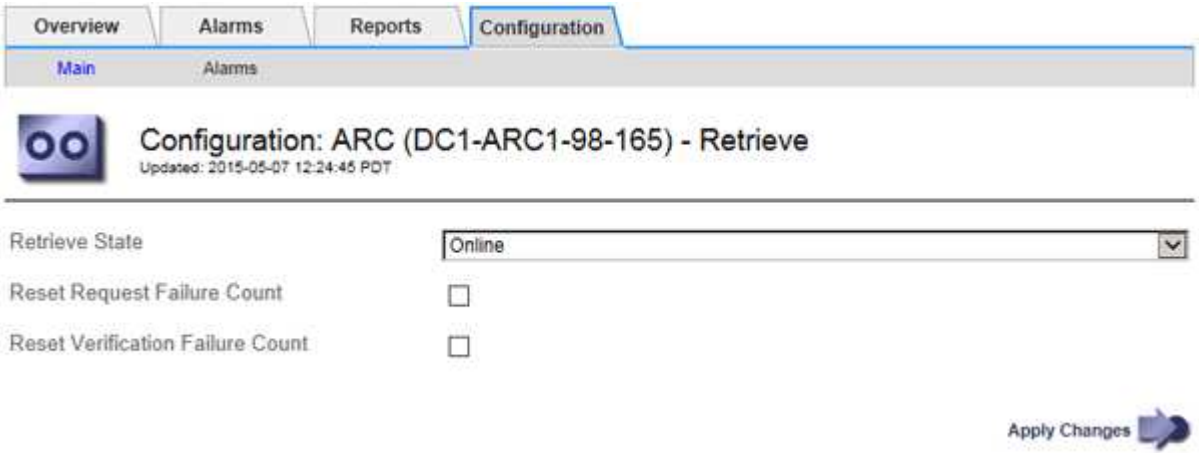
Puede configurar los ajustes de recuperación de un nodo de archivado para establecer el estado en línea o sin conexión, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Lo que necesitará

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

Pasos

1. Seleccione **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Configurar la replicación de nodos de archivado

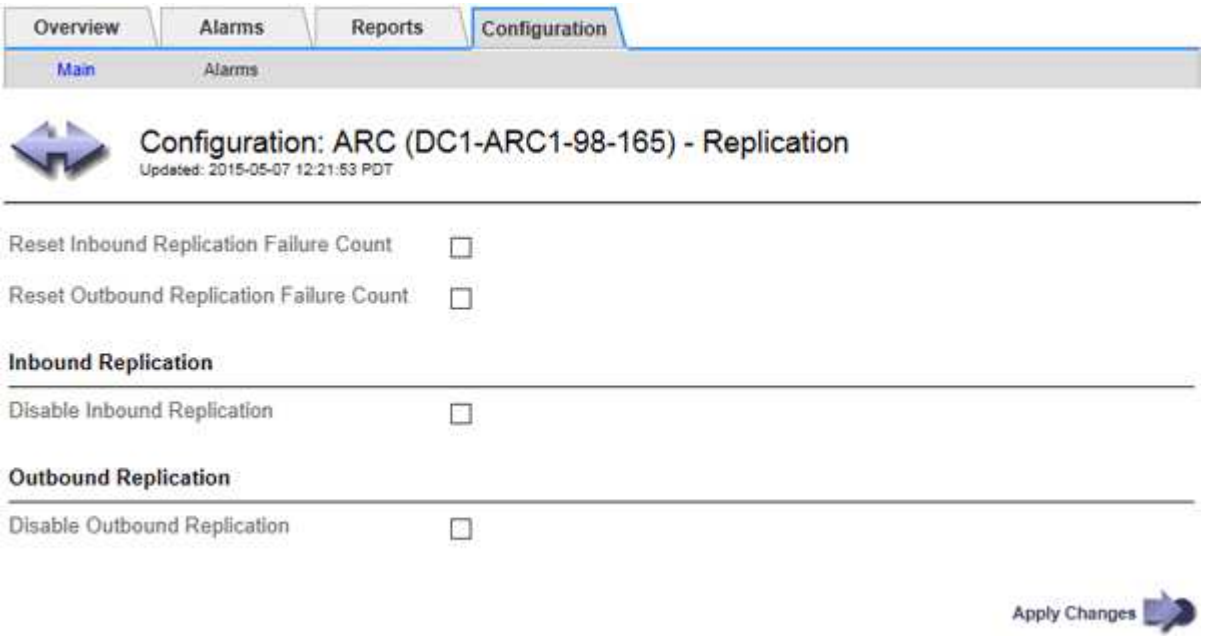
Puede configurar la configuración de replicación para un nodo de archivado y desactivar la replicación entrante y saliente, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Lo que necesitará

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

Pasos

1. Seleccione **Soporte** > **Herramientas** > **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. Haga clic en **aplicar cambios**.

Establecer 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.

Información relacionada

"Solución de problemas de monitor"

Integración de Tivoli Storage Manager

En esta sección se incluyen las prácticas recomendadas y la información de configuración para integrar un nodo de archivado con un servidor Tivoli Storage Manager (TSM), incluidos los detalles operativos del nodo de archivado que afectan a la configuración del servidor TSM.

- "Configuración y funcionamiento del nodo de archivado"
- "Prácticas recomendadas de configuración"
- "Completar la configuración del nodo de archivado"

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.

Completar 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.

Para obtener más información sobre cómo optimizar la recuperación de TSM y las sesiones de almacenamiento, consulte la información sobre cómo gestionar el almacenamiento de archivos.

- "Gestión de los nodos de archivado"

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"

Instalación de 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.

Configuración del 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.

Definición de 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).

Definir una directiva de dominio y registrar 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.

Migración de 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.

- "Confirmación de la capacidad del sistema StorageGRID"
- "Determinación de la política de ILM para los datos migrados"
- "Impacto de la migración en las operaciones"
- "Programación de la migración de datos"
- "Supervisar la migración de datos"
- "Creación de notificaciones personalizadas para las alarmas de migración"

Confirmación de 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 de disco del sistema StorageGRID, consulte las instrucciones de supervisión y resolución de problemas de StorageGRID.

Información relacionada

"Solución de problemas de monitor"

"Gestión de nodos de almacenamiento"

Determinación de 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.

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.

Información relacionada

"Gestión de objetos con ILM"

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.

Programación de 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.

Información relacionada

"Supervisar la migración de datos"

Supervisar la migración de datos

La migración de datos debe supervisarse y ajustarse según sea necesario para garantizar que los datos se ubican según la política de ILM dentro del plazo adecuado.

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 **Soporte** > **Herramientas** > **Topología de cuadrícula**. 2. Seleccione ***deployment*** > **Descripción general** > **Principal**. 3. En la sección ILM Activity, supervise el número de objetos que se muestran para los siguientes atributos: ◦ **Esperando - todos (XQUZ)**: El número total de objetos que esperan la evaluación de ILM. ◦ **Esperando - Cliente (XCQZ)**: El número total de objetos que esperan la evaluación de ILM de las operaciones cliente (por ejemplo, ingesta). 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.

Creación de notificaciones personalizadas para las alarmas de migración

Se recomienda que StorageGRID envíe notificaciones de alerta o de alarma (sistema heredado) al administrador del sistema responsable de supervisar la migración si ciertos valores superan los umbrales recomendados.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe haber configurado la configuración de correo electrónico para notificaciones de alertas (o alarma).

Pasos

1. Cree una regla de alerta personalizada o una alarma global personalizada para cada métrica Prometheus o atributo StorageGRID que desee supervisar durante la migración de datos.

   Las alertas se activan en función de los valores de métricas Prometheus. Las alarmas se activan en función de los valores de los atributos. Consulte las instrucciones para supervisar y solucionar problemas de StorageGRID para obtener más información.

2. Desactive la regla de alerta personalizada o la alarma Global Custom una vez completada la migración de datos.

Tenga en cuenta que las alarmas personalizadas globales anulan las alarmas predeterminadas.

Información relacionada

"Solución de problemas de monitor"