Configurar y gestionar

StorageGRID

NetApp
November 05, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-117/admin/index.html on November 05, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configurar y gestionar . . . 1
- Administre StorageGRID . . . 1
  - Administrar StorageGRID: Descripción general . . . 1
  - Comience a usar Grid Manager . . . 1
  - Control del acceso a StorageGRID . . . 33
  - Usar federación de grid . . . 79
  - Gestionar la seguridad . . . 116
  - Gestione inquilinos . . . 190
  - Configurar conexiones de cliente . . . 210
  - Administrar redes y conexiones . . . 251
  - Utilice AutoSupport . . . 268
  - Gestione nodos de almacenamiento . . . 283
  - Gestione los nodos de administrador . . . 307
  - Gestione los nodos de archivado . . . 318
  - Migrar datos a StorageGRID . . . 341
- Gestión de objetos con ILM . . . 343
  - Gestión de objetos con ILM: Información general . . . 343
  - ILM y ciclo de vida de los objetos . . . 344
  - Crear y asignar grados de almacenamiento . . . 366
  - Usar pools de almacenamiento . . . 368
  - Utilice Cloud Storage Pools . . . 377
  - Gestione los perfiles de código de borrado . . . 399
  - Configurar regiones (opcional solo S3) . . . 403
  - Cree la regla de ILM . . . 405
  - Cree una política de ILM . . . 422
  - Funciona con políticas de ILM y reglas de ILM . . . 437
  - Utilice el bloqueo de objetos de S3 . . . 441
  - Ejemplo de reglas y políticas de ILM . . . 450
- Endurecimiento del sistema . . . 470
  - Refuerzo del sistema: Descripción general . . . 470
  - Directrices de refuerzo para las actualizaciones de software . . . 470
  - Directrices de refuerzo para redes de StorageGRID . . . 471
  - Directrices de refuerzo para nodos de StorageGRID . . . 472
  - Directrices de refuerzo para TLS y SSH . . . 475
  - Otras directrices de endurecimiento . . . 476
- Configure StorageGRID para FabricPool . . . 477
  - Configure StorageGRID para FabricPool: Información general . . . 478
  - Información necesaria para adjuntar StorageGRID como nivel de cloud . . . 479
  - Use el asistente de configuración de FabricPool . . . 481
  - Configure StorageGRID manualmente . . . 495
  - Configure System Manager de ONTAP . . . 505
  - Configure el servidor DNS . . . 507
  - Prácticas recomendadas de StorageGRID para FabricPool . . . 507

Eliminar datos de FabricPool de StorageGRID 512

Configurar y gestionar

Administre StorageGRID

Administrar StorageGRID: Descripción general

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

Acerca de estas instrucciones

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

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

Antes de empezar

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

Comience a usar Grid Manager

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	107
Microsoft Edge	107
Mozilla Firefox	106

Debe establecer la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Inicie sesión en Grid Manager

Para acceder a la página de inicio de sesión de Grid Manager, introduzca el nombre de

dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de direcciones de un explorador web compatible.

Descripción general

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 administradores 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.

Conéctese a un grupo de alta disponibilidad

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

Utilice SSO

Los pasos de inicio de sesión son ligeramente diferentes si "Se ha configurado el inicio de sesión único (SSO)".

Inicie sesión en Grid Manager en el primer nodo de administración

Antes de empezar

- Tiene sus credenciales de inicio de sesión.
- Está utilizando un "navegador web compatible".
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene al menos un permiso.
- Tiene la dirección URL de Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  Puede usar el nombre de dominio completo, la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración.

  Para acceder a Grid Manager en un puerto que no sea el puerto predeterminado para HTTPS (443), incluya el número de puerto en la dirección URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO no está disponible en el puerto restringido de Grid Manager. Se debe usar el puerto 443.

Pasos

1. Inicie un explorador web compatible.
2. En la barra de direcciones del navegador, introduzca la dirección URL de Grid Manager.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador. Consulte "Gestionar certificados de seguridad".
4. Inicie sesión en Grid Manager.

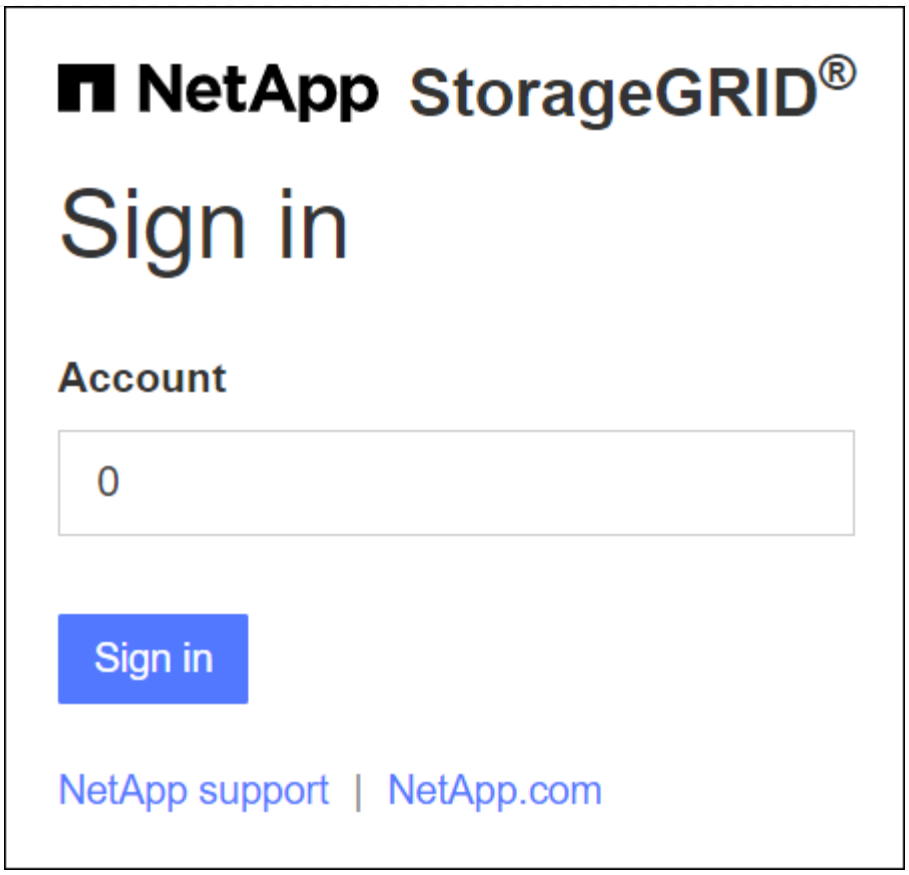
   La pantalla de inicio de sesión que aparece depende de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No se utiliza SSO

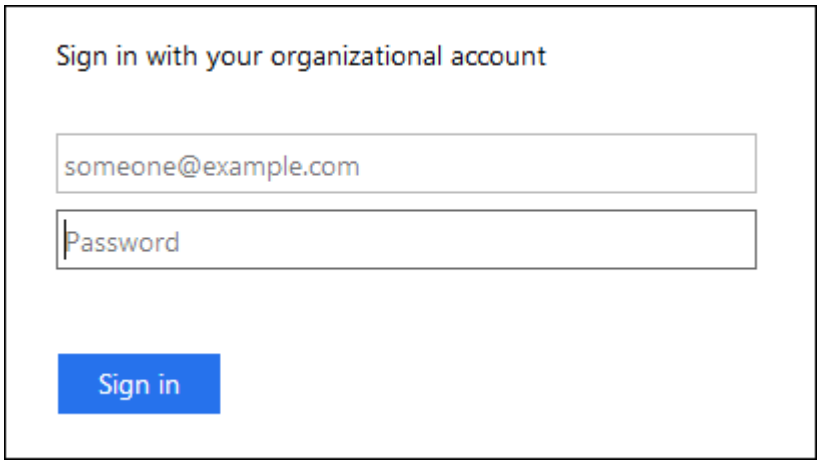
a. Introduzca su nombre de usuario y contraseña para el administrador de grid.
b. Seleccione **Iniciar sesión**.

Uso de SSO

- Si StorageGRID utiliza SSO y esta es la primera vez que accede a la URL en este explorador:
  i. Seleccione **Iniciar sesión**. Puede dejar el 0 en el campo Cuenta.



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



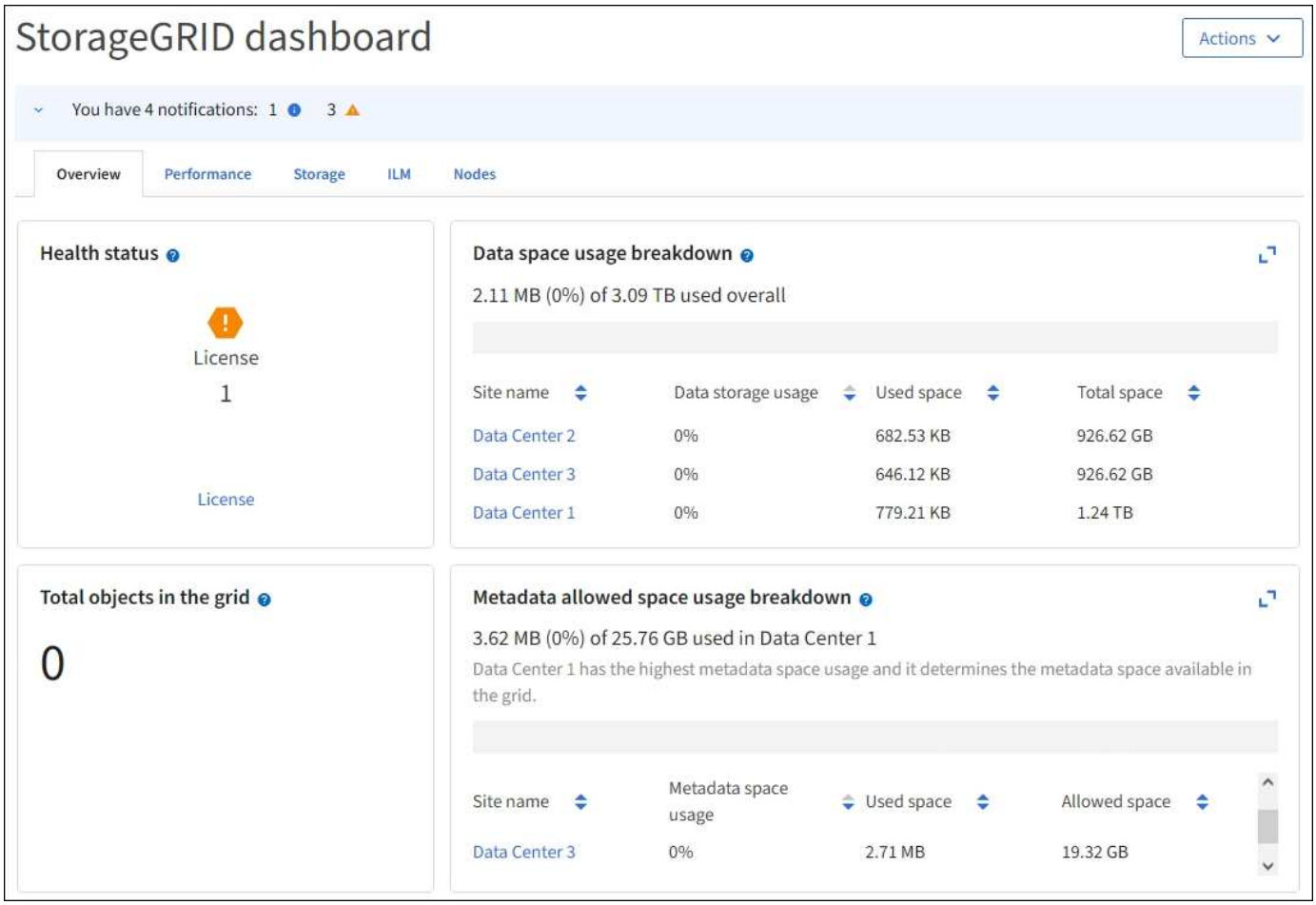
- Si StorageGRID utiliza SSO y se ha accedido previamente a Grid Manager o a una cuenta de inquilino:

  i. Introduzca **0** (el ID de cuenta de Grid Manager) o seleccione **Grid Manager** si aparece en la lista de cuentas recientes.

ii. Seleccione **Iniciar sesión**.

iii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Al iniciar sesión, aparece la página inicial de Grid Manager, que incluye el panel de control. Para saber qué información se proporciona, consulte "Permite ver y gestionar el panel de control".



Conéctese a otro nodo de administración

Siga estos pasos para iniciar sesión en otro nodo de administración.

No se utiliza SSO

Pasos

1. 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.
2. Introduzca su nombre de usuario y contraseña para el administrador de grid.
3. Seleccione **Iniciar sesión**.

Uso de SSO

Si StorageGRID está utilizando SSO y ha iniciado sesión en un nodo de administración, puede acceder a otros nodos de administración sin tener que volver a iniciar sesión.

Pasos

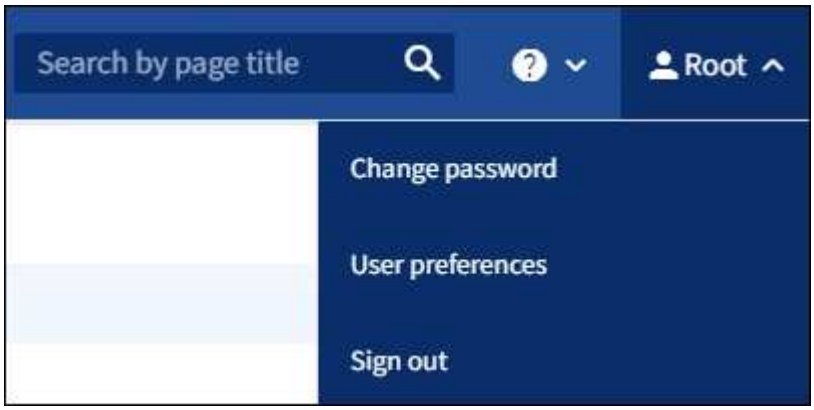
1. Introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si su sesión de SSO ha caducado, vuelva a introducir sus credenciales.

Cierre la sesión en Grid Manager

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

Pasos

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



2. Selecciona **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.
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 habilitado y usted también ha iniciado sesión en el Gestor de Inquilinos, también debe hacerlo "cierre la sesión de la cuenta de inquilino" para "Cierre la sesión de SSO".

Cambie la contraseña

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

Antes de empezar

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

Acerca de esta tarea

Si inicia sesión en StorageGRID como usuario federado o si está habilitado el inicio de sesión único (SSO), no

podrá cambiar la contraseña en Grid Manager. En su lugar, debe cambiar la contraseña en el origen de identidad externo, por ejemplo, Active Directory u OpenLDAP.

Pasos

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

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

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

Consulte la información de licencia de StorageGRID

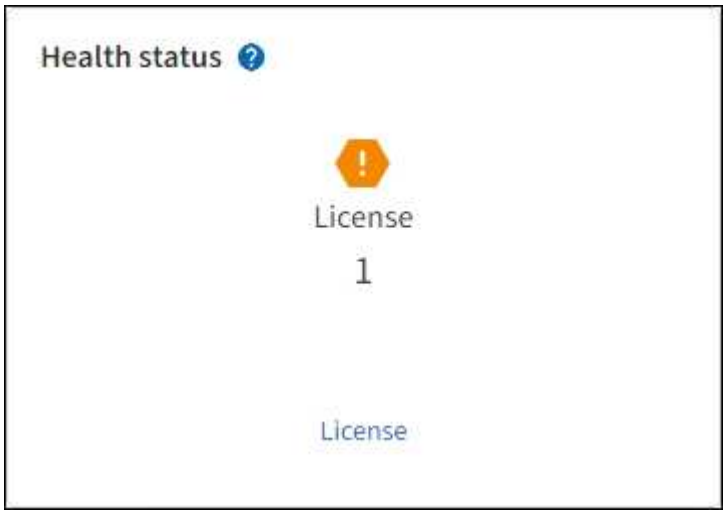
Puede ver la información de licencia del sistema StorageGRID, como la capacidad de almacenamiento máxima de su grid, cuando sea necesario.

Antes de empezar

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

Acerca de esta tarea

Si hay un problema con la licencia de software para este sistema StorageGRID, la tarjeta de estado del panel incluye un icono de estado de licencia y un enlace de **Licencia**. El número indica el número de problemas relacionados con la licencia.



Pasos

1. Para acceder a la página Licencia, realice una de las siguientes acciones:
   - En la tarjeta de estado de salud del panel de control, seleccione el icono de estado de la licencia o el enlace **Licencia**. Este vínculo sólo aparece si hay un problema con la licencia.
   - Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.
2. Vea los detalles de sólo lectura 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
- Tipo de licencia, ya sea **Perpetual** o **Suscripción**
- Capacidad de almacenamiento bajo licencia del grid
- Capacidad de almacenamiento admitida
- Fecha de finalización de la licencia. **N/A** aparece para una licencia perpetua.
- Fecha de finalización del contrato de servicio de soporte

  Esta fecha se lee del archivo de licencia actual y puede estar obsoleta si se amplió o renovó el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulte "Actualice la información de licencia de StorageGRID". También puede ver la fecha de finalización real del contrato con el asesor digital de Active IQ (también conocido como asesor digital).

- Contenido del archivo de texto de licencia

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

Actualice la información de licencia de StorageGRID

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

Antes de empezar

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

Pasos

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

   El nuevo archivo de licencia se valida y muestra.

4. Seleccione **Guardar**.

Utilice la API

Utilice la API de gestión de grid

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

los usuarios, más rápidamente.

Recursos de alto nivel

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

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

Emita solicitudes API

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

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

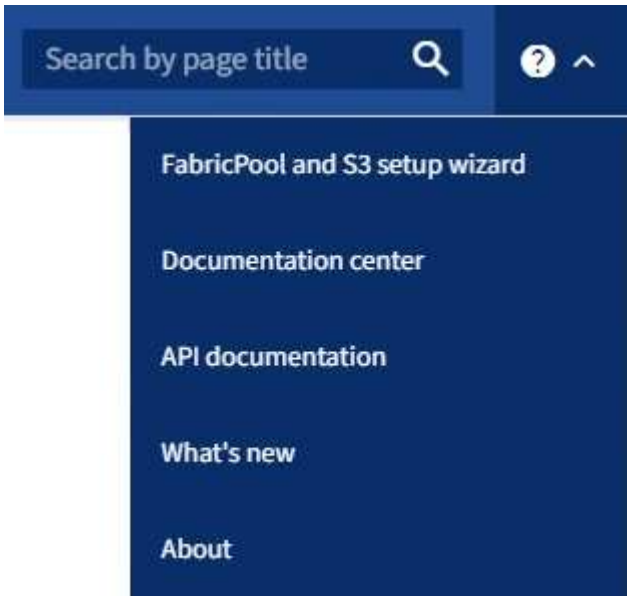
Antes de empezar

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

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

Pasos

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



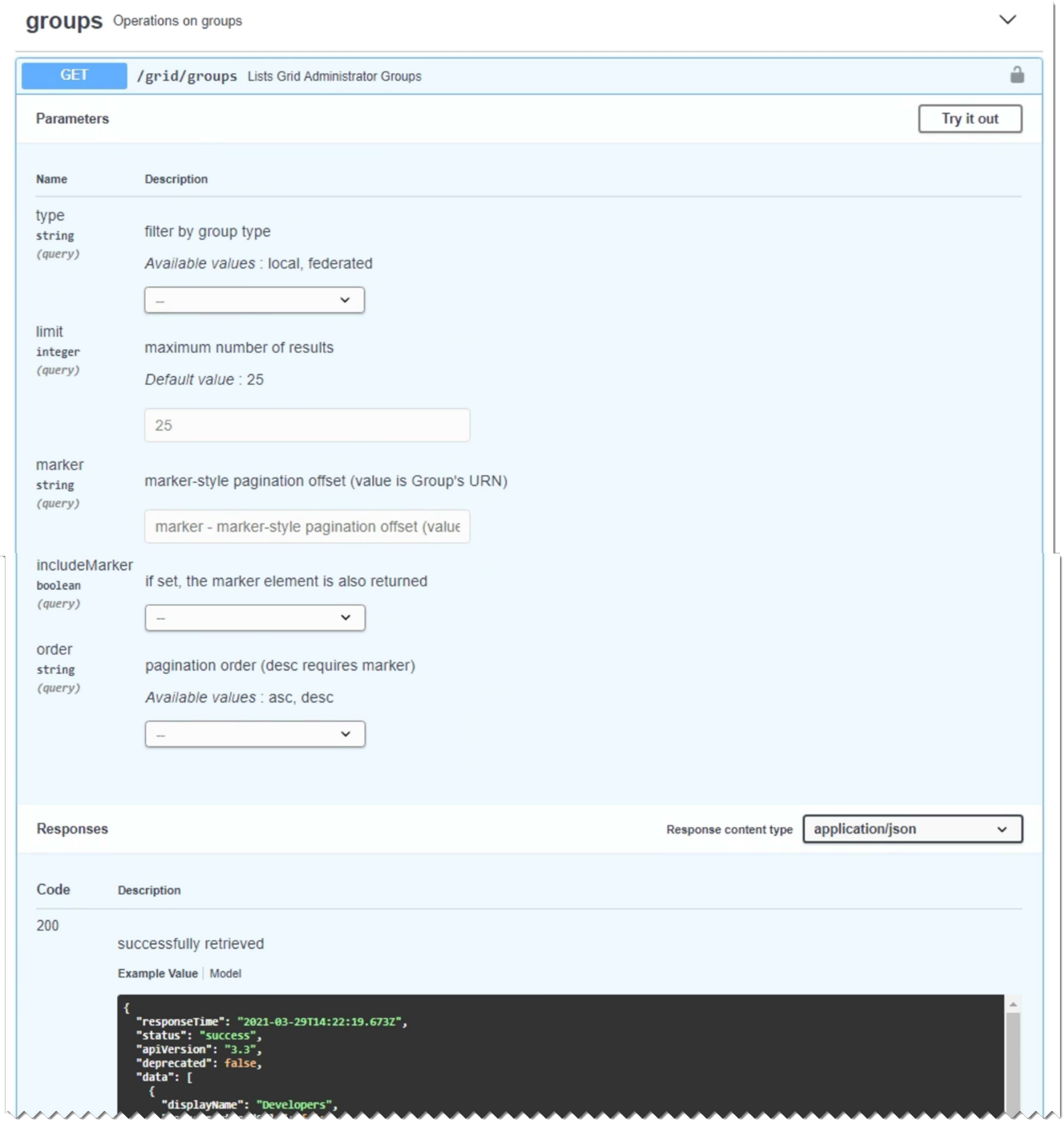
2. Para realizar una operación con la API privada, seleccione **Ir a documentación de API privada** en la página API de administración de StorageGRID.

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

3. Seleccione la operación deseada.

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

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



5. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.
6. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **probar**.
8. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
9. Seleccione **Ejecutar**.
10. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Operaciones de API de gestión de grid

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

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

- **CUENTAS**: Operaciones para administrar cuentas de inquilinos de almacenamiento, incluyendo la creación de nuevas cuentas y la recuperación del uso de almacenamiento para una cuenta dada.
- **ALARMAS**: Operaciones para listar 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 nodos.
- **ALERT-HISTORY**: Operaciones en alertas resueltas.
- **RECEPTORES DE ALERTA**: Operaciones en receptores de notificación de alerta (correo electrónico).
- **ALERT-RULES**: Operaciones en reglas de alerta.
- **ALERT-SILENCES**: Operaciones en silencios de alerta.
- **ALERTAS**: Operaciones en alertas.
- **AUDIT**: Operaciones para listar 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 errores de solicitudes entre sitios»» para obtener información sobre cómo mejorar la seguridad de la autenticación.

- **CERTIFICADOS DE CLIENTE**: Operaciones para configurar certificados de cliente de modo que se pueda acceder a StorageGRID de forma segura utilizando herramientas de monitoreo externas.
- **Config**: Operaciones relacionadas con el lanzamiento del producto y versiones de la API de administración 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.
- **Funciones desactivadas**: Operaciones para ver características que podrían haber sido desactivadas.
- **Servidores dns**: Operaciones para listar y cambiar servidores DNS externos configurados.
- **Endpoint-domain-names**: Operaciones para listar y cambiar los nombres de dominio de punto final S3.
- **Código de borrado**: Operaciones en perfiles de codificación de borrado.
- **EXPANSIÓN**: Operaciones de expansión (nivel de procedimiento).
- **EXPANSION-NODES**: Operaciones en expansión (nivel de nodo).
- **Sitios de expansión**: Operaciones en expansión (nivel de sitio).

- **Grid-networks**: Operaciones para listar y cambiar la Lista de Red de Grid.
- **Grid-passwords**: Operaciones para la gestión de contraseñas de grid.
- **GRUPOS**: Operaciones para administrar grupos de administradores de grid locales y para recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **Identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información federada del grupo y del usuario.
- **ilm**: Operaciones de 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, incluidas consultas métricas instantáneas en un único punto en el tiempo y consultas métricas de rango durante 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.

- **Node-details**: Operaciones en los detalles del nodo.
- **Node-health**: Operaciones en el estado de salud del nodo.
- **Node-storage-state**: Operaciones en el estado de almacenamiento del nodo.
- **Servidores ntp**: Operaciones para listar o actualizar servidores externos de Protocolo de Tiempo de Red (NTP).
- **OBJETOS**: Operaciones en objetos y metadatos de objetos.
- **RECUPERACIÓN**: Operaciones para el procedimiento de recuperación.
- **Recovery-package**: 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 los certificados de servidor de Grid Manager.
- **snmp**: Operaciones en la configuración SNMP actual.
- **Clases de tráfico**: Operaciones para las políticas de clasificación de tráfico.
- **Red-cliente-no confiable**: Operaciones en la configuración de la red cliente no confiable.
- **Usuarios**: Operaciones para ver y administrar usuarios de Grid Manager.

Creación de versiones de la API de gestión de grid

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

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

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

La versión principal de la API de administración de arrendatarios se bONTAP cuando se realizan cambios que son ***no compatibles*** con versiones anteriores. La versión menor de la API de administración de arrendatarios

se bONTAP cuando se hacen cambios que ***are sea compatible*** con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos extremos o nuevas propiedades. En el ejemplo siguiente se muestra cómo la versión de API se bONTAP en función del tipo de cambios realizados.

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

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

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

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

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

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

Determine qué versiones de API son compatibles con la versión actual

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

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

Especifique una versión API para una solicitud

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

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

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

Protección contra falsificación de solicitudes entre sitios (CSRF)

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

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

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

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

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

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

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

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

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

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

Use la API si está activado el inicio de sesión único

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

Pasos

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

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

   - El método SSO. Introduzca ADFS o adfs.
   - El nombre de usuario de SSO

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

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

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

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

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

   a. Declare las variables necesarias para iniciar sesión.

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

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

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

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

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

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

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

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

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

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

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

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

La respuesta incluye el ID de solicitud del cliente:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

La respuesta incluye el token de autenticación.

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

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

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

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

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

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

Acerca de esta tarea

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

Pasos

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

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

Se devuelve una URL de cierre de sesión:

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

2. Guarde la URL de cierre de sesión.

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

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

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

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

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

4. Elimine el token del portador de StorageGRID.

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

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

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

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

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

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

Pasos

1. Instale las dependencias necesarias de la siguiente manera:
   a. Instale Node.js (consulte "https://nodejs.org/en/download/").
   b. Instale los módulos Node.js necesarios (tippeteer y jsdom):

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

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

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

3. Cuando se le solicite, introduzca valores para los siguientes argumentos (o bien, pasarlos mediante parámetros):
   - La dirección de correo electrónico de SSO que se utiliza para iniciar sesión en Azure

- La dirección de StorageGRID
- El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos

4. Cuando se le solicite, introduzca la contraseña y esté preparado para proporcionar una autorización de MFA para Azure si así se lo solicita.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

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

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

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

Pasos

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

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

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

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

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

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

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

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

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

   En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada para

TENANTACCOUNTID. Los resultados se pasan a python -m json.tool para quitar la codificación JSON.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

g. Exporte el valor de 'acción':

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

h. Enviar cookies junto con credenciales:

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

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

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

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

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

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

La respuesta incluye el token de autenticación.

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

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

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

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

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

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

Acerca de esta tarea

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

Pasos

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

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

Se devuelve una URL de cierre de sesión:

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

2. Guarde la URL de cierre de sesión.

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

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

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

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

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

4. Elimine el token del portador de StorageGRID.

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

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

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

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

Desactivar las funcionalidades con la API

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

Acerca de esta tarea

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

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

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

*La empresa A puede lograr este objetivo mediante el sistema Desactivar características en la API de gestión de grid. Al desactivar completamente la característica **Cambiar contraseña raíz de arrendatario** en Grid Manager (tanto la interfaz de usuario como la API), la Compañía A puede garantizar que ningún usuario de*

*administrador (incluido el usuario raíz y los usuarios pertenecientes a grupos con el permiso **acceso raíz**) puede cambiar la contraseña para el usuario raíz de cualquier cuenta de arrendatario.*

Pasos

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

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

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

Reactivar las funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de grid para reactivar una función que se haya desactivado. Sin embargo, si desea evitar que alguna vez se reactiven las funciones desactivadas, puede desactivar la propia función **activateFeatures**.

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

Pasos

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

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

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

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

Control del acceso a StorageGRID

Control de acceso StorageGRID: Descripción general

Puede controlar quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios, y asignando permisos a cada grupo. De manera opcional, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar contraseñas de grid.

Controle el acceso a Grid Manager

Para determinar quién puede acceder a Grid Manager y a la API de gestión de grid, importe grupos y usuarios desde un servicio de federación de identidades o configure grupos locales y usuarios locales.

Uso "federación de identidades" realiza la configuración "grupos" y.. "usuarios" Más rápido, y permite a los usuarios iniciar sesión en StorageGRID usando credenciales conocidas. Puede configurar la federación de identidades si utiliza Active Directory, OpenLDAP u Oracle Directory Server.

> Póngase en contacto con el soporte técnico si desea utilizar otro servicio LDAP v3.

Puede determinar qué tareas puede realizar cada usuario asignando diferentes "permisos" a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan gestionar las reglas de ILM y los usuarios de otro grupo para realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

De manera opcional, puede configurar un grupo para que sea de sólo lectura. Los usuarios de un grupo de sólo lectura sólo pueden ver la configuración y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid.

Active el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) con el estándar de lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0). Usted primero "Configure y habilite SSO", Todos los usuarios deben ser autenticados por un proveedor de identidad externo antes de que puedan acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambie la clave de acceso de aprovisionamiento

La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, así como para descargar el paquete de recuperación de StorageGRID. También se necesita la contraseña para descargar los backups de la información de topología de la cuadrícula y las claves de cifrado del sistema StorageGRID. Puede hacerlo "cambie la contraseña" según sea necesario.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su grid tiene una contraseña única de la consola de nodos, la cual necesita iniciar sesión en el nodo como «administrador» mediante SSH, o al usuario raíz en una conexión de consola física o de máquina virtual. Según sea necesario, puedes "cambie la contraseña de la consola del nodo" para cada nodo.

Cambie la clave de acceso del aprovisionamiento

Use este procedimiento para cambiar la clave de acceso de aprovisionamiento de

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

Antes de empezar

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

Acerca de esta tarea

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **contraseñas de cuadrícula**.
2. En **Cambiar contraseña de aprovisionamiento**, selecciona **Hacer un cambio**
3. Introduzca la clave de acceso de aprovisionamiento actual.
4. Introduzca la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.
5. Almacene la nueva clave de acceso de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.
6. Vuelva a introducir la nueva contraseña y seleccione **Guardar**.

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

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

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

Cambie las contraseñas de la consola de los nodos

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

Antes de empezar

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

Acerca de esta tarea

Utilice la contraseña de la consola del nodo para iniciar sesión en un nodo como «administrador» mediante SSH, o para el usuario raíz en una conexión de consola física/máquina virtual. El proceso de cambiar la contraseña de la consola del nodo crea nuevas contraseñas para cada nodo de la cuadrícula y almacena las contraseñas en una actualización `Passwords.txt` en el paquete de recuperación. Las contraseñas se enumeran en la columna Password del archivo Passwords.txtl.

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

Acceda al asistente

Pasos

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

Introduzca la clave de acceso de aprovisionamiento

Pasos

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

Descargue el paquete de recuperación actual

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

Pasos

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

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

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

   No puede cancelar este proceso una vez que se inicia.

Cambie las contraseñas de la consola de los nodos

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

Pasos

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

   a. Abra el `.zip` archivo.

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

   c. Copie el nuevo archivo del paquete de recuperación (`.zip`) a dos ubicaciones seguras, seguras y separadas.

   > No sobrescriba el paquete de recuperación antiguo.

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

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

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

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

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

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

   b. Resuelva los problemas.

   c. Seleccione **Reintentar**.

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

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

Usar la federación de identidades

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

Configurar la federación de identidades para Grid Manager

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

Antes de empezar

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

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

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

Acerca de esta tarea

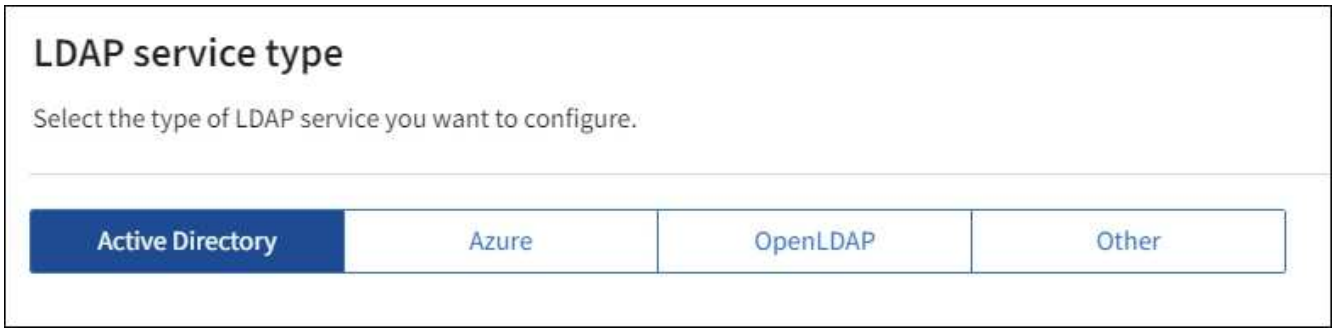
Puede configurar un origen de identidades para Grid Manager si desea importar grupos de otro sistema, como Active Directory, Azure AD, OpenLDAP u Oracle Directory Server. Puede importar los siguientes tipos de grupos:

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

Introduzca la configuración

Pasos

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



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

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

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

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

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

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

     - `sAMAccountName` o. `uid`

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

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

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

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

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

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

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

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

Introduzca uno de estos patrones:

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

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

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

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

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

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

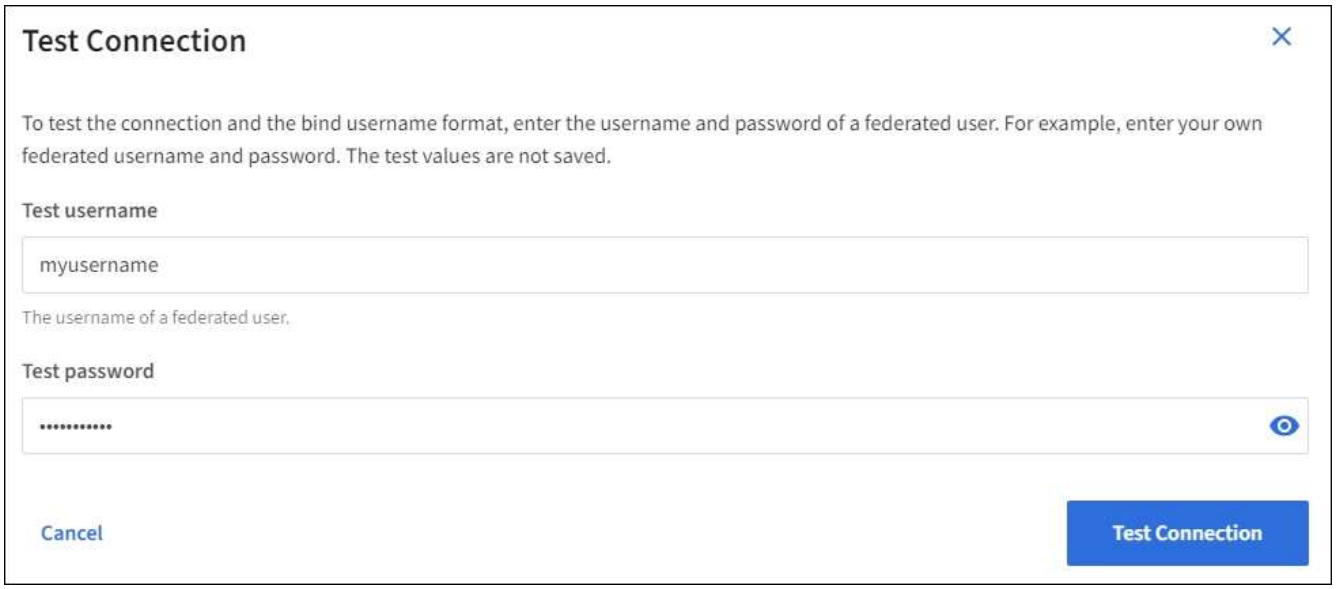
Pruebe la conexión y guarde la configuración

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

Pasos

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

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



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

Forzar la sincronización con el origen de identidades

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

Pasos

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

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

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

Deshabilitar la federación de identidades

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

Acerca de esta tarea

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

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

Pasos

1. Vaya a la página federación de identidades.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

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.

> En el caso de fuentes de identidad que no sean ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 para el usuario o elimine al usuario de todos los grupos.

Revestimientos memberOf y reft

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

Indización

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

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

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

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

Gestione los grupos de administradores

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

Antes de empezar

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

Cree un grupo de administración

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

Acceda al asistente

Pasos

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

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a los usuarios locales.
- Cree un grupo federado para importar usuarios desde el origen de identidades.

Grupo local

Pasos

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

Grupo federado

Pasos

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

Administrar permisos de grupo

Pasos

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

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

2. Seleccione uno o varios "permisos de grupo de administración".

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

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

Añadir usuarios (sólo grupos locales)

Pasos

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

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

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

Consulte y edite los grupos de administración

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

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

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

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación para el grupo.

2. Seleccione **acciones** > **Duplicar grupo**.
3. Complete el asistente para grupos duplicados.

Eliminar un grupo

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

Pasos

1. En la página Groups, seleccione la casilla de comprobación de cada grupo que desea quitar.
2. Seleccione **acciones** > **Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

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 pertenecientes a ese grupo no podrán iniciar sesión en Grid Manager o en la API de gestión de grid.

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

- Inicie sesión en Grid Manager
- Vea 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)
- Ver cierta información proporcionada en las páginas de configuración y mantenimiento

Interacción entre permisos y modo de acceso

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

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

Acceso raíz

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

Confirmar alarmas (heredadas)

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

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

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Este permiso también se usa para migrar claves S3 cuando se habilita la función de importación de claves S3. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.

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

Configuración de la página de topología de grid

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

ILM

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

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

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

Mantenimiento

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

- **CONFIGURACIÓN** > **Control de acceso**:
  - Contraseñas de grid
- **CONFIGURACIÓN** > **Red**:
  - Nombres de dominio de punto final S3
- **MANTENIMIENTO** > **tareas**:
  - Retirada

    - Expansión
    - Comprobación de existencia de objeto
    - Recuperación
- **MANTENIMIENTO** > **sistema**:
    - Paquete de recuperación
    - Actualización de software
- **SOPORTE** > **Herramientas**:
    - Registros

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

- **MANTENIMIENTO** > **Red**:
    - Servidores DNS
    - Red Grid
    - Servidores NTP
- **MANTENIMIENTO** > **sistema**:
    - Licencia
- **CONFIGURACIÓN** > **Red**:
    - Nombres de dominio de punto final S3
- **CONFIGURACIÓN** > **Seguridad**:
    - Certificados
- **CONFIGURACIÓN** > **Supervisión**:
    - Servidor de auditoría y syslog

Gestionar alertas

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

Consulta de métricas

Este permiso proporciona acceso a:

- **SOPORTE** > **Herramientas** > **Métricas** página
- Consultas personalizadas de métricas de Prometheus utilizando la sección **Metrics** de la API de administración de grid
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

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

Otra configuración de cuadrícula

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

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

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

Administrador de dispositivos de almacenamiento

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

Cuentas de inquilino

Este permiso permite:

- Acceda a la página Tenedores, donde puede crear, editar y eliminar cuentas de arrendatario
- Ver las políticas de clasificación de tráfico existentes
- Ver tarjetas de consola de Grid Manager que contienen detalles de arrendatario

Gestionar usuarios

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

Antes de empezar

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

Cree un usuario local

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

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

Grid Manager incluye un usuario local predefinido, denominado «`root». No puede eliminar el usuario root.

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

Acceda al asistente

Pasos

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

Introduzca las credenciales de usuario

Pasos

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

Asignar a grupos

Pasos

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

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

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

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

Ver y editar usuarios locales

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

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

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

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

  Los usuarios locales pueden cambiar sus propias contraseñas usando la opción **Cambiar contraseña** en el banner de Grid Manager.

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

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

Duplique un usuario

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

Pasos

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

Eliminar un usuario

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

> No puede eliminar el usuario root.

Pasos

1. En la página Usuarios, seleccione la casilla de verificación de cada usuario que desee eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

Utilizar inicio de sesión único (SSO)

Configurar el inicio de sesión único

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

Cómo funciona el inicio de sesión único

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

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

Inicie sesión cuando SSO esté habilitado

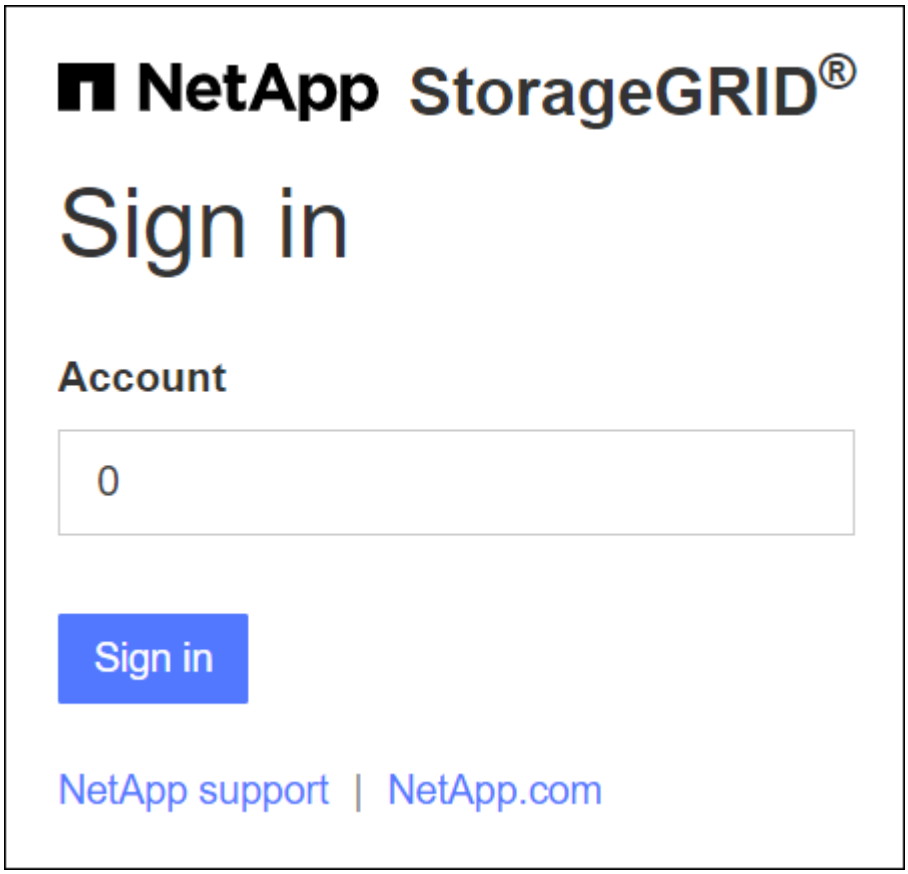
Cuando se habilita SSO y usted inicia sesión en StorageGRID, se le redirigirá a la página SSO de su organización para validar sus credenciales.

Pasos

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

   Aparece la página Inicio de sesión de StorageGRID.

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

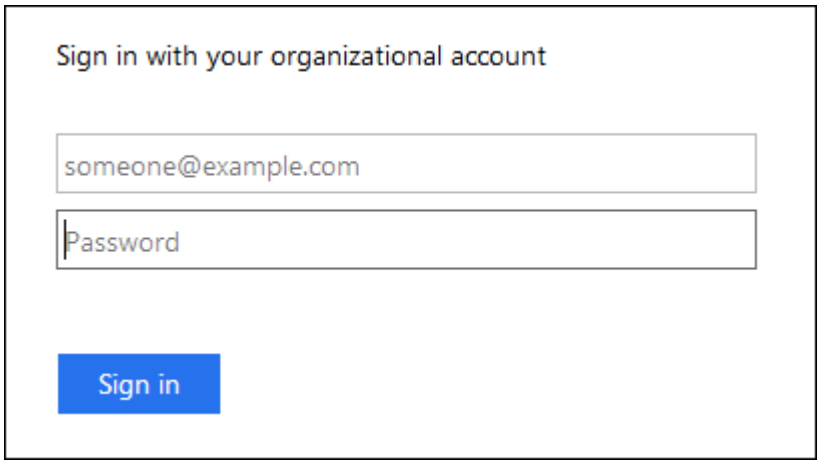


   - Si anteriormente ha accedido al administrador de grid o al administrador de inquilinos, se le pedirá que seleccione una cuenta reciente o que introduzca un ID de cuenta:

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

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

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



4. inicia sesión con sus credenciales de SSO.

Si sus credenciales de SSO son correctas:

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

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

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

   No es necesario volver a introducir las credenciales de SSO.

Cierre sesión cuando SSO esté habilitado

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

Pasos

1. Localice el enlace **Sign Out** en la esquina superior derecha de la interfaz de usuario.
2. Selecciona **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 **Nota:** Si utiliza Azure para SSO, es posible que tarde unos minutos en salir de todos los nodos de administración.
Administrador de inquilinos en uno o varios nodos de administrador	Inquilino Manager en cualquier nodo de administrador	Administrador de inquilinos en todos los nodos de administrador
Tanto Grid Manager como Inquilino Manager	Administrador de grid	Sólo Grid Manager. También debe cerrar sesión en el Administrador de inquilinos para cerrar la sesión de SSO.

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

Requisitos y consideraciones para el inicio de sesión único

Antes de activar el inicio de sesión único (SSO) para un sistema StorageGRID, revise los requisitos y consideraciones.

Requisitos del proveedor de identidades

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

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

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

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Requisitos DE AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

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

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

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

Requisitos adicionales

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

Consideraciones para Azure

Si usa Azure como tipo SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden producirse problemas de inicio de sesión si StorageGRID pierde su conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debe restaurar la conexión con el servidor LDAP.

Requisitos de certificado de servidor

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

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

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

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

Requisitos de puertos

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

Confirmar que los usuarios federados pueden iniciar sesión

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

Antes de empezar

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

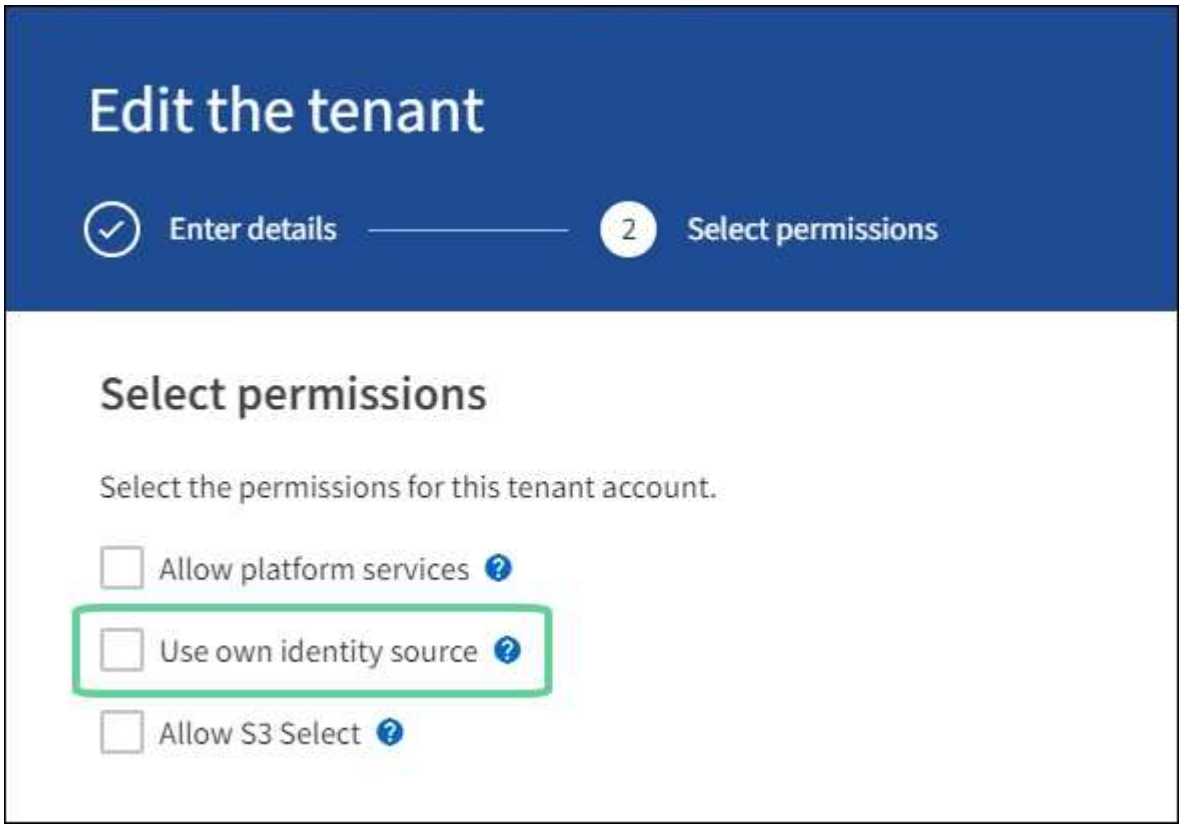
Pasos

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

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

a. Inicie sesión en el Administrador de arrendatarios para cada cuenta de arrendatario.
b. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
c. Confirme que la casilla de verificación **Habilitar federación de identidad** no está seleccionada.
d. Si lo es, confirme que los grupos federados que puedan estar en uso para esta cuenta de inquilino ya no son necesarios, desactive la casilla de verificación y seleccione **Guardar**.

2. Confirme que un usuario federado puede acceder a Grid Manager:
   a. En Grid Manager, seleccione **CONFIGURACIÓN** > **Control de acceso** > **grupos de administración**.
   b. Asegúrese de que al menos un grupo federado se ha importado del origen de identidad de Active Directory y de que se le ha asignado el permiso acceso raíz.
   c. Cierre la sesión.
   d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario en el grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado con permiso de acceso raíz puede iniciar sesión:
   a. En Grid Manager, seleccione **ARRENDATARIOS**.
   b. Seleccione la cuenta de arrendatario y seleccione **acciones** > **Editar**.
   c. En la ficha introducir detalles, seleccione **continuar**.
   d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.



Aparece la página inquilino.

a. Seleccione la cuenta de arrendatario, seleccione **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.

b. En el Administrador de inquilinos, seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

c. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso de acceso raíz para este arrendatario.

d. Cierre la sesión.

e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

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

Utilizar el modo de recinto de seguridad

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Configuró la federación de identidades para el sistema StorageGRID.
- Para la federación de identidades **Tipo de servicio LDAP**, ha seleccionado Active Directory o Azure, basándose en el proveedor de identidades SSO que planea utilizar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Acerca de esta tarea

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

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

- La respuesta de Azure incluye un nombre principal de usuario (UPN).

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

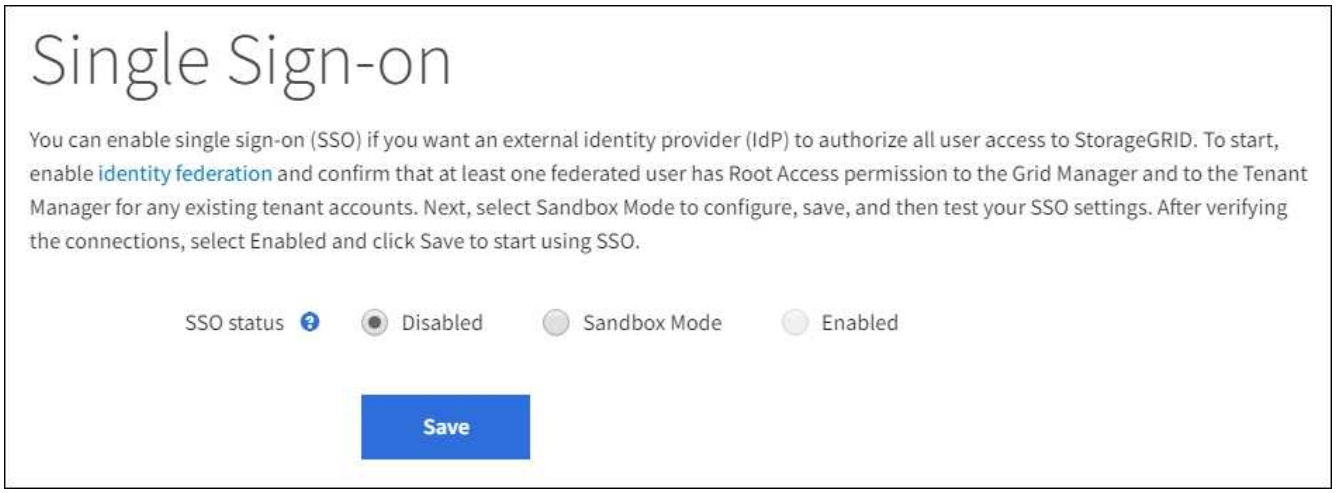
El modo de recinto de seguridad facilita la realización de esta configuración de fondo y la realización de pruebas de todos los ajustes antes de habilitar SSO. Al utilizar el modo sandbox, los usuarios no pueden iniciar sesión con SSO.

Acceder al modo de recinto de seguridad

Pasos

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

   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 el proveedor de identidad como origen de identidad federado. Consulte "Requisitos y consideraciones para el inicio de sesión único".

2. Seleccione **modo Sandbox**.

   Aparece la sección Proveedor de identidades.

Introduzca los detalles del proveedor de identidades

Pasos

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

Active Directory

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

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

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

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

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

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

4. Seleccione **Guardar**.

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

Azure

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

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

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

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

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

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

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

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

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

PingFederate

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

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

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

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

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

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

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

   Utilice el siguiente formato:

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

4. Seleccione **Guardar**.

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

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

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

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

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

Active Directory

Pasos

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

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

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

Azure

Pasos

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

PingFederate

Pasos

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

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

Probar conexiones SSO

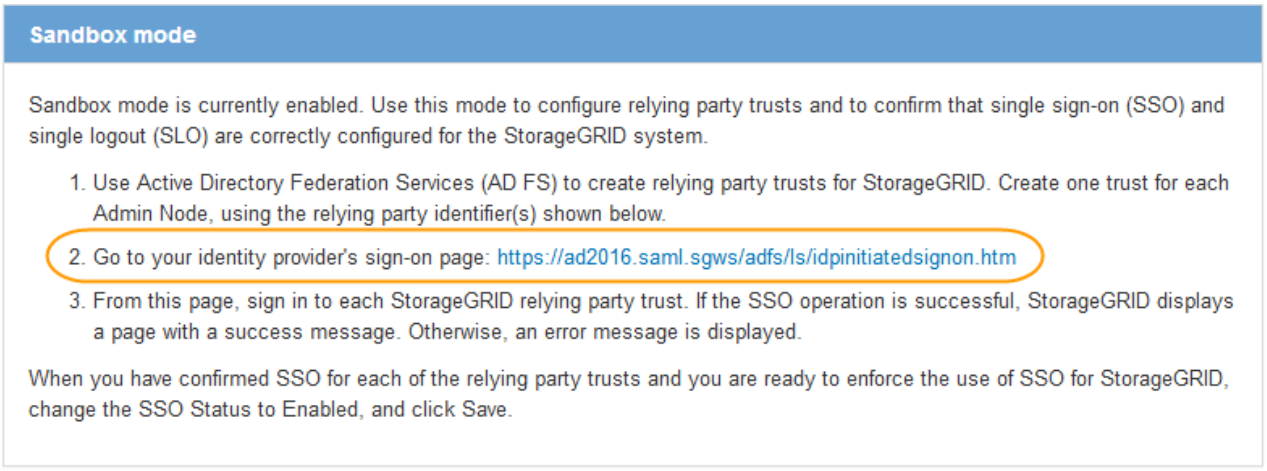
Antes de aplicar el uso del inicio de sesión único para todo el sistema StorageGRID, debe confirmar que el inicio de sesión único y el cierre de sesión único están correctamente configurados para cada nodo de administración.

Active Directory

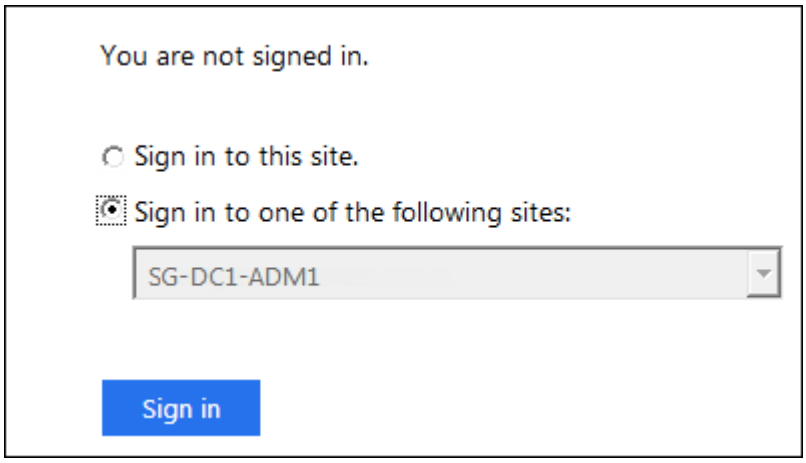
Pasos

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

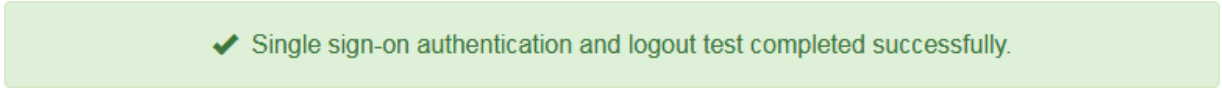
   La dirección URL se deriva del valor introducido en el campo **Nombre de servicio de Federación**.



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



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



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

Azure

Pasos

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

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

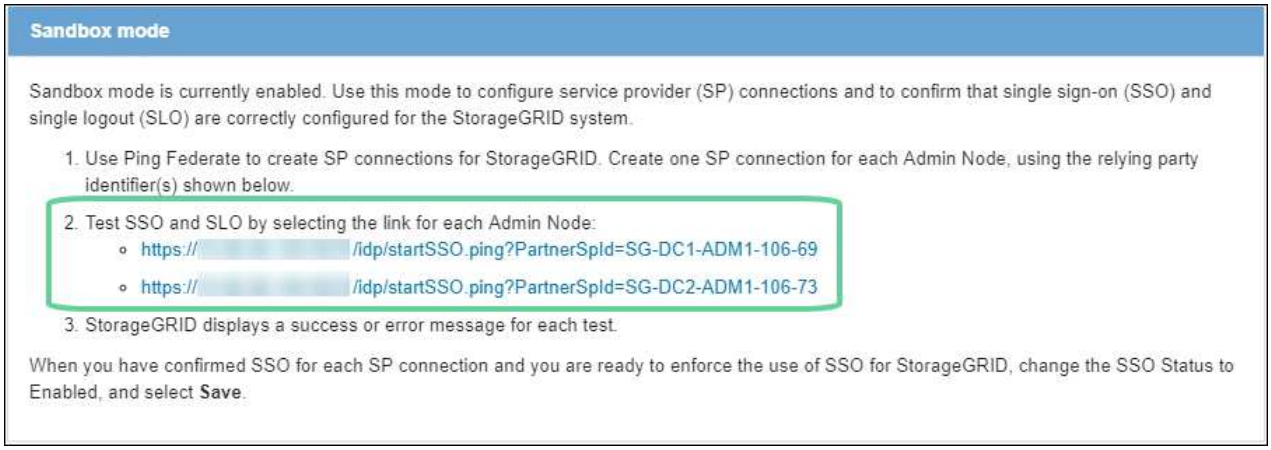
   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

PingFederate

Pasos

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

   Seleccione y pruebe un enlace cada vez.

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

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

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

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

Active el inicio de sesión único

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

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

Pasos

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

   El inicio de sesión único ahora está activado.

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

Crear confianzas de parte de confianza en AD FS

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

Antes de empezar

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

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

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

desde el shell de comandos.

Acerca de esta tarea

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

Cree una confianza de parte de confianza mediante Windows PowerShell

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

Pasos

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

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

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

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

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

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

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

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

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

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

7. Confirme que los metadatos se han importado correctamente.

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

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

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

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

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

Cree una confianza de parte de confianza importando metadatos de federación

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

Pasos

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

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

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

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

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

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

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

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

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

7. Agregar una regla de reclamación:

a. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
b. Seleccione **Agregar regla**:
c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
d. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

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

e. Para el almacén de atributos, seleccione **Active Directory**.
f. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.
g. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
h. Seleccione **Finalizar** y seleccione **Aceptar**.

8. Confirme que los metadatos se han importado correctamente.
   a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
   b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

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

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

Cree una confianza de parte de confianza manualmente

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

Pasos

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

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

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

c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo WebSSO de SAML 2,0**.

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

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

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

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

Admin_Node_Identifier

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

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

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

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

6. Para iniciar el asistente para reglas de reclamación, seleccione **Agregar regla**:

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

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

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

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

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

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

f. Seleccione **Finalizar** y seleccione **Aceptar**.

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

8. En la ficha **endpoints**, configure el extremo para un único cierre de sesión (SLO):

a. Seleccione **Añadir SAML**.

b. Seleccione **Tipo de extremo** > **SAML Logout**.

c. Seleccione **enlace** > **Redirigir**.

d. En el campo **Trusted URL**, introduzca la dirección URL utilizada para cerrar sesión único (SLO) desde este nodo de administración:

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

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

a. Seleccione **OK**.

9. En la ficha **firma**, especifique el certificado de firma para esta confianza de parte de confianza:
   a. Agregue el certificado personalizado:
      - Si posee el certificado de gestión personalizado cargado en StorageGRID, seleccione ese certificado.
      - Si no tiene el certificado personalizado, inicie sesión en el nodo de administración, vaya a. `/var/local/mgmt-api` directorio del nodo Admin y añada el `custom-server.crt` archivo de certificado.

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

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

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

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

Cree aplicaciones empresariales en Azure AD

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

Antes de empezar

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

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

- Tiene experiencia en la creación de aplicaciones empresariales en Azure Active Directory.
- Tiene una cuenta de Azure con una suscripción activa.

- Tiene uno de los siguientes roles en la cuenta de Azure: Administrador global, administrador de aplicaciones de cloud, administrador de aplicaciones o propietario del director del servicio.

Acceda a Azure AD

Pasos

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

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

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

Pasos

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

Descargue los metadatos de SAML para cada nodo de administración

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

Pasos

1. Repita estos pasos para cada nodo de administración.
   a. Inicie sesión en StorageGRID desde el nodo de administrador.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.

c. Seleccione el botón para descargar los metadatos de SAML de ese nodo de administración.

d. Guarde el archivo, que cargará en Azure AD.

Cargue metadatos de SAML en cada aplicación empresarial

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

Pasos

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

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

   a. Vaya a la página Propiedades de la aplicación de empresa.

   b. Establezca **asignación requerida** en **no** (a menos que desee configurar las asignaciones por separado).

   c. Vaya a la página Single Sign-On.

   d. Complete la configuración de SAML.

   e. Seleccione el botón **Upload metadata file** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.

   f. Después de cargar el archivo, seleccione **Guardar** y, a continuación, seleccione **X** para cerrar el panel. Volverá a la página Set up Single Sign-On with SAML.

3. Siga los pasos de "Utilizar el modo de recinto de seguridad" para probar cada aplicación.

Cree conexiones de proveedores de servicios (SP) en PingFederate

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

Antes de empezar

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

Acerca de esta tarea

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

Complete los requisitos previos en PingFederate

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

Crear almacén de datos

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

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

Crear validador de credenciales de contraseña

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

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

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

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

Pasos

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

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

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

Pasos

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

Cree una conexión SP en PingFederate

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

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

Elija el tipo de conexión del SP

Pasos

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

Importe los metadatos de SP

Pasos

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

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

4. Seleccione **Siguiente**.

Configure el SSO del explorador IDP

Pasos

1. En la ficha SSO del explorador, seleccione **Configurar SSO del explorador**.
2. En la ficha Perfiles de SAML, seleccione las opciones **SSO iniciado por el SP**, **SLO inicial de SP**, **SSO iniciado por IDP** y **SLO iniciado por IDP**.
3. Seleccione **Siguiente**.
4. En la ficha ciclo de vida de las aserción, no realice cambios.
5. En la ficha creación de aserción, seleccione **Configurar creación de aserción**.
   a. En la ficha asignación de identidades, seleccione **Estándar**.

b. En la ficha Contrato de atributo, utilice el formato **SAML_SUBJECT** como atributo Contract y el formato de nombre no especificado que se importó.

6. Para extender el contrato, seleccione **Eliminar** para eliminar `urn:oid`, que no se utiliza.

Asigne la instancia del adaptador

Pasos

1. En la ficha asignación de origen de autenticación, seleccione **asignar nueva instancia de adaptador**.
2. En la ficha instancias del adaptador, seleccione instancia del adaptador que haya creado.
3. En la ficha método de asignación, seleccione **recuperar atributos adicionales de un almacén de datos**.
4. En la ficha origen del atributo y Búsqueda del usuario, seleccione **Agregar origen del atributo**.
5. En la ficha almacén de datos, proporcione una descripción y seleccione almacén de datos usted agregó.
6. En la ficha Búsqueda de directorios LDAP:
   - Introduzca el **DN base**, que debe coincidir exactamente con el valor especificado en StorageGRID para el servidor LDAP.
   - Para el ámbito de búsqueda, seleccione **Subtree**.
   - Para la clase de objeto raíz, busque el atributo **objectGUID** y añádalo.
7. En la ficha tipos de codificación de atributos binarios LDAP , seleccione **Base64** para el atributo **objectGUID** .
8. En la ficha filtro LDAP, introduzca **sAMAccountName=${username}**.
9. En la ficha cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en la lista desplegable origen y seleccione **objectGUID** en la lista desplegable valor.
10. Revise y, a continuación, guarde el origen del atributo.
11. En la ficha origen del atributo Failsave, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **hecho**.
13. Seleccione **Listo**.

Configure los ajustes de protocolo

Pasos

1. En la ficha **Conexión SP** > **SSO del navegador** > **Configuración de protocolo**, seleccione **Configurar ajustes de protocolo**.
2. En la ficha URL del servicio de consumidor de aserción , acepte los valores predeterminados que se importaron desde los metadatos SAML de StorageGRID (**POST** para el enlace y. `/api/saml-response` Para la URL del extremo).
3. En la ficha direcciones URL del servicio SLO , acepte los valores predeterminados, que se importaron desde los metadatos SAML de StorageGRID (**REDIRECT** para el enlace y. `/api/saml-logout` Para la dirección URL del extremo.
4. En la pestaña Enlaces SAML permitidos, desactive **ARTEFACTO** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje las casillas de verificación **Requerir que se firmen las solicitudes AUTHN** y **Siempre firmar afirmación** seleccionadas.
6. En la ficha Directiva de cifrado, seleccione **Ninguno**.

7. Revise el resumen y seleccione **hecho** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **hecho** para guardar la configuración de SSO del explorador.

Configurar credenciales

Pasos

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

Cree conexiones adicionales del SP

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

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

Pasos

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

Desactive el inicio de sesión único

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

federación de identidades.

Antes de empezar

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

Pasos

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

   Aparece la página Single Sign-On.

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

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

4. Seleccione **OK**.

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

> La deshabilitación de SSO para un nodo de administrador no afecta la configuración de SSO para ningún otro nodo de administrador que esté en el grid. La casilla de verificación **Enable SSO** en la página Single Sign-On en Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

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

3. Confirme que desea deshabilitar SSO.

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

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

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

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

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

7. Si ha desactivado SSO temporalmente porque necesita acceder a Grid Manager por algún otro motivo:

   a. Realice cualquier tarea o tarea que necesite realizar.
   b. Seleccione **Cerrar sesión** y cierre Grid Manager.
   c. Vuelva a habilitar SSO en el nodo de administrador. Puede realizar cualquiera de los siguientes pasos:

      - Ejecute el siguiente comando: `enable-saml`

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

      Confirme que desea habilitar SSO.

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

      - Reinicie el nodo de cuadrícula: `reboot`

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

Usar federación de grid

¿Qué es GRID federation?

Puede utilizar la federación de grid para clonar inquilinos y replicar sus objetos entre dos

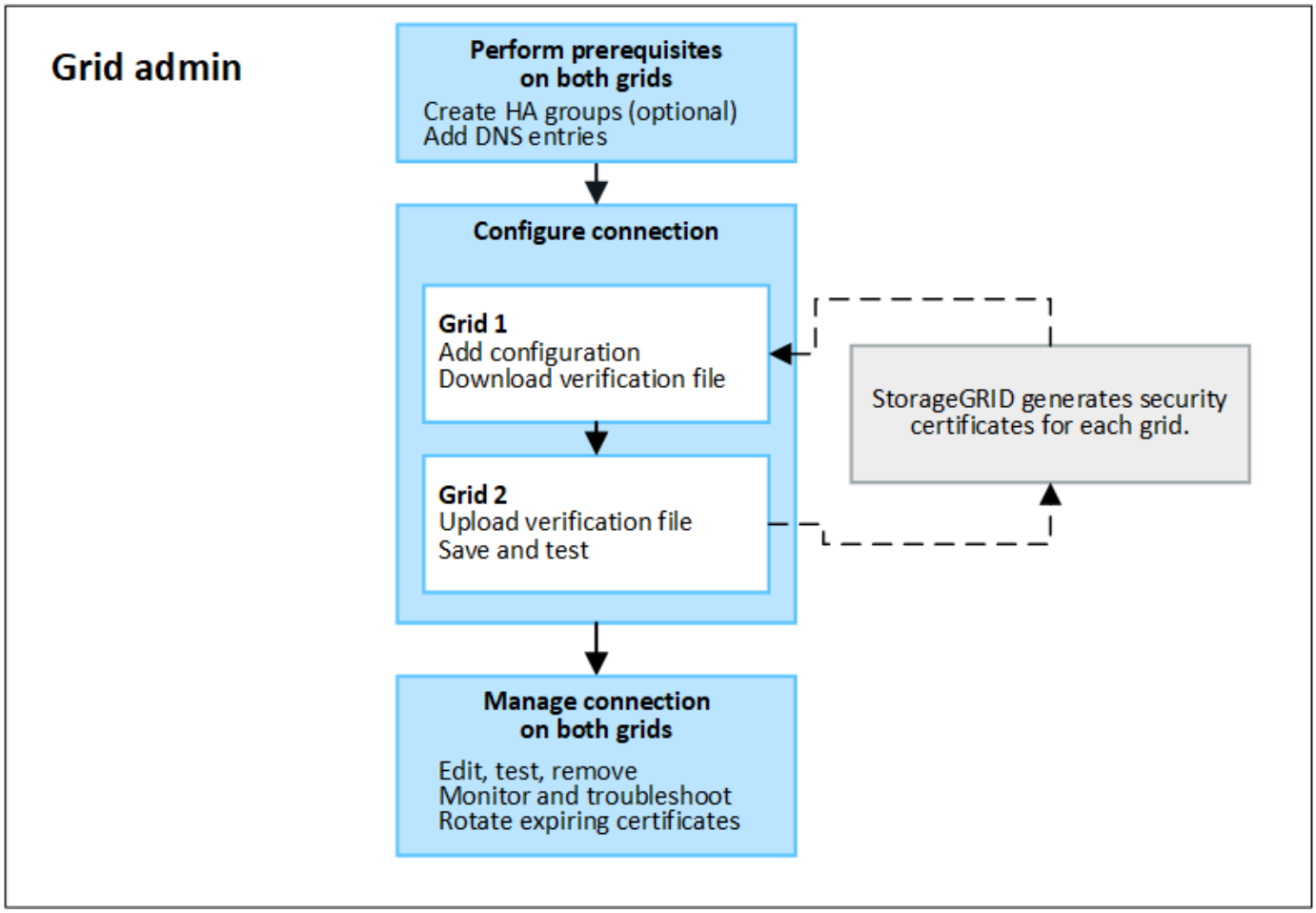
sistemas StorageGRID para la recuperación ante desastres.

¿Qué es una conexión de federación de grid?

Una conexión de federación de grid es una conexión bidireccional, de confianza y segura entre los nodos de administración y puerta de enlace en dos sistemas StorageGRID.

Flujo de trabajo de federación de grid

El diagrama de flujo de trabajo resume los pasos para configurar una conexión de federación de grid entre dos cuadrículas.



Consideraciones y requisitos para las conexiones de federación de grid

- Los dos grids utilizados para la federación de grid deben ejecutar StorageGRID 11,7.
- Un grid puede tener una o más conexiones de federación de grid a otras grids. Cada conexión de federación de grid es independiente de cualquier otra conexión. Por ejemplo, si Grid 1 tiene una conexión con Grid 2 y una segunda conexión con Grid 3, no hay ninguna conexión implícita entre Grid 2 y Grid 3.
- Las conexiones de federación de grid son bidireccionales. Una vez establecida la conexión, puede supervisar y gestionar la conexión desde cualquiera de las dos redes.
- Debe existir al menos una conexión de federación de grid para poder utilizarla "clon de cuenta" o. "replicación entre grid".

Requisitos de redes y dirección IP

- Las conexiones de federación de grid se pueden producir en la red de grid, la red de administración o la red de cliente.
- Una conexión de federación de grid conecta un grid a otro. La configuración de cada grid especifica un extremo de federación de grid en el otro grid que consta de nodos de administración, nodos de puerta de enlace o ambos.
- La práctica recomendada es conectar "Grupos de alta disponibilidad" De nodos de puerta de enlace y administración en cada grid. El uso de grupos de alta disponibilidad ayuda a garantizar que las conexiones de federación de grid permanecerán en línea en caso de que los nodos dejen de estar disponibles. Si la interfaz activa en cualquiera de los grupos de alta disponibilidad falla, la conexión puede usar una interfaz de backup.
- No se recomienda crear una conexión de federación de grid que utilice la dirección IP de un único nodo de administración o nodo de pasarela. Si el nodo deja de estar disponible, la conexión de federación de grid también no estará disponible.
- "Replicación entre grid" De objetos requiere que los nodos de almacenamiento de cada grid puedan acceder a los nodos de administración y puerta de enlace configurados en el otro grid. En cada grid, confirme que todos los nodos de almacenamiento tienen una ruta de ancho de banda alto a los nodos de administración o puerta de enlace utilizados para la conexión.

Utilice FQDN para equilibrar la carga de la conexión

En un entorno de producción, utilice nombres de dominio completamente cualificados (FQDN) para identificar cada cuadrícula en la conexión. A continuación, cree las entradas DNS apropiadas, de la siguiente manera:

- El FQDN para Grid 1 se asignó a una o más direcciones IP virtuales (VIP) para grupos de alta disponibilidad en Grid 1, o a la dirección IP de uno o más nodos de administración o puerta de enlace en Grid 1.
- El FQDN para Grid 2 asignado a una o más direcciones VIP para Grid 2 o a la dirección IP de uno o más nodos de administración o puerta de enlace en Grid 2.

Cuando utiliza varias entradas DNS, las solicitudes para utilizar la conexión se equilibran de carga, de la siguiente manera:

- Las entradas de DNS que se asignan a las direcciones VIP de varios grupos de alta disponibilidad se equilibran la carga entre los nodos activos de los grupos de alta disponibilidad.
- Las entradas de DNS que se asignan a las direcciones IP de varios nodos de administración o nodos de pasarela se equilibran la carga entre los nodos asignados.

Requisitos de puertos

Al crear una conexión de federación de grid, puede especificar cualquier número de puerto no utilizado de 23000 a 23999. Ambas rejillas de esta conexión utilizarán el mismo puerto.

Debe asegurarse de que ningún nodo de ninguno de los grid utilice este puerto para otras conexiones.

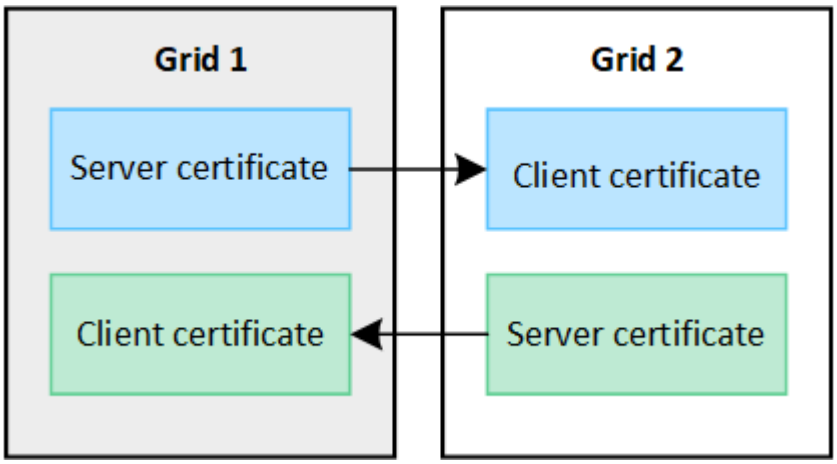
Requisitos de certificado

Cuando se configura una conexión de federación de grid, StorageGRID genera automáticamente cuatro certificados SSL:

- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la cuadrícula 1 a la

cuadrícula 2

- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la cuadrícula 2 a la cuadrícula 1



Por defecto, los certificados son válidos durante 730 días (2 años). Cuando estos certificados se acercan a su fecha de vencimiento, la alerta **Vencimiento del certificado de federación de grid** le recuerda que debe rotar los certificados, lo que puede hacer con el Administrador de grid.

> Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar. La replicación de datos estará pendiente hasta que se actualicen los certificados.

Leer más

- "Crear conexiones de federación de grid"
- "Gestionar conexiones de federación de grid"
- "Solucionar errores de federación de grid"

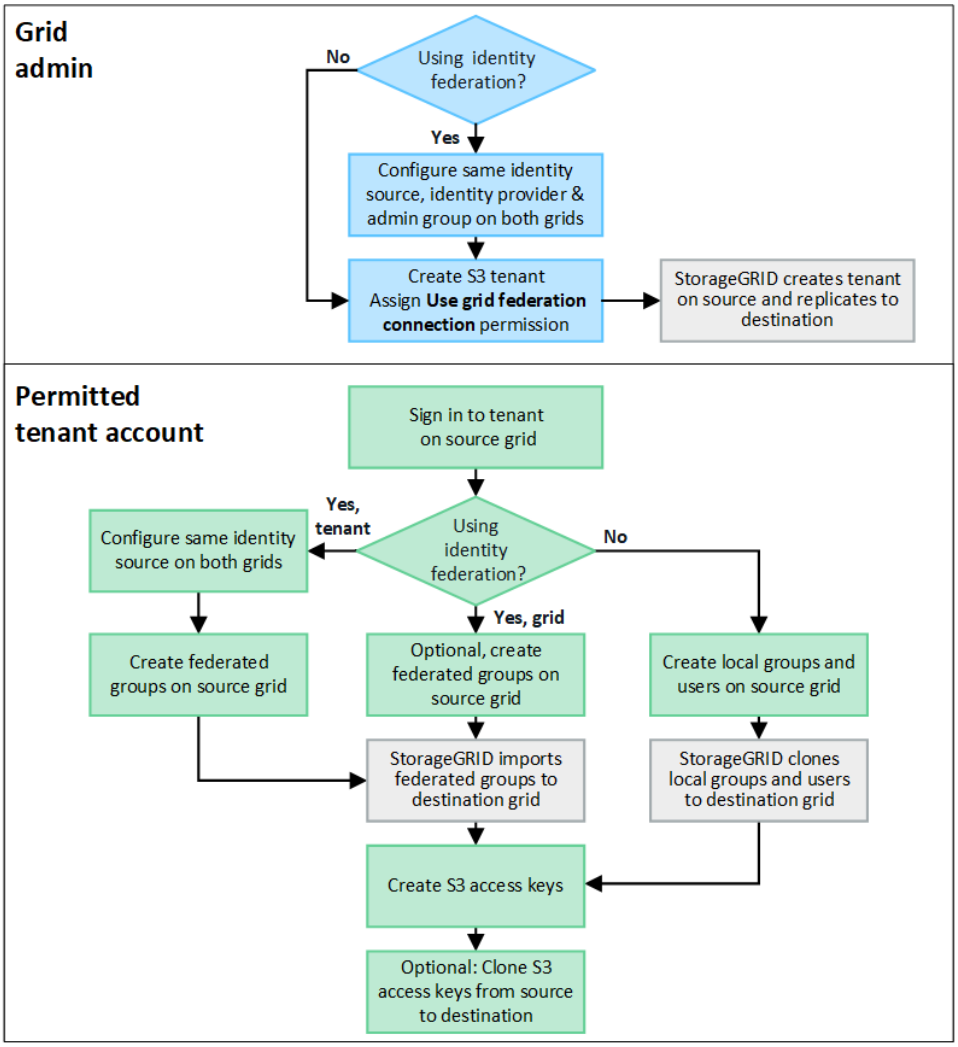
¿Qué es el clon de cuenta?

El clon de la cuenta es la replicación automática de una cuenta de inquilino, grupos de inquilinos, usuarios de inquilinos y, opcionalmente, S3 claves de acceso entre los sistemas StorageGRID en un "conexión de federación de grid".

La clonación de cuenta es necesaria para "replicación entre grid". Al clonar la información de la cuenta desde un sistema StorageGRID de origen a un sistema StorageGRID de destino se garantiza que los usuarios y grupos inquilinos puedan acceder a los bloques y objetos correspondientes en cualquiera de los grid.

Flujo de trabajo del clon de cuenta

El diagrama de flujo de trabajo muestra los pasos que realizarán los administradores de grid y los inquilinos permitidos para configurar el clon de cuenta. Estos pasos se realizan después del "la conexión de federación de grid está configurada".



Flujo de trabajo del administrador de grid

Los pasos que realizan los administradores de grid dependen de si los sistemas StorageGRID del "conexión de federación de grid" Utilice el inicio de sesión único (SSO) o la federación de identidades.

Configurar SSO para el clon de cuenta (opcional)

Si alguno de los sistemas StorageGRID de la conexión de federación de grid utiliza SSO, ambos grids deben utilizar SSO. Antes de crear las cuentas de inquilino para la federación de grid, los administradores de grid de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure el mismo origen de identidad para ambas cuadrículas. Consulte "Usar la federación de identidades".
2. Configure el mismo proveedor de identidad de SSO (IdP) para ambas cuadrículas. Consulte "Configurar el inicio de sesión único".
3. "Cree el mismo grupo de administración" en ambas cuadrículas importando el mismo grupo federado.

   Al crear el inquilino, seleccionará este grupo para que tenga el permiso inicial de acceso raíz para las cuentas de inquilino de origen y de destino.

Si este grupo de administración no existe en ambas cuadrículas antes de crear el arrendatario, el arrendatario no se replica en el destino.

Configurar federación de identidades a nivel de cuadrícula para el clon de cuenta (opcional)

Si alguno de los sistemas StorageGRID utiliza la federación de identidades sin SSO, ambas cuadrículas deben utilizar la federación de identidades. Antes de crear las cuentas de inquilino para la federación de grid, los administradores de grid de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure el mismo origen de identidad para ambas cuadrículas. Consulte "Usar la federación de identidades".
2. Opcionalmente, si un grupo federado tendrá permiso inicial de acceso root para las cuentas de arrendatario de origen y destino, "cree el mismo grupo de administración" en ambas cuadrículas importando el mismo grupo federado.

   Si asigna permiso de acceso raíz a un grupo federado que no existe en ambas cuadrículas, el inquilino no se replica en la cuadrícula de destino.

3. Si no desea que un grupo federado tenga permiso de acceso raíz inicial para ambas cuentas, especifique una contraseña para el usuario raíz local.

Cree una cuenta de inquilino de S3 permitida

Después de configurar, de manera opcional, el inicio de sesión único o la federación de identidades, un administrador de grid lleva a cabo estos pasos para determinar qué inquilinos pueden replicar objetos del bloque en otros sistemas StorageGRID.

Pasos

1. Determine qué grid desea que sea la cuadrícula de origen del inquilino para las operaciones de clonación de cuentas.

   La cuadrícula donde se creó originalmente el inquilino se conoce como *source grid* del inquilino. La cuadrícula donde se replica el inquilino se conoce como *grid de destino* del inquilino.

2. Cree una nueva cuenta de inquilino de S3 en ese grid.
3. Asigne el permiso **Use grid federation connection**.
4. Si la cuenta de inquilino administrará sus propios usuarios federados, asigne el permiso **Usar propia fuente de identidad**.

   Si se asigna este permiso, tanto las cuentas de arrendatario de origen como las de destino deben configurar el mismo origen de identidad antes de crear grupos federados. Los grupos federados agregados al inquilino de origen no se pueden clonar en el inquilino de destino a menos que ambas cuadrículas utilicen el mismo origen de identidad.

5. Seleccione una conexión de federación de cuadrícula específica.
6. Guarde el inquilino.

   Cuando se guarda un nuevo inquilino con el permiso **Usar conexión de federación de grid**, StorageGRID crea automáticamente una réplica de ese inquilino en la otra cuadrícula, de la siguiente manera:

- Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, cuota de almacenamiento y permisos asignados.
- Si seleccionó un grupo federado para tener permiso de acceso raíz para el inquilino, ese grupo se clona en el inquilino de destino.
- Si seleccionó un usuario local para que tenga permiso de acceso raíz para el inquilino, ese usuario se clona en el inquilino de destino. Sin embargo, la contraseña para ese usuario no está clonada.

Para obtener más información, consulte"Gestionar inquilinos permitidos para la federación de grid".

Flujo de trabajo de cuenta de inquilino permitido

Después de que un inquilino con el permiso **Usar conexión de federación de grid** se replica en la cuadrícula de destino, las cuentas de inquilino permitidas pueden realizar estos pasos para clonar grupos de inquilinos, usuarios y claves de acceso S3.

Pasos

1. Inicie sesión en la cuenta de inquilino en la cuadrícula de origen del inquilino.
2. Si está permitido, configure Identify federation tanto en las cuentas de arrendatario de origen como en las de destino.
3. Cree grupos y usuarios en el arrendatario de origen.

   Cuando se crean nuevos grupos o usuarios en el inquilino de origen, StorageGRID los clona automáticamente en el inquilino de destino, pero no se produce ningún clonado del destino al origen.

4. Crear claves de acceso S3.
5. Opcionalmente, clone las claves de acceso S3 del inquilino de origen al inquilino de destino.

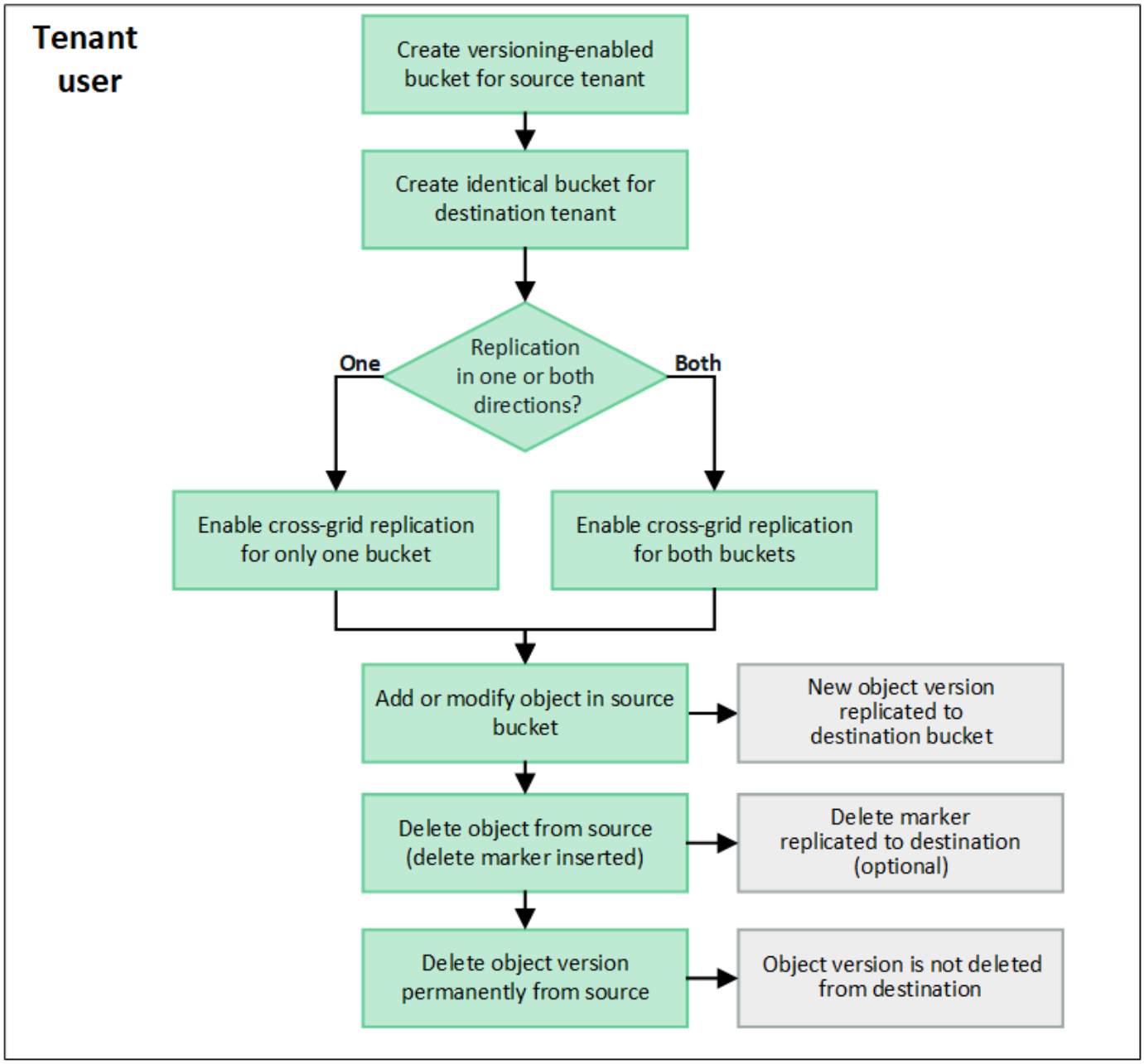
Para obtener detalles sobre el flujo de trabajo permitido de la cuenta de inquilino y saber cómo se clonan los grupos, los usuarios y las claves de acceso S3, consulte "Clone los usuarios y los grupos de inquilinos" y.. "Clone las claves de acceso S3 mediante la API".

¿Qué es la replicación entre grid?

La replicación entre grid es la replicación automática de objetos entre buckets de S3 seleccionados en dos sistemas StorageGRID conectados en un "conexión de federación de grid". "Clon de cuenta" es necesario para la replicación entre grid.

Flujo de trabajo de replicación entre grid

El diagrama de flujo de trabajo resume los pasos para configurar la replicación entre bloques en dos cuadrículas.



Requisitos de la replicación entre grid

Si una cuenta de inquilino tiene el permiso **Use grid federation connection** para usar uno o más "conexiones de federación de grid", Un usuario inquilino con permiso de acceso root puede crear cubos idénticos en las cuentas de inquilino correspondientes en cada cuadrícula. Estos bloques:

- Debe tener el mismo nombre y región
- Debe tener el control de versiones activado
- Debe tener S3 Object Lock desactivado
- Debe estar vacío

Una vez creados ambos bloques, la replicación entre grid se puede configurar para uno o ambos bloques.

Leer más

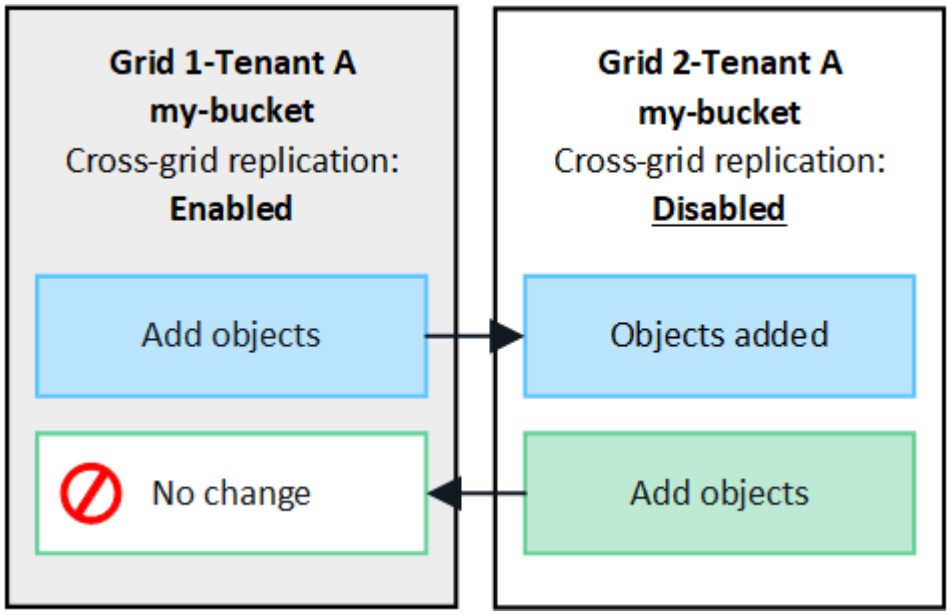
"Gestionar la replicación entre grid"

Funcionamiento de la replicación entre grid

La replicación entre grid puede configurarse para que ocurra en una dirección o en ambas direcciones.

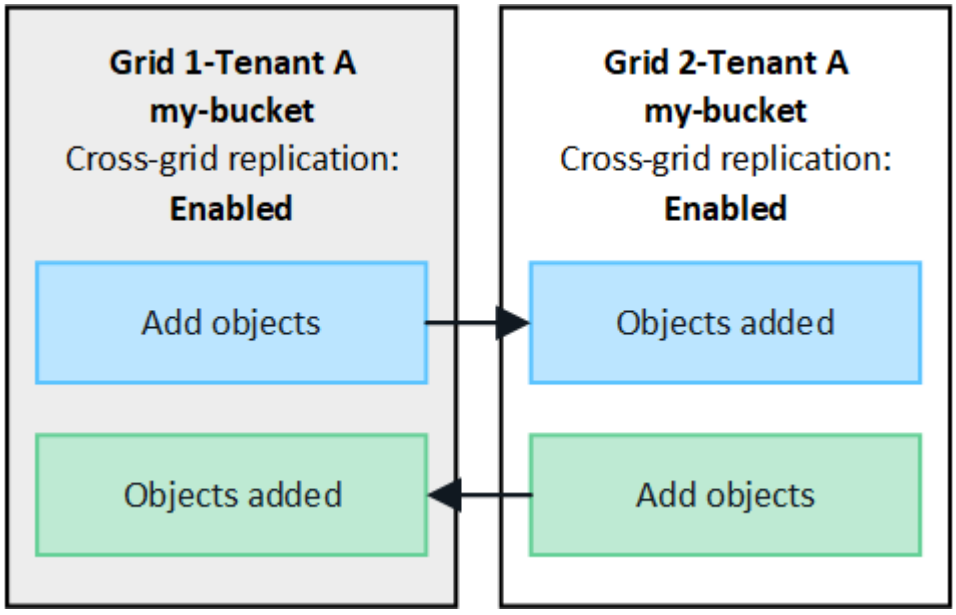
Replicación en una dirección

Si habilita la replicación entre grid para un bucket en solo una grid, los objetos agregados a ese bucket (el bucket de origen) se replican en el bucket correspondiente en la otra grid (el bucket de destino). Sin embargo, los objetos añadidos al depósito de destino no se vuelven a replicar en el origen. En la figura, la replicación entre grid está activada para `my-bucket` De la cuadrícula 1 a la cuadrícula 2, pero no está activada en la otra dirección.



Replicación en ambas direcciones

Si habilita la replicación entre grid para el mismo bucket en ambos grids, los objetos agregados a cada bucket se replican en el otro grid. En la figura, la replicación entre grid está activada para `my-bucket` en ambas direcciones.



¿Qué sucede cuando se ingieren objetos?

Cuando un cliente S3 agrega un objeto a un bloque que tiene habilitada la replicación entre grid, sucede lo siguiente:

1. StorageGRID replica automáticamente el objeto del bloque de origen al de destino. El tiempo para realizar esta operación de replicación en segundo plano depende de varios factores, incluidos la cantidad de otras operaciones de replicación pendientes.

   El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GET Object o HEAD Object. La respuesta incluye un recurso específico de StorageGRID `x-ntap-sg-cgr-replication-status` Encabezado de respuesta, que tendrá uno de los siguientes valores: El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GET Object o HEAD Object. La respuesta incluye un recurso específico de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **ÉXITO**: La replicación fue exitosa para todas las conexiones a la red. • **PENDIENTE**: El objeto no ha sido replicado en al menos una conexión de red. • **FALLO**: La replicación no está pendiente para ninguna conexión a la red y al menos una falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

   > ⓘ StorageGRID no admite el `x-amz-replication-status` encabezado.

2. StorageGRID utiliza la política de ILM activa de cada grid para gestionar los objetos, al igual que lo haría con cualquier otro objeto. Por ejemplo, el objeto A en Grid 1 se puede almacenar como dos copias replicadas y conservarse permanentemente, mientras que la copia del objeto A replicado en Grid 2 se puede almacenar con el código de borrado 2+1 y eliminarse después de tres años.

¿Qué sucede cuando se eliminan los objetos?

Como se describe en "Eliminar flujo de datos", StorageGRID puede eliminar un objeto por cualquiera de estos motivos:

- El cliente S3 emite una solicitud de eliminación.
- Un usuario del gestor de inquilinos selecciona el "Suprimir objetos del depósito" opción para eliminar todos los objetos de un depósito.
- El bloque tiene una configuración del ciclo de vida que caduca.
- El último periodo de tiempo de la regla de ILM para el objeto finaliza, y no se han especificado más ubicaciones.

Cuando StorageGRID elimina un objeto debido a una operación Eliminar objetos en el bloque, la caducidad del ciclo de vida del bloque o la caducidad de la ubicación de ILM, el objeto replicado nunca se elimina del otro grid en una conexión de la federación de grid. Sin embargo, los marcadores de borrado que se han añadido al bloque de origen mediante eliminaciones de clientes de S3 se pueden replicar opcionalmente en el bloque de

destino.

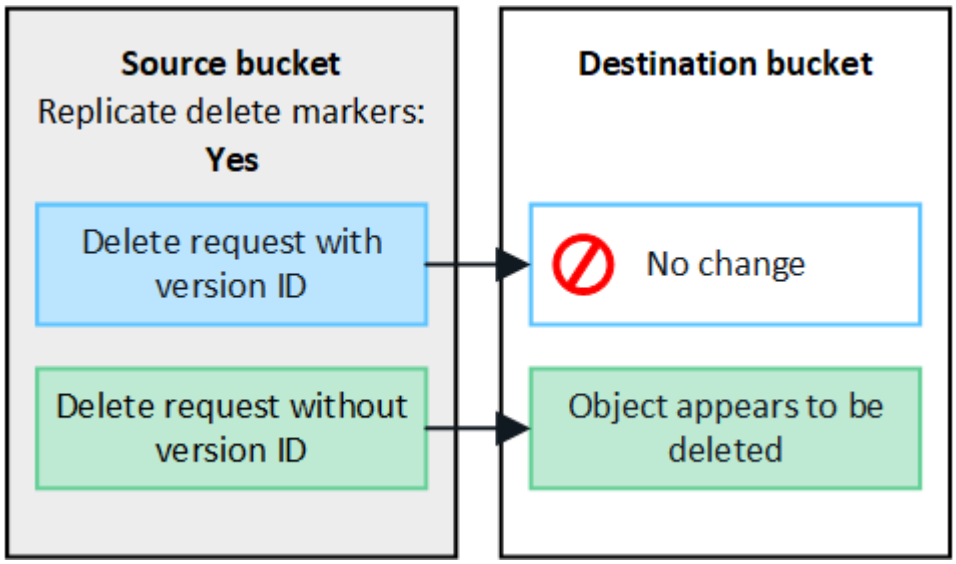
Para comprender qué sucede cuando un cliente S3 elimina objetos de un bloque que tiene habilitada la replicación entre grid, revise cómo los clientes S3 eliminan objetos de los bloques que tienen el control de versiones activado, de la siguiente manera:

- Si un cliente S3 emite una solicitud de eliminación que incluye un ID de versión, esa versión del objeto se elimina de forma permanente. No se ha añadido ningún marcador de borrado al depósito.
- Si un cliente S3 emite una solicitud de eliminación que no incluye un ID de versión, StorageGRID no elimina ninguna versión de objeto. En su lugar, agrega un marcador de borrado al cubo. El marcador de borrado hace que StorageGRID actúe como si el objeto se hubiera eliminado:
  - Una solicitud GET sin un ID de versión fallará con `404 No Object Found`
  - Una solicitud GET con un identificador de versión válido se realizará correctamente y devolverá la versión del objeto solicitado.

Cuando un cliente S3 elimina un objeto de un bloque que tiene habilitada la replicación entre grid, StorageGRID determina si desea replicar la solicitud de eliminación en el destino, de la siguiente manera:

- Si la solicitud de eliminación incluye un ID de versión, esa versión de objeto se elimina permanentemente de la cuadrícula de origen. Sin embargo, StorageGRID no replica las solicitudes de eliminación que incluyan un ID de versión, por lo que la misma versión del objeto no se elimina del destino.
- Si la solicitud de eliminación no incluye un ID de versión, StorageGRID puede replicar opcionalmente el marcador de eliminación, en función de cómo se configure la replicación entre grid para el bloque:
  - Si decide replicar marcadores de eliminación (valor predeterminado), se agrega un marcador de eliminación al bloque de origen y se replica en el bloque de destino. De hecho, el objeto parece eliminarse en ambas cuadrículas.
  - Si decide no replicar marcadores de eliminación, se agrega un marcador de eliminación al depósito de origen, pero no se replica en el depósito de destino. De hecho, los objetos que se eliminan en la cuadrícula de origen no se eliminan en la cuadrícula de destino.

En la figura, **REPLY DELETE MARKERS** se estableció en **Yes** cuando "se ha activado la replicación entre grid". Las solicitudes de supresión para el bloque de origen que incluyan un identificador de versión no suprimirán los objetos del bloque de destino. Las solicitudes de supresión del depósito de origen que no incluyan un ID de versión aparecerán para suprimir objetos del depósito de destino.



Si desea mantener sincronizadas las eliminaciones de objetos entre las cuadrículas, cree las correspondientes "Configuraciones de ciclo de vida de S3" para los cucharones de ambas rejillas.

Cómo se replican los objetos cifrados

Cuando se utiliza la replicación entre grid para replicar objetos entre grids, se pueden cifrar objetos individuales, utilizar el cifrado de bucket predeterminado o configurar el cifrado de toda la grid. Puede agregar, modificar o eliminar la configuración de cifrado predeterminada de bloque o de grid antes o después de habilitar la replicación entre grid para un bloque.

Para cifrar objetos individuales, puede utilizar SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID) al agregar los objetos al depósito de origen. Utilice la `x-amz-server-side-encryption` solicitar cabecera y especificar `AES256`. Consulte "Usar cifrado del servidor".

El uso de SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente) no es compatible para la replicación entre grid. La operación de ingesta fallará.

Para utilizar el cifrado predeterminado para un depósito, utilice una solicitud de cifrado de depósito PUT y establezca el `SSEAlgorithm` parámetro a. `AES256`. El cifrado de nivel de bloque se aplica a cualquier objeto ingerido sin `x-amz-server-side-encryption` solicite el encabezado. Consulte "Operaciones en bloques".

Para utilizar el cifrado a nivel de cuadrícula, establezca la opción **cifrado de objetos almacenados** en **AES-256**. El cifrado de nivel de grid se aplica a cualquier objeto que no esté cifrado en el nivel del bloque o que se ingiera sin `x-amz-server-side-encryption` solicite el encabezado. Consulte "Configure las opciones de red y objeto".

SSE no admite AES-128. Si la opción **cifrado de objetos almacenados** está habilitada para la cuadrícula de origen mediante la opción **AES-128**, el uso del algoritmo AES-128 no se propagará al objeto replicado. En su lugar, el objeto replicado utilizará la configuración de cifrado de nivel de grid o bloque predeterminada del destino, si está disponible.

Al determinar cómo cifrar los objetos de origen, StorageGRID aplica estas reglas:

1. Utilice la `x-amz-server-side-encryption` encabezado de ingesta, si existe.
2. Si no hay una cabecera de ingesta, utilice la configuración de cifrado predeterminado de depósito, si está configurada.
3. Si no se ha configurado una configuración de depósito, utilice la configuración de cifrado de toda la cuadrícula, si está configurada.
4. Si no hay una configuración para toda la cuadrícula, no cifre el objeto de origen.

Al determinar cómo cifrar los objetos replicados, StorageGRID aplica estas reglas en este orden:

1. Use el mismo cifrado que el objeto de origen, a menos que ese objeto utilice cifrado AES-128.
2. Si el objeto de origen no está cifrado o utiliza AES-128, utilice la configuración de cifrado predeterminada del depósito de destino, si está configurada.
3. Si el depósito de destino no tiene una configuración de cifrado, utilice la configuración de cifrado de toda la cuadrícula del destino, si está configurada.
4. Si no hay una configuración de toda la cuadrícula, no cifre el objeto de destino.

No se admiten el etiquetado de objetos PUT ni el etiquetado de objetos DELETE

Las solicitudes de etiquetado de objetos PUT y DELETE no se admiten para los objetos de los bloques que tienen activada la replicación entre grid.

Si un cliente S3 emite una solicitud de etiquetado PUT Object o DELETE Object, `501 Not Implemented` se devuelve. El mensaje es `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Cómo se replican los objetos segmentados

El tamaño máximo del segmento de la cuadrícula de origen se aplica a los objetos replicados a la cuadrícula de destino. Cuando los objetos se replican en otra cuadrícula, el ajuste **Tamaño de segmento máximo** (**CONFIGURACIÓN** > **Sistema** > **Opciones de almacenamiento**) de la cuadrícula de origen se utilizará en ambas cuadrículas. Por ejemplo, supongamos que el tamaño máximo del segmento para la cuadrícula de origen es de 1 GB, mientras que el tamaño máximo del segmento de la cuadrícula de destino es de 50 MB. Si ingiere un objeto de 2 GB en la cuadrícula de origen, ese objeto se guarda como dos segmentos de 1 GB. También se replicará en la cuadrícula de destino como dos segmentos de 1 GB, aunque el tamaño máximo del segmento de esa cuadrícula sea de 50 MB.

Compare la replicación entre grid y la replicación de CloudMirror

A medida que comience a utilizar la federación de cuadrícula, revise las similitudes y diferencias entre "replicación entre grid" y la "Servicio de replicación CloudMirror de StorageGRID".

	Replicación entre grid	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Un sistema StorageGRID actúa como sistema de recuperación ante desastres. Los objetos de un depósito se pueden replicar entre las cuadrículas en una o en ambas direcciones.	Permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) a un bloque S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura de S3 independiente. Esta copia independiente no se usa como backup, pero suele procesarse en el cloud.
¿Cómo se configura?	1. Configure una conexión de federación de grid entre dos cuadrículas. 2. Agregar nuevas cuentas de inquilino, que se clonan automáticamente en el otro grid. 3. Añadir usuarios y grupos de inquilinos nuevos que también se clonan. 4. Crea los bloques correspondientes en cada grid y permite que la replicación entre grid se realice en una o en ambas direcciones.	1. Un usuario de inquilino configura la replicación de CloudMirror definiendo un extremo de CloudMirror (dirección IP, credenciales, etc.) mediante el administrador de inquilinos o la API de S3. 2. Se puede configurar cualquier bloque que pertenezca a esa cuenta de inquilino para que apunte al extremo de CloudMirror.

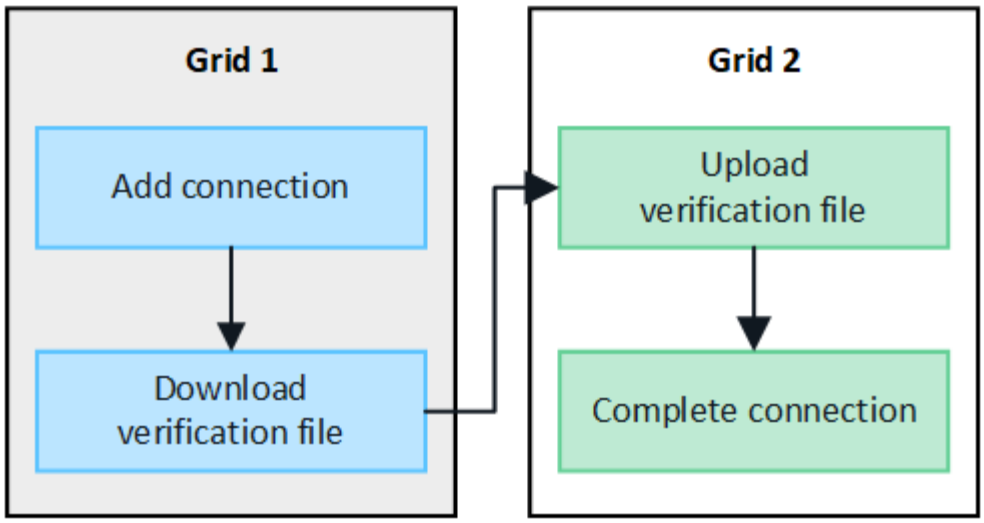
	Replicación entre grid	Servicio de replicación de CloudMirror
¿Quién es responsable de su configuración ?	• Un administrador de grid configura la conexión y los inquilinos. • Los usuarios inquilinos configuran los grupos, los usuarios, las claves y los buckets.	Normalmente, un usuario inquilino.
¿Cuál es el destino?	Un bloque de S3 correspondiente e idéntico en el otro sistema StorageGRID de la conexión de federación de grid.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • Google Cloud Platform (GCP)
¿Se requiere el control de versiones de objetos?	Sí, tanto los depósitos de origen como de destino deben tener activado el control de versiones de objetos.	No, la replicación de CloudMirror admite cualquier combinación de buckets sin versiones y con versiones tanto en el origen como en el destino.
¿Qué hace que los objetos se muevan al destino?	Los objetos se replican automáticamente cuando se añaden a un bloque que tiene habilitada la replicación entre grid.	Los objetos se replican automáticamente cuando se añaden a un bloque que se ha configurado con un extremo de CloudMirror. Los objetos que existían en el bloque de origen antes de que se configurara con el extremo de CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre grid crea objetos con versiones y replica el identificador de versión del bloque de origen al bloque de destino. Esto permite mantener el orden de versión en ambas cuadrículas.	La replicación de CloudMirror no requiere buckets habilitados para el control de versiones, por lo que CloudMirror solo puede mantener el pedido de una clave dentro de un sitio. No hay garantías de que el pedido se mantendrá para las solicitudes a un objeto en un sitio diferente.
¿Qué pasa si un objeto no se puede replicar?	El objeto se pone en cola para la replicación, sujeto a los límites de almacenamiento de metadatos.	El objeto se pone en cola para la replicación, sujeto a los límites de servicios de la plataforma (consulte "Recomendaciones para el uso de servicios de plataformas").
¿Se replican los metadatos del sistema del objeto?	Sí, cuando un objeto se replica en la otra cuadrícula, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambas cuadrículas.	No, cuando un objeto se replica en el depósito externo, sus metadatos del sistema se actualizan. Los metadatos variarán entre ubicaciones, en función del tiempo de procesamiento y del comportamiento de la infraestructura S3 independiente.

	Replicación entre grid	Servicio de replicación de CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones pueden recuperar o leer objetos mediante la realización de una solicitud al depósito en cualquier cuadrícula.	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud en StorageGRID o en el destino de S3. Por ejemplo, supongamos que usa la replicación de CloudMirror para reflejar objetos en una organización asociada. El partner puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Qué sucede si se elimina un objeto?	• Las solicitudes de supresión que incluyan un ID de versión nunca se replican en la cuadrícula de destino. • Las solicitudes de eliminación que no incluyen un ID de versión agregan un marcador de eliminación al depósito de origen, que opcionalmente se puede replicar en la cuadrícula de destino. • Si la replicación entre grid se configura para una sola dirección, los objetos del bucket de destino se pueden eliminar sin afectar al origen.	Los resultados variarán en función del estado de control de versiones de los depósitos de origen y destino (que no necesitan ser los mismos): • Si ambos cubos están versionados, una solicitud de eliminación agregará un marcador de eliminación en ambas ubicaciones. • Si sólo se ha versionado el depósito de origen, una solicitud de supresión agregará un marcador de supresión al origen pero no al destino. • Si ninguno de los depósitos está versionado, una solicitud de supresión suprimirá el objeto del origen pero no del destino. Del mismo modo, los objetos del bloque de destino se pueden eliminar sin que ello afecte al origen.

Crear conexiones de federación de grid

Puede crear una conexión de federación de grid entre dos sistemas StorageGRID si desea clonar detalles de inquilinos y replicar datos de objetos.

Como se muestra en la figura, la creación de una conexión de federación de cuadrícula incluye pasos en ambas cuadrículas. Agrega la conexión en una cuadrícula y la completa en la otra. Puede empezar desde cualquiera de las dos cuadrículas.



Antes de empezar

- Ha revisado el "consideraciones y requisitos" para configurar conexiones de federación de grid.
- Si planea utilizar nombres de dominio completos (FQDN) para cada cuadrícula en lugar de direcciones IP o VIP, sabrá qué nombres utilizar y confirmará que el servidor DNS de cada cuadrícula tiene las entradas adecuadas.
- Está utilizando un "navegador web compatible".
- Debe tener permiso de acceso raíz y la frase de acceso de aprovisionamiento para ambas cuadrículas.

Agregar conexión

Realice estos pasos en cualquiera de los dos sistemas StorageGRID.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Selecciona **Añadir conexión**.
4. Introduzca los detalles de la conexión.

Campo	Descripción
Nombre de conexión	Un nombre único para ayudarte a reconocer esta conexión, por ejemplo, “Grid 1-Grid 2”.
FQDN o IP para este grid	Uno de los siguientes: • El FQDN del grid en el que está conectado actualmente • Dirección VIP de un grupo de alta disponibilidad en esta cuadrícula • La dirección IP de un nodo de administración o un nodo de pasarela en este grid. La IP puede estar en cualquier red a la que pueda acceder la cuadrícula de destino.

Campo	Descripción
Puerto	Puerto que desea utilizar para esta conexión. Puede introducir cualquier número de puerto no utilizado del 23000 al 23999. Ambas rejillas de esta conexión utilizarán el mismo puerto. Debe asegurarse de que ningún nodo de ninguno de los grid utilice este puerto para otras conexiones.
Días válidos de certificado para esta cuadrícula	El número de días que desea que los certificados de seguridad de esta cuadrícula de la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puede introducir cualquier valor de 1 a 762 días. StorageGRID genera automáticamente certificados de cliente y de servidor para cada grid al guardar la conexión.
Aprovisionamiento de la clave de acceso para este grid	La clave de acceso de aprovisionamiento para el grid en el que ha iniciado sesión.
FQDN o IP para el otro grid	Uno de los siguientes: • El FQDN del grid al que desea conectarse • Una dirección VIP de un grupo de alta disponibilidad en la otra cuadrícula • Una dirección IP de un nodo de administración o nodo de pasarela en el otro grid. La IP puede estar en cualquier red a la que pueda acceder la red de origen.

5. Selecciona **Guardar y continuar**.
6. Para el paso Descargar archivo de verificación, seleccione **Descargar archivo de verificación**.

   Una vez completada la conexión en la otra cuadrícula, ya no podrá descargar el archivo de verificación de ninguna de las dos.

7. Busque el archivo descargado (*`connection-name`*`.grid-federation`), y guárdelo en un lugar seguro.

   > Este archivo contiene secretos (enmascarados como *****) y otros datos confidenciales y deben almacenarse y transmitirse de forma segura.

8. Selecciona **Cerrar** para volver a la página de Grid federation.
9. Confirme que se muestra la nueva conexión y que su **estado de conexión** está **esperando para conectarse**.
10. Proporcione el *`connection-name`*`.grid-federation` en el administrador de grid para el otro grid.

Conexión completa

Realice estos pasos en el sistema StorageGRID al que se está conectando (la otra cuadrícula).

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página Cargar.
4. Seleccione **Cargar archivo de verificación**. A continuación, busque y seleccione el archivo que se descargó de la primera cuadrícula (*connection-name*`.grid-federation`).

   Se muestran los detalles de la conexión.

5. Opcionalmente, introduzca un Núm. Diferente de días válidos para los certificados de seguridad de esta cuadrícula. La entrada **Certificate Valid Days** establece por defecto el valor que ingresaste en la primera cuadrícula, pero cada cuadrícula puede usar diferentes fechas de vencimiento.

   En general, utilice el mismo número de días para los certificados en ambos lados de la conexión.

   > Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones estarán pendientes hasta que se actualicen los certificados.

6. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que está conectado actualmente.
7. Seleccione **Guardar y probar**.

   Los certificados se generan y se prueba la conexión. Si la conexión es válida, aparece un mensaje de éxito y la nueva conexión se muestra en la página federación de Cuadrícula. El **Estado de conexión** será **Conectado**.

   Si aparece un mensaje de error, solucione cualquier problema. Consulte "Solucionar errores de federación de grid".

8. Vaya a la página Grid federation en la primera cuadrícula y actualice el explorador. Confirme que el **Estado de conexión** es ahora **Conectado**.
9. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

   Si edita esta conexión, se creará un nuevo archivo de verificación. No se puede volver a utilizar el archivo original.

Después de terminar

- Revise las consideraciones para "gestión de inquilinos permitidos".
- "Cree una o más cuentas de arrendatario nuevas", Asigne el permiso **Use grid federation connection** y seleccione la nueva conexión.
- "Gestionar la conexión" según sea necesario. Puede editar valores de conexión, probar una conexión, rotar certificados de conexión o eliminar una conexión.
- "Supervise la conexión" Como parte de sus actividades normales de monitoreo de StorageGRID.
- "Solucione los problemas de la conexión", incluyendo la resolución de alertas y errores relacionados con la clonación de cuentas y la replicación entre redes.

Gestionar conexiones de federación de grid

La gestión de las conexiones de federación de grid entre sistemas StorageGRID incluye editar detalles de conexión, girar los certificados, eliminar permisos de inquilinos y

eliminar conexiones que no se utilizan.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las tablas mediante un "navegador web compatible".
- Tiene el permiso de acceso root para la cuadrícula en la que ha iniciado sesión.

Edite una conexión de federación de cuadrícula

Puede editar una conexión de federación de grid iniciando sesión en el nodo de administración principal en cualquier cuadrícula de la conexión. Después de realizar cambios en la primera cuadrícula, debe descargar un nuevo archivo de verificación y cargarlo en la otra cuadrícula.

> Mientras se edita la conexión, las solicitudes de clonación de cuentas o replicación entre cuadrículas seguirán utilizando la configuración de conexión existente. Las ediciones que realice en la primera cuadrícula se guardan localmente, pero no se utilizan hasta que se hayan cargado en la segunda cuadrícula, se hayan guardado y probado.

Comience a editar la conexión

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Seleccione * NODOS * y confirme que todos los demás nodos de administración del sistema estén en línea.

   > Al editar una conexión de federación de grid, StorageGRID intenta guardar un archivo de configuración de candidato en todos los nodos de administración de la primera cuadrícula. Si este archivo no se puede guardar en todos los nodos de administración, aparecerá un mensaje de advertencia al seleccionar **Guardar y probar**.

3. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
4. Edite los detalles de la conexión utilizando el menú **Acciones** de la página de federación de cuadrícula o la página de detalles de una conexión específica. Consulte "Crear conexiones de federación de grid" para qué entrar.

   Menú Actions

   a. Seleccione el botón de opción para la conexión.
   b. Selecciona **Acciones** > **Editar**.
   c. Introduzca la nueva información.

   Detalles

   a. Seleccione un nombre de conexión para mostrar sus detalles.
   b. Seleccione **Editar**.
   c. Introduzca la nueva información.

5. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que ha iniciado sesión.
6. Selecciona **Guardar y continuar**.

Los nuevos valores se guardan, pero no se aplicarán a la conexión hasta que haya cargado el nuevo archivo de verificación en la otra cuadrícula.

7. Seleccione **Descargar archivo de verificación**.

   Para descargar este archivo más adelante, vaya a la página de detalles de la conexión.

8. Busque el archivo descargado (*connection-name*`.grid-federation`), y guárdelo en un lugar seguro.

   El archivo de verificación contiene secretos y debe almacenarse y transmitirse de forma segura.

9. Selecciona **Cerrar** para volver a la página de Grid federation.
10. Confirme que el **Estado de conexión** es **Edición pendiente**.

    Si el estado de la conexión no era **Connected** cuando comenzó a editar la conexión, no cambiará a **Pending edit**.

11. Proporcione el *connection-name*`.grid-federation` en el administrador de grid para el otro grid.

Termine de editar la conexión

Termine de editar la conexión cargando el archivo de verificación en la otra cuadrícula.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Cargar archivo de verificación**. A continuación, busque y seleccione el archivo que se descargó de la primera cuadrícula.
5. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que está conectado actualmente.
6. Seleccione **Guardar y probar**.

   Si la conexión se puede establecer mediante los valores editados, aparece un mensaje de éxito. De lo contrario, aparecerá un mensaje de error. Revise el mensaje y resuelva cualquier problema.

7. Cierre el asistente para volver a la página Grid federation.
8. Confirme que el **Estado de conexión** es **Conectado**.
9. Vaya a la página Grid federation en la primera cuadrícula y actualice el explorador. Confirme que el **Estado de conexión** es ahora **Conectado**.
10. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

Pruebe una conexión de federación de grid

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.

3. Pruebe la conexión utilizando el menú **Acciones** de la página de Grid federation o la página de detalles de una conexión específica.

   Menú Actions

   a. Seleccione el botón de opción para la conexión.

   b. Selecciona **Acciones** > **Prueba**.

   Detalles

   a. Seleccione un nombre de conexión para mostrar sus detalles.

   b. Seleccione **probar conexión**.

4. Revise el estado de conexión:

Estado de conexión	Descripción
Conectado	Ambas rejillas están conectadas y se comunican con normalidad.
Error	La conexión está en estado de error. Por ejemplo, un certificado ha caducado o un valor de configuración ya no es válido.
Edición pendiente	Ha editado la conexión en esta cuadrícula, pero la conexión sigue utilizando la configuración existente. Para completar la edición, cargue el nuevo archivo de verificación en la otra cuadrícula.
Esperando conexión	Ha configurado la conexión en esta cuadrícula, pero la conexión no se ha completado en la otra. Descargue el archivo de verificación de esta cuadrícula y cárguelo en la otra cuadrícula.
Desconocido	La conexión está en estado desconocido, posiblemente debido a un problema de red o a un nodo sin conexión.

5. Si el estado de la conexión es **Error**, resuelva cualquier problema. A continuación, seleccione **Probar conexión** de nuevo para confirmar que el problema se ha solucionado.

Girar certificados de conexión

Cada conexión de federación de grid utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados para cada cuadrícula se acercan a su fecha de vencimiento, la alerta **Caducidad del certificado de federación de cuadrícula** le recuerda que debe rotar los certificados.

> Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones estarán pendientes hasta que se actualicen los certificados.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. En cualquiera de los separadores de la página Grid federation, seleccione el nombre de la conexión para

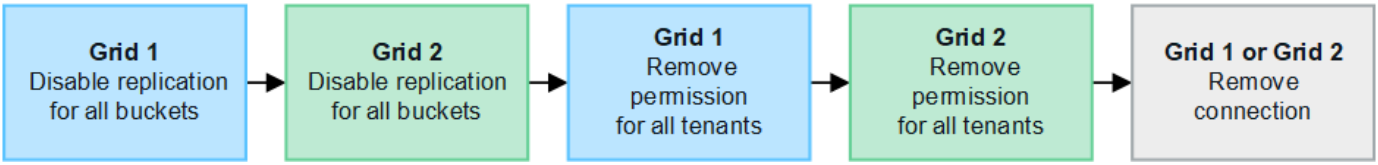
mostrar sus detalles.

4. Seleccione la ficha **certificados**.
5. Seleccione **Girar certificados**.
6. Especifique cuántos días deben ser válidos los certificados nuevos.
7. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que ha iniciado sesión.
8. Seleccione **Girar certificados**.
9. Si es necesario, repita estos pasos en la otra cuadrícula de la conexión.

   En general, utilice el mismo número de días para los certificados en ambos lados de la conexión.

Elimine una conexión de federación de cuadrícula

Puede eliminar una conexión de federación de cuadrícula de cualquiera de las dos cuadrículas de la conexión. Como se muestra en la figura, debe realizar los pasos de requisitos previos en ambas cuadrículas para confirmar que la conexión no está siendo utilizada por ningún inquilino en ninguna de las cuadrículas.



Antes de eliminar una conexión, tenga en cuenta lo siguiente:

- La eliminación de una conexión no elimina ningún elemento que ya se haya copiado entre las cuadrículas. Por ejemplo, los usuarios, grupos y objetos de arrendatarios que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del arrendatario. Si desea eliminar estos elementos, debe eliminarlos manualmente de ambas cuadrículas.
- Al eliminar una conexión, cualquier objeto que esté pendiente de replicación (ingerido pero que aún no se haya replicado en la otra cuadrícula) tendrá un fallo permanente en su replicación.

Desactive la replicación para todos los bloques de inquilinos

Pasos

1. A partir de cualquier cuadrícula, inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Arrendatarios permitidos**, determine si la conexión está siendo utilizada por algún inquilino.
5. Si se muestra algún arrendatario, indique a todos los arrendatarios que "desactive la replicación entre grid" para todos sus cucharones en ambas rejillas de la conexión.

> No puede eliminar el permiso **Usar conexión de federación de grid** si algún depósito de inquilino tiene habilitada la replicación entre grid. Cada cuenta de inquilino debe deshabilitar la replicación entre grid en sus bloques en ambos grids.

Eliminar permiso para cada inquilino

Después de que la replicación entre redes se haya desactivado para todos los depósitos de inquilinos, elimine el permiso **Usar federación de grid** de todos los inquilinos en ambas cuadrículas.

Pasos

1. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
2. Seleccione el nombre de la conexión para mostrar sus detalles.
3. Para cada inquilino en la pestaña **Arrendatarios permitidos**, elimine el permiso **Usar conexión de federación de grid** de cada inquilino. Consulte "Gestionar inquilinos permitidos".
4. Repita estos pasos para los inquilinos permitidos en la otra cuadrícula.

Retire la conexión

Pasos

1. Cuando ningún inquilino de ninguna de las dos rejillas esté usando la conexión, seleccione **Eliminar**.
2. Revise el mensaje de confirmación y seleccione **Eliminar**.
   - Si se puede eliminar la conexión, se muestra un mensaje de éxito. La conexión de federación de cuadrícula se elimina ahora de ambas cuadrículas.
   - Si la conexión no se puede eliminar (por ejemplo, aún está en uso o hay un error de conexión), se muestra un mensaje de error. Puede realizar una de las siguientes acciones:
     - Resuelva el error (recomendado). Consulte "Solucionar errores de federación de grid".
     - Retire la conexión por la fuerza. Consulte la siguiente sección.

Elimine una conexión de federación de cuadrícula por fuerza

Si es necesario, puede forzar la eliminación de una conexión que no tiene el estado **CONECTADA**.

La eliminación forzada sólo elimina la conexión de la rejilla local. Para eliminar completamente la conexión, realice los mismos pasos en ambas rejillas.

Pasos

1. En el cuadro de diálogo de confirmación, selecciona **Forzar eliminación**.

   Aparece un mensaje de éxito. Esta conexión de federación de grid ya no se puede utilizar. Sin embargo, es posible que los bloques de inquilinos aún tengan habilitada la replicación entre grid, y es posible que algunas copias de objeto ya se hayan replicado entre los grids en la conexión.

2. Desde la otra cuadrícula de la conexión, inicie sesión en Grid Manager desde el nodo de administración principal.
3. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
4. Seleccione el nombre de la conexión para mostrar sus detalles.
5. Selecciona **Eliminar** y **Sí**.
6. Seleccione **Forzar eliminación** para eliminar la conexión de esta cuadrícula.

Gestione los inquilinos permitidos para la federación de grid

Puede permitir que las nuevas cuentas de inquilino de S3 usen una conexión de

federación de grid entre dos sistemas StorageGRID. Cuando se permite a los inquilinos utilizar una conexión, se requieren pasos especiales para editar los detalles del arrendatario o para eliminar permanentemente el permiso de un arrendatario para usar la conexión.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las tablas mediante un "navegador web compatible".
- Tiene el permiso de acceso root para la cuadrícula en la que ha iniciado sesión.
- Ya tienes "se ha creado una conexión de federación de grid" entre dos cuadrículas.
- Ha revisado los flujos de trabajo para "clon de cuenta" y.. "replicación entre grid".
- Según sea necesario, ya ha configurado Single Sign-On (SSO) o Identify federation para ambas cuadrículas en la conexión. Consulte "Qué es el clon de cuenta".

Cree un inquilino permitido

Si desea permitir que una cuenta de inquilino utilice una conexión de federación de grid para el clon de cuenta y la replicación entre grid, siga las instrucciones generales a. "Cree un nuevo inquilino S3" y tenga en cuenta lo siguiente:

- Puede crear el inquilino desde cualquier cuadrícula en la conexión. La cuadrícula donde se crea un inquilino es la cuadrícula de origen del *tenant*.
- El estado de la conexión debe ser **Conectado**.
- Solo puede seleccionar el permiso **Usar conexión de federación de grid** cuando está creando un nuevo inquilino de S3; no puede habilitar este permiso cuando edita un inquilino existente.
- Cuando el nuevo inquilino se guarda en la primera cuadrícula, un inquilino idéntico se replica automáticamente en la otra cuadrícula. La cuadrícula en la que se replica el inquilino es la cuadrícula de destino del *tenant*.
- Los inquilinos de ambas cuadrículas tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puede utilizar el campo **Descripción** para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en la cuadrícula 1 también aparecerá para el inquilino replicado en la cuadrícula 2: «`Este inquilino se creó en la cuadrícula 1`».
- Por motivos de seguridad, la contraseña de un usuario raíz local no se copia en la cuadrícula de destino.

  Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la cuadrícula de destino, un administrador de grid para ese grid debe "cambie la contraseña del usuario raíz local".

- Una vez que el nuevo inquilino esté disponible en ambas cuadrículas, los usuarios inquilinos pueden realizar estas operaciones:
  - A partir del grid de origen del inquilino, cree grupos y usuarios locales que se clonan automáticamente en el grid de destino del inquilino. Consulte "Clone los usuarios y los grupos de inquilinos".
  - Crear nuevas claves de acceso S3, que se pueden clonar opcionalmente en el grid de destino del inquilino. Consulte "Clone las claves de acceso S3 mediante la API".
  - Cree depósitos idénticos en ambas cuadrículas de la conexión y habilite la replicación entre cuadrículas en una dirección o en ambas direcciones. Consulte "Gestionar la replicación entre grid".

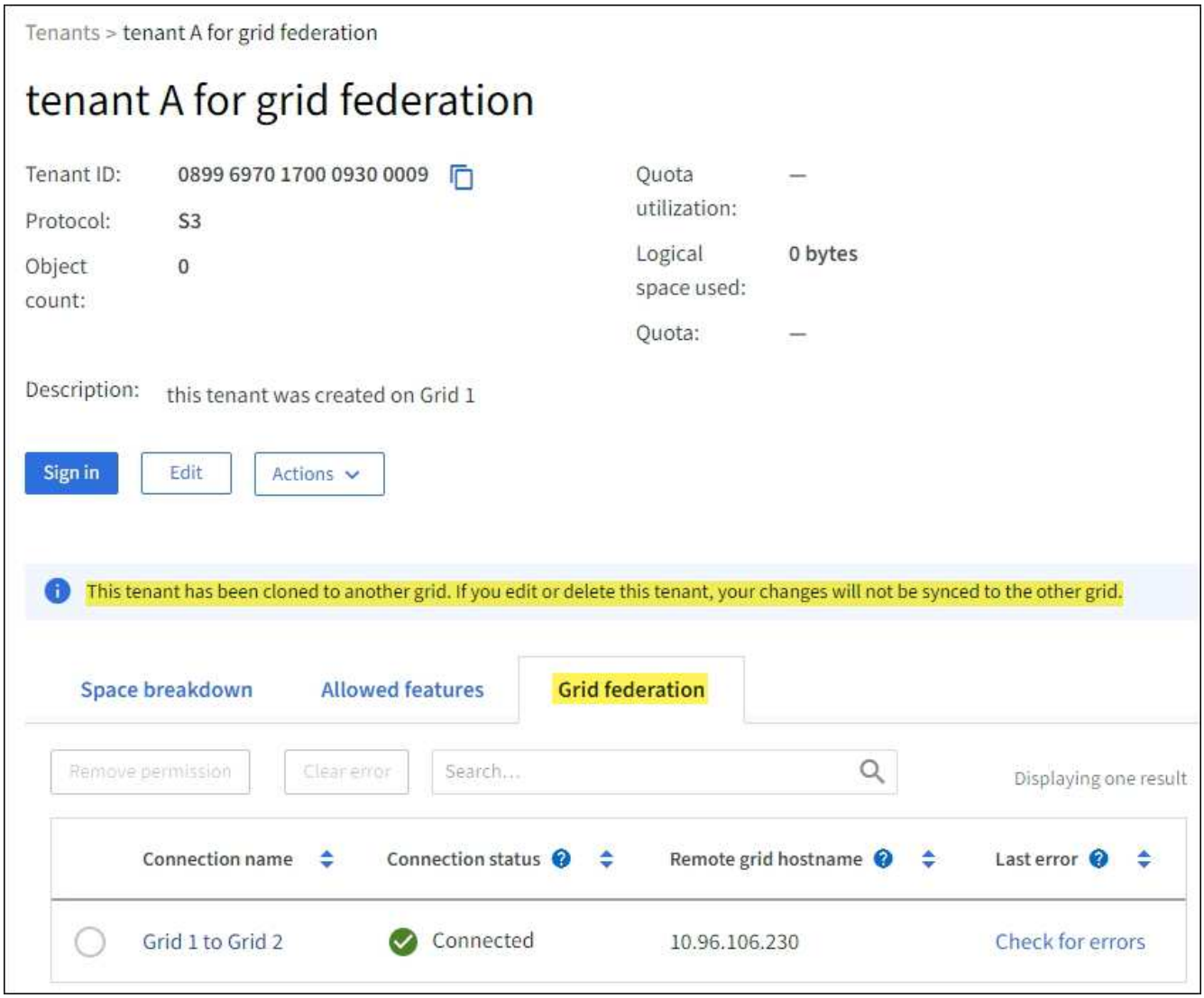
Ver un inquilino permitido

Puede ver los detalles de un inquilino con permiso para utilizar una conexión de federación de grid.

Pasos

1. Seleccione **ARRENDATARIOS**.
2. En la página Tenedores, seleccione el nombre del arrendatario para ver la página de detalles del arrendatario.

   Si se trata de la cuadrícula de origen del inquilino (es decir, si el inquilino se creó en esta cuadrícula), aparece un banner para recordarle que el inquilino se clonó en otra cuadrícula. Si edita o elimina este arrendatario, los cambios no se sincronizarán con la otra cuadrícula.



3. Opcionalmente, seleccione la pestaña **Grid federation** a. "supervise la conexión de federación de grid".

Editar un arrendatario permitido

Si necesita editar un inquilino que tiene el permiso **Usar conexión de federación de grid**, siga las instrucciones generales para "editar una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puede editar los detalles del inquilino desde cualquier cuadrícula en la conexión. Sin embargo, los cambios que realice no se copiarán

en la otra cuadrícula. Si desea mantener sincronizados los detalles del arrendatario entre las cuadrículas, debe realizar las mismas modificaciones en ambas cuadrículas.

- No puede borrar el permiso **Usar conexión de federación de grid** cuando está editando un inquilino.
- No puede seleccionar una conexión de federación de grid diferente al editar un inquilino.

Suprimir un arrendatario permitido

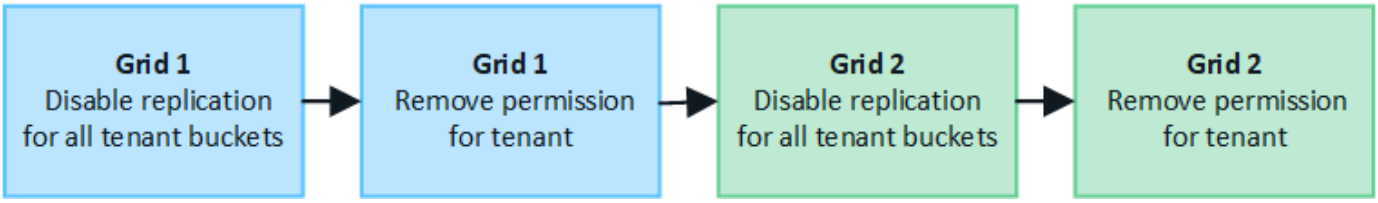
Si necesita eliminar un inquilino que tiene el permiso **Usar conexión de federación de grid**, siga las instrucciones generales para "eliminación de una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Antes de poder eliminar el arrendatario original en la cuadrícula de origen, debe eliminar todos los depósitos de la cuenta en la cuadrícula de origen.
- Para poder quitar el inquilino clonado en la cuadrícula de destino, debe eliminar todos los buckets de la cuenta de la cuadrícula de destino.
- Si quita el inquilino original o el clonado, la cuenta ya no se puede usar para la replicación entre grid.
- Si va a eliminar el inquilino original en la cuadrícula de origen, los grupos de inquilinos, usuarios o las claves que se hayan clonado en el grid de destino no se verán afectados. Puede eliminar el inquilino clonado o permitir que gestione sus propios grupos, usuarios, claves de acceso y bloques.
- Si va a quitar el inquilino clonado en la cuadrícula de destino, se producirán errores de clonado si se añaden usuarios o grupos nuevos al inquilino original.

  Para evitar estos errores, elimine el permiso del inquilino para utilizar la conexión de federación de grid antes de eliminar el inquilino de esta cuadrícula.

Eliminar el permiso de conexión Usar federación de grid

Para evitar que un inquilino utilice una conexión de federación de grid, debe eliminar el permiso **Usar conexión de federación de grid**.



Antes de eliminar el permiso de un inquilino para utilizar una conexión de federación de grid, tenga en cuenta lo siguiente:

- Eliminar el permiso **Usar conexión de federación de grid** de un inquilino es una acción permanente. No se puede volver a habilitar el permiso para este inquilino.
- No puede eliminar el permiso **Usar conexión de federación de grid** si alguno de los depósitos del inquilino tiene habilitada la replicación entre grid. La cuenta de inquilino debe deshabilitar primero la replicación entre grid en todos sus bloques.
- Eliminar el permiso **Usar conexión de federación de cuadrícula** no elimina ningún elemento que ya se haya replicado entre las cuadrículas. Por ejemplo, los usuarios, grupos y objetos de arrendatarios que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del arrendatario. Si desea eliminar estos elementos, debe eliminarlos manualmente de ambas cuadrículas.

Antes de empezar

- Está utilizando un "navegador web compatible".

- Tiene el permiso de acceso root para ambas cuadrículas.

Desactive la replicación para bloques de clientes

Como primer paso, deshabilite la replicación entre grid para todos los buckets de inquilinos.

Pasos

1. A partir de cualquier cuadrícula, inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Arrendatarios permitidos**, determine si el inquilino está usando la conexión.
5. Si el inquilino aparece en la lista, indíquele que lo haga "desactive la replicación entre grid" para todos sus cucharones en ambas rejillas de la conexión.

> No puede eliminar el permiso **Usar conexión de federación de grid** si algún depósito de inquilino tiene habilitada la replicación entre grid. El inquilino debe deshabilitar la replicación entre grid en sus buckets en ambas grids.

Eliminar permiso para arrendatario

Una vez deshabilitada la replicación entre grid para bloques de inquilinos, puede eliminar el permiso del inquilino para utilizar la conexión de federación de grid.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Elimine el permiso de las páginas Grid federation o Tenants.

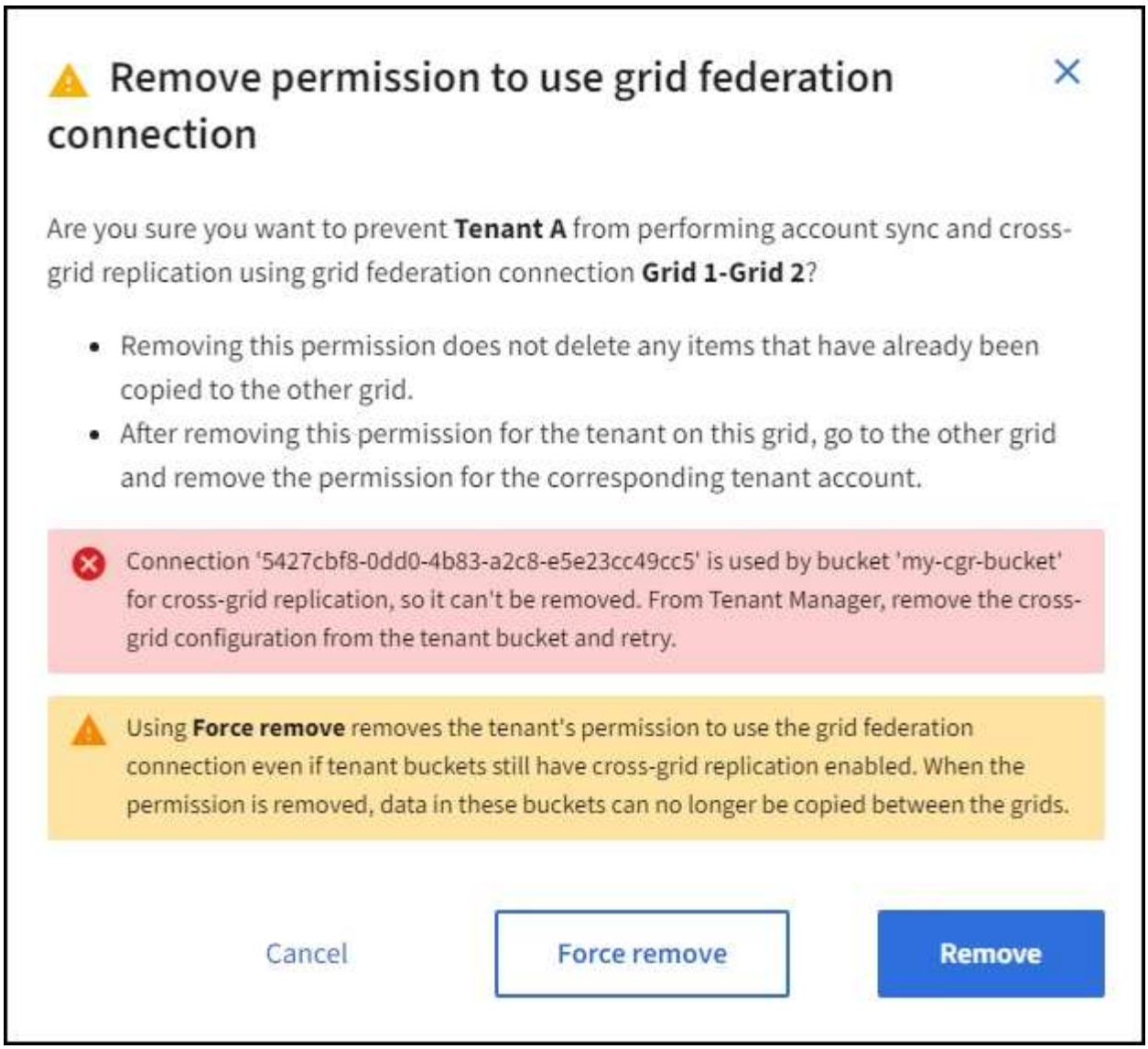
Página de federación de grid

a. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
b. Seleccione el nombre de la conexión para mostrar su página de detalles.
c. En la pestaña **Arrendatarios permitidos**, seleccione el botón de radio para el inquilino.
d. Selecciona **Eliminar permiso**.

Inquilinos

a. Seleccione **ARRENDATARIOS**.
b. Seleccione el nombre del arrendatario para mostrar la página de detalles.
c. En la pestaña **Grid federation**, seleccione el botón de radio para la conexión.
d. Selecciona **Eliminar permiso**.

3. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Eliminar**.
   - Si el permiso se puede eliminar, volverá a la página de detalles y aparecerá un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.
   - Si uno o más bloques de inquilinos aún tienen habilitada la replicación entre grid, se muestra un error.



Puede realizar una de las siguientes acciones:

- (Recomendado). Inicie sesión en el Gestor de inquilinos y deshabilite la replicación para cada uno de los buckets del inquilino. Consulte "Gestionar la replicación entre grid". Luego, repita los pasos para eliminar el permiso **Usar conexión a la cuadrícula**.
- Elimine el permiso por la fuerza. Consulte la siguiente sección.

4. Vaya a la otra cuadrícula y repita estos pasos para eliminar el permiso para el mismo inquilino en la otra cuadrícula.

Elimine el permiso por la fuerza

Si es necesario, puede forzar la eliminación del permiso de un inquilino para utilizar una conexión de federación de grid incluso si los buckets de inquilinos tienen habilitada la replicación entre grid.

Antes de eliminar el permiso de un inquilino por la fuerza, tenga en cuenta las consideraciones generales para eliminando el permiso así como estas consideraciones adicionales:

- Si elimina el permiso **Usar conexión de federación de grid** por fuerza, cualquier objeto que esté pendiente de replicación en la otra cuadrícula (ingerido pero no replicado aún) seguirá siendo replicado. Para evitar que estos objetos en curso lleguen al depósito de destino, también debe eliminar el permiso

del inquilino en la otra cuadrícula.

- Cualquier objeto ingerido en el depósito de origen después de eliminar el permiso **Usar conexión de federación de grid** nunca se replicará en el depósito de destino.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione el nombre de la conexión para mostrar su página de detalles.
4. En la pestaña **Arrendatarios permitidos**, seleccione el botón de radio para el inquilino.
5. Selecciona **Eliminar permiso**.
6. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Forzar eliminación**.

   Aparece un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.

7. Según sea necesario, vaya a la otra cuadrícula y repita estos pasos para forzar la eliminación del permiso para la misma cuenta de inquilino en la otra cuadrícula. Por ejemplo, debe repetir estos pasos en la otra cuadrícula para evitar que los objetos en curso lleguen al depósito de destino.

Solucionar errores de federación de grid

Es posible que deba solucionar alertas y errores relacionados con las conexiones de federación de grid, el clon de cuenta y la replicación entre grid.

Alertas y errores de conexión de federación de grid

Es posible que reciba alertas o se produzcan errores con las conexiones de federación de grid.

Después de realizar cualquier cambio para resolver un problema de conexión, pruebe la conexión para asegurarse de que el estado de la conexión vuelva a **CONECTADA**. Para ver instrucciones, consulte "Gestionar conexiones de federación de grid".

Alerta de fallo de conexión de federación de grid

Problema

Se ha activado la alerta de error de conexión **Grid federation**.

Detalles

Esta alerta indica que la conexión de federación de rejilla entre las cuadrículas no funciona.

Acciones recomendadas

1. Revise la configuración en la página Grid Federation para ambas cuadrículas. Confirme que todos los valores son correctos. Consulte "Gestionar conexiones de federación de grid".
2. Revise los certificados utilizados para la conexión. Asegúrese de que no haya alertas para los certificados de federación de grid vencidos y que los detalles de cada certificado sean válidos. Consulte las instrucciones para girar los certificados de conexión en "Gestionar conexiones de federación de grid".
3. Confirme que todos los nodos ADMIN y Gateway de ambas cuadrículas están en línea y disponibles. Resuelva las alertas que puedan estar afectando a estos nodos y vuelva a intentarlo.
4. Si proporcionó un nombre de dominio completo (FQDN) para la cuadrícula local o remota, confirme que el servidor DNS esté en línea y disponible. Consulte "¿Qué es GRID federation?" Para los requisitos de

redes, dirección IP y DNS.

La alerta de caducidad del certificado de federación de grid

Problema

Se activó la alerta **Expiración del certificado de federación de red**.

Detalles

Esta alerta indica que uno o más certificados de federación de grid están a punto de caducar.

Acciones recomendadas

Consulte las instrucciones para girar los certificados de conexión en "Gestionar conexiones de federación de grid".

Error al editar una conexión de federación de cuadrícula

Problema

Al editar una conexión de federación de grid, aparece el siguiente mensaje de advertencia cuando selecciona **Guardar y probar**: “No se pudo crear un archivo de configuración de candidato en uno o más nodos”.

Detalles

Cuando edita una conexión de federación de grid, StorageGRID intenta guardar un archivo de configuración de candidato en todos los nodos de administración de la primera cuadrícula. Aparece un mensaje de advertencia si este archivo no se puede guardar en todos los nodos de administración, por ejemplo, porque un nodo de administración está fuera de línea.

Acciones recomendadas

1. En la cuadrícula que está utilizando para editar la conexión, seleccione * NODOS *.
2. Confirmar que todos los nodos de administración de ese grid están en línea.
3. Si alguno de los nodos está sin conexión, vuelva a conectarlo e intente editar nuevamente la conexión.

Errores de clonación de cuenta

No se puede iniciar sesión en una cuenta de inquilino clonada

Problema

No puede iniciar sesión en una cuenta de inquilino clonada. El mensaje de error en la página de inicio de sesión del Gestor de inquilinos es «`Sus credenciales para esta cuenta no son válidas. Por favor, inténtelo de nuevo.`”

Detalles

Por motivos de seguridad, cuando se clona una cuenta de inquilino desde la cuadrícula de origen del inquilino a la cuadrícula de destino del inquilino, la contraseña que configuró para el usuario raíz local del inquilino no se clona. De la misma forma, cuando un inquilino crea usuarios locales en su grid de origen, las contraseñas de usuario local no se clonan en el grid de destino.

Acciones recomendadas

Antes de que el usuario raíz pueda iniciar sesión en la cuadrícula de destino del inquilino, primero debe hacerlo un administrador de grid "cambie la contraseña del usuario raíz local" en la cuadrícula de destino.

Para que un usuario local clonado pueda iniciar sesión en la cuadrícula de destino del inquilino, el usuario raíz del inquilino clonado debe agregar una contraseña para el usuario en la cuadrícula de destino. Para ver

instrucciones, consulte "Gestionar usuarios locales" En las instrucciones de uso del Gestor de inquilinos.

Inquilino creado sin un clon

Problema

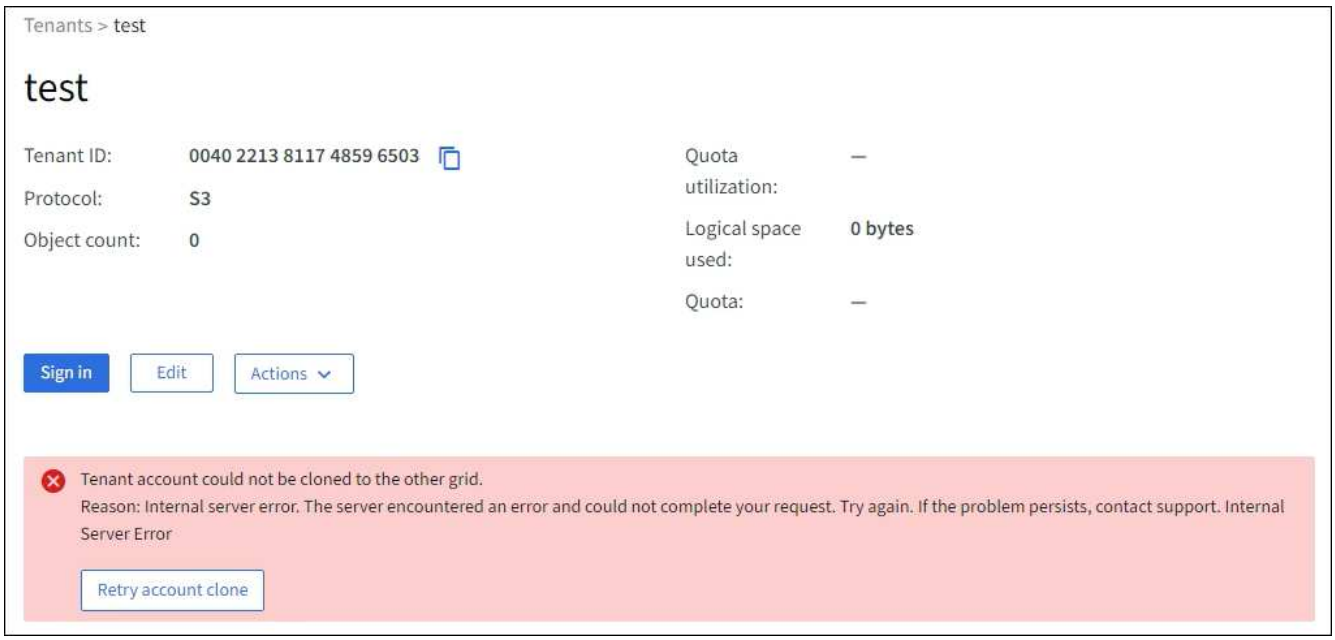
Usted ve el mensaje "`Tenant created without a clone`" después de crear un nuevo inquilino con el permiso **use grid federation connection**.

Detalles

Este problema puede ocurrir si las actualizaciones del estado de conexión se retrasan, lo que podría provocar que una conexión no saludable se listara como **Connected**.

Acciones recomendadas

1. Revise el motivo que aparece en el mensaje de error y resuelva cualquier problema de red u otros problemas que puedan impedir el funcionamiento de la conexión. Consulte Alertas y errores de conexión de federación de grid.
2. Siga las instrucciones para probar una conexión de federación de rejilla en "Gestionar conexiones de federación de grid" para confirmar que se ha solucionado el problema.
3. Desde la cuadrícula de origen del inquilino, seleccione **TENANTS**.
4. Localice la cuenta de inquilino que no se pudo clonar.
5. Seleccione el nombre del arrendatario para mostrar la página de detalles.
6. Seleccione **Reintentar clon de cuenta**.



Si se ha resuelto el error, la cuenta de inquilino se clonará ahora en la otra cuadrícula.

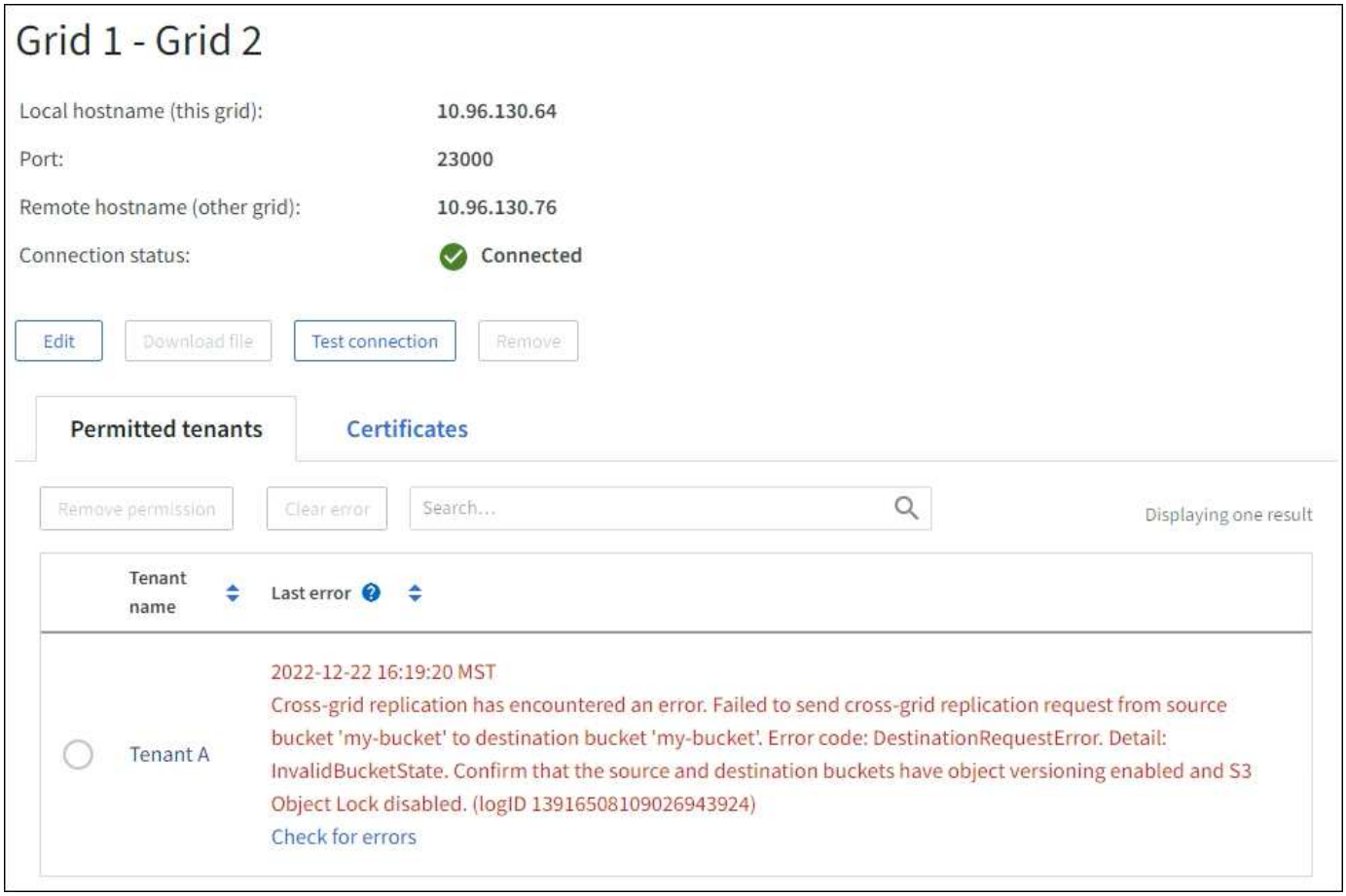
Alertas y errores de replicación entre grid

Último error mostrado para conexión o arrendatario

Problema

Cuando "visualización de una conexión de federación de grid" (o cuando "gestión de los inquilinos permitidos" Para una conexión), usted nota un error en la columna **Último error** en la página de detalles de la conexión.

Por ejemplo:



Detalles

Para cada conexión de federación de grid, la columna **last error** muestra el error más reciente que se producirá, si lo hubiera, cuando los datos de un inquilino se estaban replicando en la otra cuadrícula. Esta columna solo muestra el último error de replicación entre cuadrículas que se produce; no se mostrarán los errores anteriores que podrían haberse producido. Un error en esta columna puede ocurrir por uno de estos motivos:

- No se ha encontrado la versión del objeto de origen.
- No se ha encontrado el depósito de origen.
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.

Acciones recomendadas

Si aparece un mensaje de error en la columna **Último error**, siga estos pasos:

1. Revise el texto del mensaje.
2. Realice las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bloque de destino para la replicación entre grid, vuelva a habilitar el control de versiones para ese bloque.
3. Seleccione la conexión o la cuenta de inquilino de la tabla.

4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

> Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

> Después de borrar el error, puede aparecer un nuevo **last error** si los objetos se ingieren en un depósito diferente que también tiene un error.

7. Para determinar si se ha producido un error en la replicación de algún objeto debido al error de depósito, consulte "Identifique y vuelva a intentar operaciones de replicación fallidas".

Alerta de error permanente de replicación entre grid

Problema

Se activó la alerta de error permanente de replicación cruzada de la red*.

Detalles

Esta alerta indica que los objetos de arrendatario no se pueden replicar entre los buckets de dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlos. Esta alerta suele deberse a un cambio en el depósito de origen o de destino.

Acciones recomendadas

1. Inicie sesión en la cuadrícula donde se activó la alerta.
2. Vaya a **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula** y localice el nombre de la conexión que aparece en la alerta.
3. En la pestaña de inquilinos permitidos, mire la columna **Último error** para determinar qué cuentas de inquilino tienen errores.
4. Para obtener más información sobre el fallo, consulte las instrucciones en "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre cuadrículas.
5. Para cada cuenta de inquilino afectada:
   a. Consulte las instrucciones en "Supervise la actividad de los inquilinos" para confirmar que el inquilino no ha superado su cuota en la cuadrícula de destino para la replicación entre grid.
   b. Según sea necesario, aumente la cuota del inquilino en la cuadrícula de destino para permitir guardar nuevos objetos.
6. Para cada inquilino afectado, inicie sesión en el Gestor de inquilinos en ambas cuadrículas, de modo que pueda comparar la lista de bloques.
7. Para cada bloque que tiene habilitada la replicación entre grid, confirme lo siguiente:
   - Hay un depósito correspondiente para el mismo inquilino en la otra cuadrícula (debe usar el nombre exacto).
   - Ambos cubos tienen activado el control de versiones de objetos (el control de versiones no se puede suspender en ninguna cuadrícula).
   - Ambos cubos tienen S3 Object Lock desactivado.
   - Ninguno de los depósitos está en el estado **Deleting objects: Read-only**.

8. Para confirmar que el problema se ha resuelto, consulte las instrucciones de "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre cuadrículas, o realice los siguientes pasos:

   a. Vuelva a la página Grid federation.
   b. Seleccione el inquilino afectado y seleccione **Borrar error** en la columna **Último error**.
   c. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
   d. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

   > Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

   > Puede que la alerta tarde hasta un día en borrarse una vez que se resuelve.

   a. Vaya a. "Identifique y vuelva a intentar operaciones de replicación fallidas" para identificar objetos o eliminar marcadores que no se han podido replicar en la otra cuadrícula y volver a intentar la replicación según sea necesario.

Alerta no disponible del recurso de replicación entre grid

Problema

Se activó la alerta **Cross-grid replication resource unavailable**.

Detalles

Esta alerta indica que las solicitudes de replicación entre grid están pendientes porque un recurso no está disponible. Por ejemplo, puede haber un error de red.

Acciones recomendadas

1. Supervise la alerta para ver si el problema se resuelve por sí solo.
2. Si el problema persiste, determine si cualquiera de las redes tiene una alerta de **Error de conexión de federación de red** para la misma conexión o una alerta de **No se puede comunicar con el nodo** para un nodo. Es posible que esta alerta se resuelva al resolver esas alertas.
3. Para obtener más información sobre el fallo, consulte las instrucciones en "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre cuadrículas.
4. Si no puede resolver la alerta, póngase en contacto con el soporte técnico.

La replicación entre cuadrículas continuará con normalidad una vez resuelto el problema.

Identifique y vuelva a intentar operaciones de replicación fallidas

Después de resolver la alerta de error permanente * de replicación entre redes, debe determinar si algún objeto o marcador de borrado no se pudo replicar en la otra cuadrícula. A continuación, puede volver a ingerir estos objetos o utilizar la API de administración de grid para volver a intentar la replicación.

La alerta de error permanente * de replicación cruzada de la red indica que los objetos del inquilino no se pueden replicar entre los depósitos en dos cuadrículas por una razón que requiere la intervención del usuario para resolverlos. Esta alerta suele deberse a un cambio en el depósito de origen o de destino. Para obtener

más información, consulte "Solucionar errores de federación de grid".

Determine si se ha producido un fallo en la replicación de algún objeto

Para determinar si algún objeto o marcador de borrado no se ha replicado en la otra cuadrícula, puede buscar en el registro de auditoría "CGRR (Solicitud de Replicación entre Grid)" mensajes. Este mensaje se agrega al registro cuando StorageGRID no puede replicar un objeto, un objeto multiparte o un marcador de eliminación en el bloque de destino.

Puede utilizar el "herramienta audit-explain" para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tiene permiso de acceso raíz.
- Usted tiene la `Passwords.txt` archivo.
- Conoce la dirección IP del nodo de administración principal.

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. Busque en audit.log mensajes CGRR y utilice la herramienta audit-explain para dar formato a los resultados.

   Por ejemplo, este comando greps para todos los mensajes CGRR en los últimos 30 minutos y utiliza la herramienta audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
   print }' audit.log | grep CGRR | audit-explain
   ```

Los resultados del comando se parecerán a este ejemplo, que tiene entradas para seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre grid devolvieron un error general porque el objeto no se pudo replicar. Los tres primeros errores son para las operaciones de «objeto de réplica», y los tres últimos errores son para las operaciones de «marcador de borrado de réplica».

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Cada entrada contiene la siguiente información:

Campo	Descripción
Solicitud de Replicación de Cuadrícula Cruzada de CGRR	Nombre de la solicitud
inquilino	El ID de cuenta del inquilino
conexión	El ID de la conexión de federación de grid
funcionamiento	Tipo de operación de replicación que se intentó: • replicar objeto • replicar marcador de borrado • replicar objeto de varias partes
cucharón	El nombre del cubo
objeto	El nombre del objeto
versión	El ID de versión del objeto

Campo	Descripción
error	Tipo de error. Si se produce un error en la replicación entre cuadrículas, el error es Error general.

Vuelva a intentar las replicaciones fallidas

Después de generar una lista de objetos y de eliminar marcadores que no se han replicado en el depósito de destino y resolver los problemas subyacentes, puede volver a intentar la replicación de una de las dos formas siguientes:

- Vuelva a ingerir cada objeto en el bloque de origen.
- Utilice la API privada de Grid Management, tal y como se describe.

Pasos

1. En la parte superior de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de API**.
2. Seleccione **Ir a documentación privada de API**.

   Los puntos finales de la API de StorageGRID que están marcados como “Privados” están sujetos a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

3. En la sección **cross-grid-replication-advanced**, seleccione el siguiente punto final:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Seleccione **probar**.
5. En el cuadro de texto **body**, reemplace la entrada de ejemplo para **versionID** por un ID de versión del audit.log que corresponda a una solicitud fallida de replicación cruzada.

   Asegúrese de conservar las comillas dobles alrededor de la cadena.

6. Seleccione **Ejecutar**.
7. Confirme que el código de respuesta del servidor es **204**, lo que indica que el objeto o marcador de borrado se ha marcado como pendiente para la replicación de cuadrícula cruzada a la otra cuadrícula.

   Pendiente significa que la solicitud de replicación entre grid se ha agregado a la cola interna para su procesamiento.

Supervisar reintentos de replicación

Debe supervisar las operaciones de reintento de replicación para asegurarse de que se completen.

Puede que un objeto o marcador de eliminación tarde varias horas o más en la otra cuadrícula.

Es posible supervisar las operaciones de reintento de dos maneras:

- Utilice un S3 "OBJETO HEAD" o. "OBTENER objeto" solicitud. La respuesta incluye los recursos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **ÉXITO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

- Utilice la API privada de Grid Management, tal y como se describe.

Pasos

1. En la sección **cross-grid-replication-advanced** de la documentación de la API privada, seleccione el siguiente punto final:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Seleccione **probar**.
3. En la sección Parámetro, introduzca el ID de versión que utilizó en el `cross-grid-replication-retry-failed` solicitud.
4. Seleccione **Ejecutar**.
5. Confirme que el código de respuesta del servidor es **200**.
6. Revise el estado de replicación, que será uno de los siguientes:
   - **PENDIENTE**: El objeto aún no ha sido replicado.
   - **COMPLETADO**: La replicación fue exitosa.
   - **ERROR**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.

Gestionar la seguridad

Gestionar la seguridad: Información general

Puede configurar varias opciones de seguridad desde Grid Manager para ayudar a proteger el sistema StorageGRID.

Gestione el cifrado

StorageGRID ofrece varias opciones para el cifrado de datos. Usted debe "revise los métodos de cifrado disponibles" para determinar cuáles satisfacen sus requisitos de protección de datos.

Gestionar certificados

Puede hacerlo "configurar y gestionar los certificados de servidor" Se utiliza para las conexiones HTTP o los certificados de cliente utilizados para autenticar una identidad de cliente o usuario en el servidor.

Configuración de servidores de gestión de claves

Utilizar un "servidor de gestión de claves" Le permite proteger los datos de StorageGRID incluso si se ha quitado un dispositivo del centro de datos. Una vez que se han cifrado los volúmenes del dispositivo, no podrá

acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el KMS.

> Para utilizar la administración de claves de cifrado, debe activar el ajuste **cifrado de nodos** para cada dispositivo durante la instalación, antes de agregar el dispositivo a la cuadrícula.

Administrar la configuración de proxy

Si utiliza servicios de plataforma S3 o pools de almacenamiento en la nube, puede configurar un "Servidor proxy de almacenamiento" Entre los nodos de almacenamiento y los extremos externos de S3. Si envía mensajes de AutoSupport con HTTPS o HTTP, puede configurar un "Servidor proxy de administración" Entre los nodos de administración y el soporte técnico.

Controle los firewalls

Para mejorar la seguridad de su sistema, puede controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en la "firewall externo". También es posible controlar el acceso de la red a cada nodo configurando su "firewall interno". Puede evitar el acceso a todos los puertos, excepto a los necesarios para la implementación.

Consulte los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para el cifrado de 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	Usted "configurar un servidor de gestión de claves" Para el sitio de StorageGRID y. "habilite 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. La gestión de claves de cifrado con un KMS solo es compatible con los nodos de almacenamiento y los dispositivos de servicio.

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 SG5700 o SG6000, es posible usar "System Manager de SANtricity" para crear y gestionar la clave de seguridad. Se requiere la clave para acceder a los datos en las unidades seguras.	Los dispositivos de almacenamiento que tienen unidades de cifrado de disco completo (FDE) o FIPS. Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. No se puede usar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio.
Cifrado de objetos almacenados	Puede activar el "Cifrado de objetos almacenados" En Grid Manager. Cuando se habilita, todos los objetos nuevos que no se cifren a nivel de bucket o de objeto se cifran durante la ingesta.	Datos de objetos S3 y Swift recientemente procesados. Los objetos almacenados existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.
Cifrado de bloques de S3	Se emite una solicitud DE cifrado PUT Bucket para habilitar el cifrado en el bloque. Todos los objetos nuevos que no se cifren en el nivel de objeto se cifran durante la ingesta.	Solo datos de objetos S3 procesados recientemente. Debe especificarse el cifrado para el bloque. Los objetos de cubo existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en bloques"
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 los objetos y otros datos confidenciales no están cifrados. StorageGRID gestiona las claves. "Usar cifrado del servidor"

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 los objetos y otros datos confidenciales no están cifrados. Las claves se gestionan fuera de StorageGRID. "Usar cifrado del servidor"
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"

Utilice varios métodos de cifrado

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

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

Gestionar certificados

Gestionar certificados de seguridad: Información general

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

StorageGRID utiliza dos tipos de certificados de seguridad:

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

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

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

Certificado de CA de cuadrícula predeterminado

StorageGRID incluye una entidad de certificación (CA) integrada que genera un certificado de CA de grid interno durante la instalación del sistema. El certificado de CA de cuadrícula se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una entidad de certificación externa (CA) puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de su empresa. Aunque se puede utilizar el certificado de CA de cuadrícula para un entorno que no sea de producción, la práctica recomendada para un entorno de producción es utilizar certificados personalizados firmados por una entidad de certificación externa. También se admiten conexiones no seguras sin certificado, pero no se recomienda.

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

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

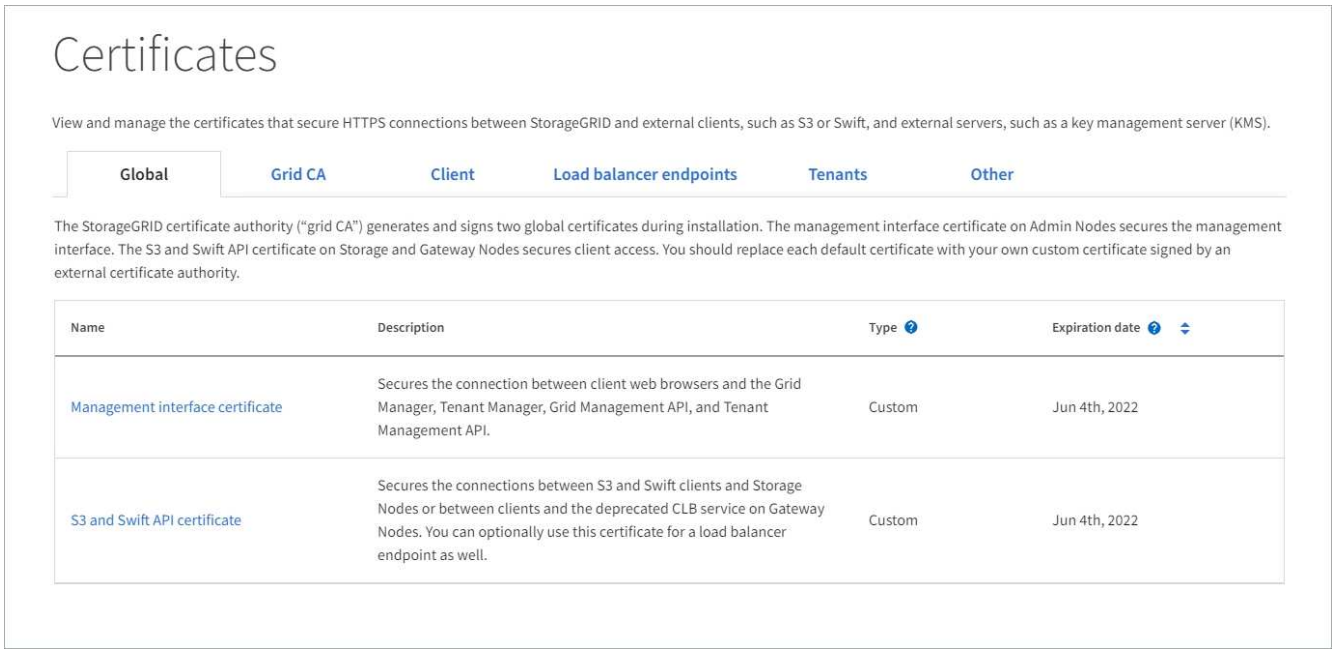
Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Es necesario tener preparados todos los certificados necesarios para la configuración específica de StorageGRID antes de configurar el sistema.

Acceda a los certificados de seguridad

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

Pasos

1. En Grid Manager, selecciona **CONFIGURACIÓN** > **Seguridad** > **Certificados**.



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

   - **Global**: Protege el acceso a StorageGRID desde navegadores web y clientes API externos.
   - **Grid CA**: Protege el tráfico interno de StorageGRID.
   - **Cliente**: Protege las conexiones entre clientes externos y la base de datos Prometheus de StorageGRID.
   - **Puntos finales del equilibrador de carga**: Protege las conexiones entre los clientes S3 y Swift y el equilibrador de carga StorageGRID.
   - **Arrendatarios**: Protege las conexiones a servidores de federación de identidades o desde extremos de servicio de plataforma a recursos de almacenamiento S3.
   - **Otros**: Protege las conexiones StorageGRID que requieren certificados específicos.

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

Global

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

- Certificado de interfaz de gestión: Protege las conexiones del explorador Web cliente a las interfaces de administración de StorageGRID.
- Certificado API S3 y Swift: Protege las conexiones API de cliente a los nodos de almacenamiento, los nodos de administración y los nodos de puerta de enlace, que las aplicaciones de cliente S3 y Swift utilizan para cargar y descargar datos de objetos.

Entre la información sobre los certificados globales instalados se incluyen:

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

Podrá:

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

CA de grid

La Certificado de CA de grid, Generado por la autoridad de certificación StorageGRID durante la instalación de StorageGRID, protege todo el tráfico interno de StorageGRID.

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

Puede hacerlo "Copie o descargue el certificado de Grid CA", pero no se puede cambiar.

Cliente

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

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

Podrá:

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

Puntos finales del equilibrador de carga

Certificados de punto final de equilibrador de carga Proteja las conexiones entre los clientes S3 y Swift y el servicio de equilibrador de carga de StorageGRID en los nodos de pasarela y los nodos de administración.

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

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

Podrá:

- "Ver un punto final de equilibrio de carga", incluyendo sus detalles de certificado.
- "Especifique un certificado de extremo de equilibrio de carga para FabricPool."
- "Use el certificado global de la API de S3 y Swift" en lugar de generar un nuevo certificado de extremo de equilibrio de carga.

Clientes

Los inquilinos pueden usar certificados de servidor de federación de identidades o. certificados de extremo de servicio de plataforma Para asegurar sus conexiones con StorageGRID.

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

Podrá:

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

Otros

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

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

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

> Solo puede ver y acceder a la información de otros certificados si dispone del permiso correspondiente.

Podrá:

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

Detalles del certificado de seguridad

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

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	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 predeterminado creado durante la instalación o cargar un certificado personalizado.	**CONFIGURACIÓN** > **Seguridad** > **certificados**, seleccione la ficha **Global** y, a continuación, seleccione **Certificado de interfaz de administración**	"Configure los certificados de interfaz de gestión"

Certificado API S3 y Swift

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica conexiones de cliente S3 o Swift seguras a un nodo de almacenamiento y a extremos de balanceador de carga (opcional).	**CONFIGURATION** > **Security** > **Certificates**, seleccione la ficha **Global** y, a continuación, seleccione **S3 y Swift API Certificate**	"Configure los certificados API S3 y Swift"

Certificado de CA de grid

Consulte Descripción de certificado de CA de cuadrícula predeterminada.

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos. • 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** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**	"Configurar certificados de cliente"

Certificado de punto final de equilibrador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre clientes S3 o Swift y el servicio StorageGRID Load Balancer en nodos de puerta de enlace y nodos de administrador. Puede cargar o generar un certificado de equilibrador de carga al configurar un extremo de equilibrador de carga. Las aplicaciones cliente utilizan el certificado de equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objeto. También puede utilizar una versión personalizada del global Certificado API S3 y Swift Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar las conexiones del equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada punto final del equilibrador de carga. **Nota:** el certificado utilizado para la autenticación del equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.	**CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**	• "Configurar puntos finales del equilibrador de carga" • "Cree un extremo de equilibrador de carga para FabricPool"

Certificado de extremo de Cloud Storage Pool

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

Certificado de notificación de alertas por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	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**	"Configure notificaciones por correo electrónico para las alertas"

Certificado de servidor de syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID. **Nota:** no se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	**CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog** y, a continuación, seleccione **Configurar servidor de syslog externo**	"Configure un servidor de syslog externo"

Certificado de conexión de la federación de cuadrícula

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema de StorageGRID actual y otro grid en una conexión de federación de grid.	**CONFIGURACIÓN** > **Sistema** > **Grid federation**	• "Crear conexiones de federación de grid" • "Rotar certificados de conexión"

Certificado de federación de identidades

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

Certificado de servidor de gestión de claves (KMS)

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

Certificado de extremo de servicios de plataforma

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

Certificado de inicio de sesión único (SSO)

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

Ejemplos de certificados

Ejemplo 1: Servicio de equilibrador de carga

En este ejemplo, StorageGRID actúa como servidor.

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

HTTPS.

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

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

En este ejemplo, StorageGRID actúa como cliente.

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

Configurar certificados de servidor

Tipos de certificado de servidor admitidos

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

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

Para obtener más información sobre cómo StorageGRID protege las conexiones del cliente para la API de REST, consulte "Configure la seguridad para la API de REST DE S3" o. "Configure la seguridad de la API de REST DE Swift".

Configure los certificados de interfaz de gestión

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

Acerca de esta tarea

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

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

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

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

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

- El certificado de la interfaz de gestión personalizada caduca.
- Usted revertir de un certificado de interfaz de gestión personalizado al certificado de servidor predeterminado.

Añada un certificado de interfaz de gestión personalizado

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

Pasos

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

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

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

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

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

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

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

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

  Por ejemplo: `storagegrid_certificate.pem`

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

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

Generar certificado

Genere los archivos de certificado de servidor.

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

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

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

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

c. Seleccione **generar**.

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

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

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

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

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

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

Restaure el certificado de interfaz de gestión predeterminado

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

Pasos

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

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

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

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

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

Antes de empezar

- Tiene permisos de acceso específicos.
- Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

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

Pasos

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

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

3. Configure StorageGRID con un certificado autofirmado nuevo.

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

   - Para `--domains`, Utilice comodines para representar los nombres de dominio completos de todos los nodos Admin. Por ejemplo: `*.ui.storagegrid.example.com` utiliza el comodín * que se va a representar `admin1.ui.storagegrid.example.com` y.. `admin2.ui.storagegrid.example.com`.

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

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

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

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

4. Seleccione y copie el certificado.

   Incluya las etiquetas INICIAL Y FINAL en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`
6. Confirme que se configuró el certificado:
   a. Acceda a Grid Manager.
   b. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**
   c. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
7. Configure el cliente de administración para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Descargue o copie el certificado de la interfaz de gestión

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

Pasos

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

Descargue el archivo de certificado o el paquete de CA

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

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

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

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

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados API S3 y Swift

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

Acerca de esta tarea

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

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

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

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

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

Añada un certificado API de S3 y Swift personalizado

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.
b. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (codificado con PEM).
   - **Clave privada de certificado**: Archivo de clave privada de certificado de servidor personalizado (`.key`).

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

   - **Paquete CA**: Un único archivo opcional que contiene los certificados de cada autoridad de certificación de emisión intermedia. El archivo debe contener cada uno de los archivos de certificado de CA codificados con PEM, concatenados en el orden de la cadena de certificados.
c. Seleccione los detalles del certificado para mostrar los metadatos y PEM de cada certificado API de S3 y Swift personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.
   - Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

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

     Por ejemplo: `storagegrid_certificate.pem`

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

   El certificado de servidor personalizado se usa para conexiones posteriores de clientes S3 y Swift.

Generar certificado

Genere los archivos de certificado de servidor.

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

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

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

c. Seleccione **generar**.

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

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

e. Seleccione **Guardar**.

   El certificado de servidor personalizado se usa para conexiones posteriores de clientes S3 y Swift.

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

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

6. Actualice la página para garantizar que se actualice el explorador web.
7. Después de añadir un certificado de API personalizado de S3 y Swift, la página de certificados de la API

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

Restaure el certificado API S3 y Swift predeterminado

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

Pasos

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

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

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

   Si tiene permiso de acceso raíz y se utilizó el certificado de API Swift y S3 personalizado para conexiones de extremos de equilibrio de carga, se muestra una lista de extremos de equilibrio de carga que ya no se podrán acceder mediante el certificado API predeterminado S3 y Swift. Vaya a. "Configurar puntos finales del equilibrador de carga" para editar o eliminar los puntos finales afectados.

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

Descargue o copie el certificado de la API S3 y Swift

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

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

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

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

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

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- "USE LA API DE REST DE S3"
- "Use la API DE REST de Swift"
- "Configure los nombres de dominio de punto final S3"

Copie el certificado de la CA de cuadrícula

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

Antes de empezar

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

Acerca de esta tarea

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **CA** de cuadrícula.
2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado `.pem` archivo.

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

   Por ejemplo: `storagegrid_certificate.pem`

PEM de certificado de copia

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

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

   Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados StorageGRID para FabricPool

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

Antes de empezar

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

Acerca de esta tarea

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

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

Pasos

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

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

3. Adjuntar StorageGRID como nivel de cloud en ONTAP.

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

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

Configurar certificados de cliente

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

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

Consulte "Gestionar certificados de seguridad" y.. "Configurar certificados de servidor personalizados".

> Para garantizar que las operaciones no se interrumpan por un certificado de servidor fallido, la alerta **Caducidad de certificados de cliente configurados en la página Certificados** se activa cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **certificados** y mirando la fecha de caducidad del certificado de cliente en la ficha Cliente.

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

Antes de empezar

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

Añada certificados de cliente

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

- El certificado de interfaz de gestión ya está configurado
- CERTIFICADO de cliente emitido por CA
- Certificado generado desde Grid Manager

El certificado de interfaz de gestión ya está configurado

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

Pasos

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

      El nuevo certificado aparece en la ficha Cliente.
7. Configurar una herramienta de supervisión externa, Como Grafana.

CERTIFICADO de cliente emitido por CA

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

Pasos

1. Siga los pasos a. "configure un certificado de interfaz de gestión".
2. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione

Permitir prometheus.

6. Seleccione **continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado de cliente, la clave privada y los archivos del paquete de CA:
   a. Seleccione **cargar certificado**.
   b. Seleccione **Examinar** y seleccione el certificado de cliente, la clave privada y los archivos de paquete de CA (`.pem`).
      - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en Grid Manager.

      Los nuevos certificados aparecen en la ficha Cliente.
8. Configurar una herramienta de supervisión externa, Como Grafana.

Certificado generado desde Grid Manager

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

Pasos

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

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

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

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

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

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

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

     Por ejemplo: `storagegrid_certificate.pem`

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

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

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

    El nuevo certificado aparece en la ficha Cliente.

11. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Global**.
12. Seleccione **Certificado de interfaz de administración**.
13. Seleccione **utilizar certificado personalizado**.
14. Cargue los archivos certificate.pem y private_key.pem desde el detalles del certificado de cliente paso. No es necesario cargar un paquete de CA.
    a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
    b. Cargue cada archivo de certificado (`.pem`).
    c. Seleccione **Crear** para guardar el certificado en Grid Manager.

       El nuevo certificado aparece en la ficha Cliente.

15. Configurar una herramienta de supervisión externa, Como Grafana.

Configure una herramienta de monitorización externa

Pasos

1. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.
   a. **Nombre**: Escriba un nombre para la conexión.

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

   b. **URL**: Introduzca el nombre de dominio o la dirección IP del nodo de administración. Especifique HTTPS y el puerto 9091.

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

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

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

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

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

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

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

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

Para obtener más información sobre las métricas, consulte "Instrucciones para supervisar StorageGRID".

Editar certificados de cliente

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.

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

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y, a continuación, seleccione **Editar nombre y permiso**
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
6. Seleccione **continuar** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Adjunte un nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.

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

una alerta.

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

Cargue el certificado

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

a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.

b. Cargue el nombre de certificado de cliente (`.pem`).

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

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

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

   Por ejemplo: `storagegrid_certificate.pem`

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

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

   El certificado actualizado se muestra en la ficha Cliente.

Generar certificado

Genere el texto del certificado para pegarlo en otro lugar.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

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

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

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

c. Seleccione **generar**.

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

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

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

otro lugar.

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

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

  Por ejemplo: `storagegrid_certificate.pem`

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

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

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

El nuevo certificado aparece en la ficha Cliente.

Descargar o copiar certificados de cliente

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado `.pem` archivo.

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

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

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

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

   Por ejemplo: `storagegrid_certificate.pem`

Quite certificados de cliente

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y, a continuación, confirme.

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

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

Configurar los ajustes de seguridad

Gestione la política TLS y SSH

La política de TLS y SSH determina qué protocolos y cifrados se usan para establecer conexiones TLS seguras con aplicaciones de cliente y conexiones SSH seguras a servicios StorageGRID internos.

La directiva de seguridad controla cómo TLS y SSH cifran los datos en movimiento. En general, utilice la directiva de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con Common Criteria o que necesite utilizar otros cifrados.

> Algunos servicios de StorageGRID no se han actualizado para utilizar los cifrados en estas políticas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Seleccione una política de seguridad

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.

   La pestaña **Políticas TLS y SSH** muestra las políticas disponibles. La política actualmente activa se indica mediante una marca de verificación verde en el mosaico de políticas.

2. Revise los mosaicos para obtener más información sobre las políticas disponibles.

Política	Descripción
Compatibilidad moderna (predeterminado)	Use la directiva predeterminada si necesita cifrado seguro y a menos que tenga requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.
Compatibilidad con versiones anteriores	Utilice esta directiva si necesita opciones de compatibilidad adicionales para clientes antiguos. Las opciones adicionales de esta política podrían hacerlo menos seguro que la política de compatibilidad moderna.
Criterios comunes	Utilice esta política si necesita la certificación Common Criteria.
Estricta con FIPS	Use esta directiva si necesita la certificación de criterios comunes y necesita utilizar el módulo de seguridad criptográfica 3.0.0 de NetApp para conexiones de clientes externos a extremos del equilibrador de carga, tenant Manager y Grid Manager. El uso de esta política puede reducir el rendimiento.
Personalizado	Cree una política personalizada si necesita aplicar sus propios cifrados.

3. Para ver detalles sobre los cifrados, protocolos y algoritmos de cada política, selecciona **Ver detalles**.
4. Para cambiar la política actual, seleccione **Usar política**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Cree una política de seguridad personalizada

Puede crear una política personalizada si necesita aplicar sus propios cifrados.

Pasos

1. Desde el mosaico de la política que es más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Selecciona **Copiar al portapapeles** y luego selecciona **Cancelar**.

3. En el mosaico **Política personalizada**, selecciona **Configurar y usar**.
4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Usar política**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico Política personalizada.

6. Opcionalmente, seleccione **Editar configuración** para realizar más cambios en la nueva política personalizada.

Vuelva temporalmente a la política de seguridad predeterminada

Si ha configurado una política de seguridad personalizada, es posible que no pueda iniciar sesión en Grid Manager si la política TLS configurada es incompatible con el "certificado de servidor configurado".

Puede revertir temporalmente a la política de seguridad predeterminada.

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:

   ```
   restore-default-cipher-configurations
   ```

3. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.
4. Siga los pasos de Seleccione una política de seguridad para volver a configurar la política.

Puede configurar la seguridad de red y de objetos para cifrar objetos almacenados, para evitar ciertas solicitudes S3 y Swift, o para permitir que las conexiones de cliente a los nodos de almacenamiento utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite el cifrado de todos los datos de objetos tal como se ingieren a través de S3. De forma predeterminada, los objetos almacenados no se cifran, pero puede optar por cifrar objetos mediante el algoritmo de cifrado AES-128 o AES-256. 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 procesados no se cifran.

La configuración de cifrado de objetos almacenados se aplica solo a objetos S3 que no han sido cifrados por el cifrado a nivel de cubo o de objeto.

Para obtener más información sobre los métodos de cifrado StorageGRID, consulte "Consulte los métodos de cifrado de StorageGRID".

Impida la modificación del cliente

Impedir la modificación del cliente es una configuración en todo el sistema. Cuando se selecciona la opción **Evitar modificación de cliente**, se rechazan las siguientes solicitudes.

API REST DE 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

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.

Active HTTP para las conexiones del nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea de producción.

Utilice HTTP para las conexiones de nodos de almacenamiento solo si los clientes S3 y Swift necesitan establecer conexiones HTTP directamente a los nodos de almacenamiento. No es necesario que utilice esta opción para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio de Equilibrador de Carga (porque puede hacerlo "configure cada punto final del equilibrador de carga" Para usar HTTP o HTTPS).

Consulte "Resumen: Direcciones IP y puertos para conexiones cliente" Para saber qué puertos S3 y los clientes Swift usan al conectarse a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccione las opciones

Antes de empezar

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

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.
2. Seleccione la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utilice la configuración **Ninguno** (predeterminada) si no desea que los objetos almacenados se cifren, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación de cliente** si desea evitar que los clientes S3 y Swift realicen solicitudes específicas.

   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.

5. Opcionalmente, seleccione **Activar HTTP para conexiones de nodos de almacenamiento** si los clientes se conectan directamente a nodos de almacenamiento y desea utilizar conexiones HTTP.

   Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

6. Seleccione **Guardar**.

Cambiar el tiempo de espera de inactividad del navegador

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.

Antes de empezar

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

Acerca de esta tarea

El tiempo de espera de inactividad del navegador es de forma predeterminada 15 minutos. Si el explorador de un usuario no está activo durante este período de tiempo, el usuario se cerrará la sesión.

Según sea necesario, puede aumentar o disminuir el período de tiempo de espera configurando la opción **Cerrar sesión de usuarios inactivos después**.

El tiempo de espera de inactividad del navegador también se controla mediante 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 desconecta automáticamente, incluso si el tiempo de espera de inactividad del explorador está desactivado o no se ha alcanzado el valor del tiempo de espera del explorador. Para renovar el token, el usuario debe volver a iniciar sesión.

- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está activado para StorageGRID.

  Si se activa SSO y se agota el tiempo de espera del explorador de un usuario, el usuario debe volver a introducir sus credenciales SSO para volver a acceder a StorageGRID. Consulte "Configurar el inicio de sesión único".

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.
2. Seleccione la pestaña **Tiempo de inactividad del navegador**.
3. En el campo **Cerrar sesión de usuarios inactivos después**, especifique un período de tiempo de espera del navegador entre 60 segundos y 7 días.

   Puede especificar el período de tiempo de espera del explorador en segundos, minutos, horas o días.

4. Seleccione **Guardar**. Si un explorador está inactivo durante la cantidad de tiempo especificada, el usuario se cierra sesión en Grid Manager o Tenant Manager.

   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.

Configuración de servidores de gestión de claves

Configurar servidores de gestión de claves: Descripción general

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

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

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

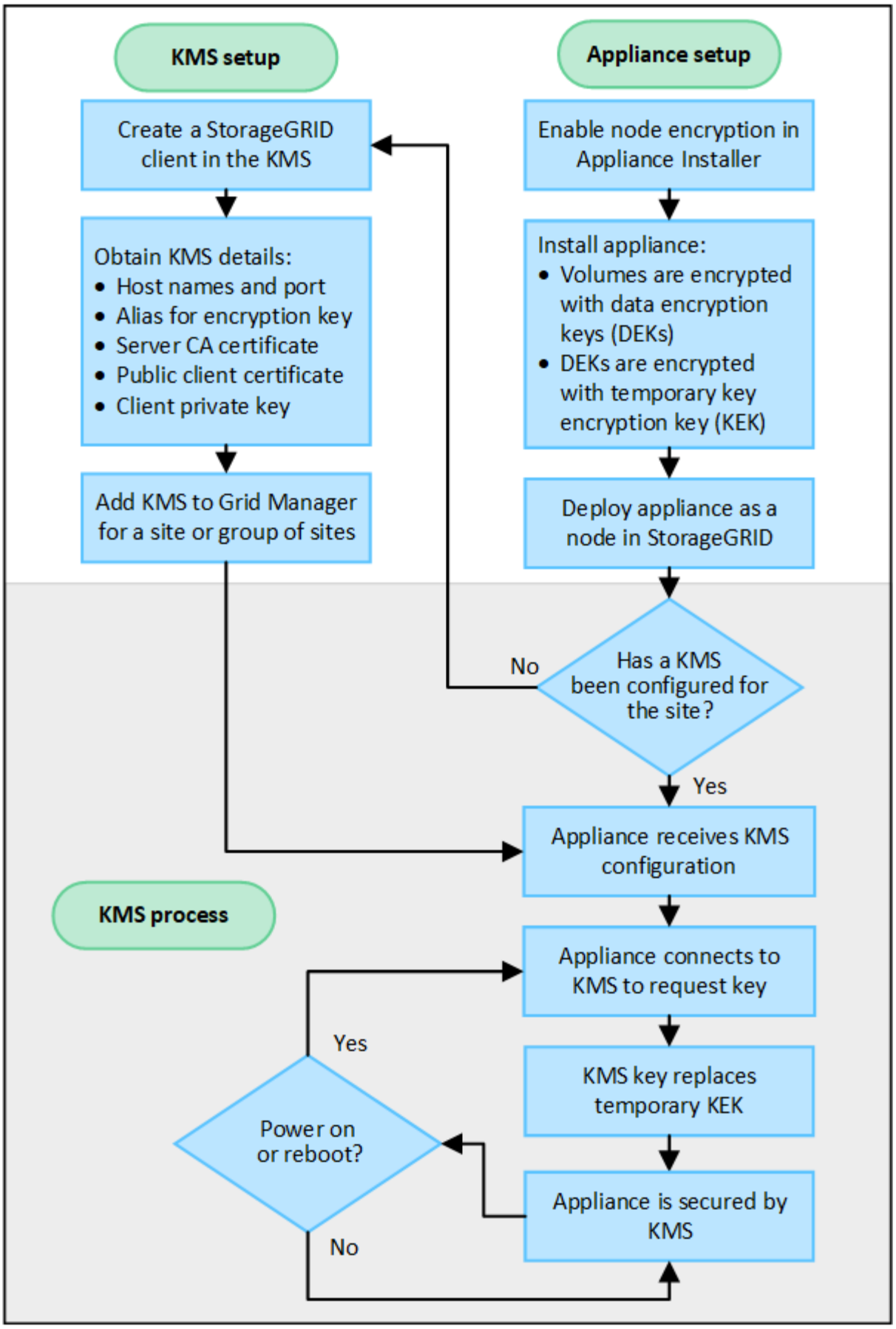
Puede utilizar uno o varios servidores de gestión de claves para administrar las claves de cifrado de nodos para los nodos de dispositivo StorageGRID que tengan activada la configuración * cifrado de nodos* durante la instalación. El uso de servidores de gestión de claves con estos nodos de dispositivos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

Información general de la configuración de KMS y dispositivos

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

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



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

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

Configurar el servidor de gestión de claves (KMS)

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

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

Configure el aparato

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

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

   > ⓘ No puede habilitar la configuración **Node Encryption** después de agregar un dispositivo a la cuadrícula, y no puede usar 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 mediante el cifrado de disco de Linux Unified Key Setup (LUKS) en el SO 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.

Consulte "Habilite el cifrado del nodo" para obtener más detalles.

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 clave, 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 nodo después de añadir un dispositivo al grid, y no se puede usar la gestión de claves externa para dispositivos que no tienen el cifrado de nodo habilitado.

Puede usar el KMS configurado para dispositivos StorageGRID y nodos de dispositivos.

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

- Nodos puestos en marcha como máquinas virtuales (VM)

- Nodos implementados en motores de contenedor en hosts Linux

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

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

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

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

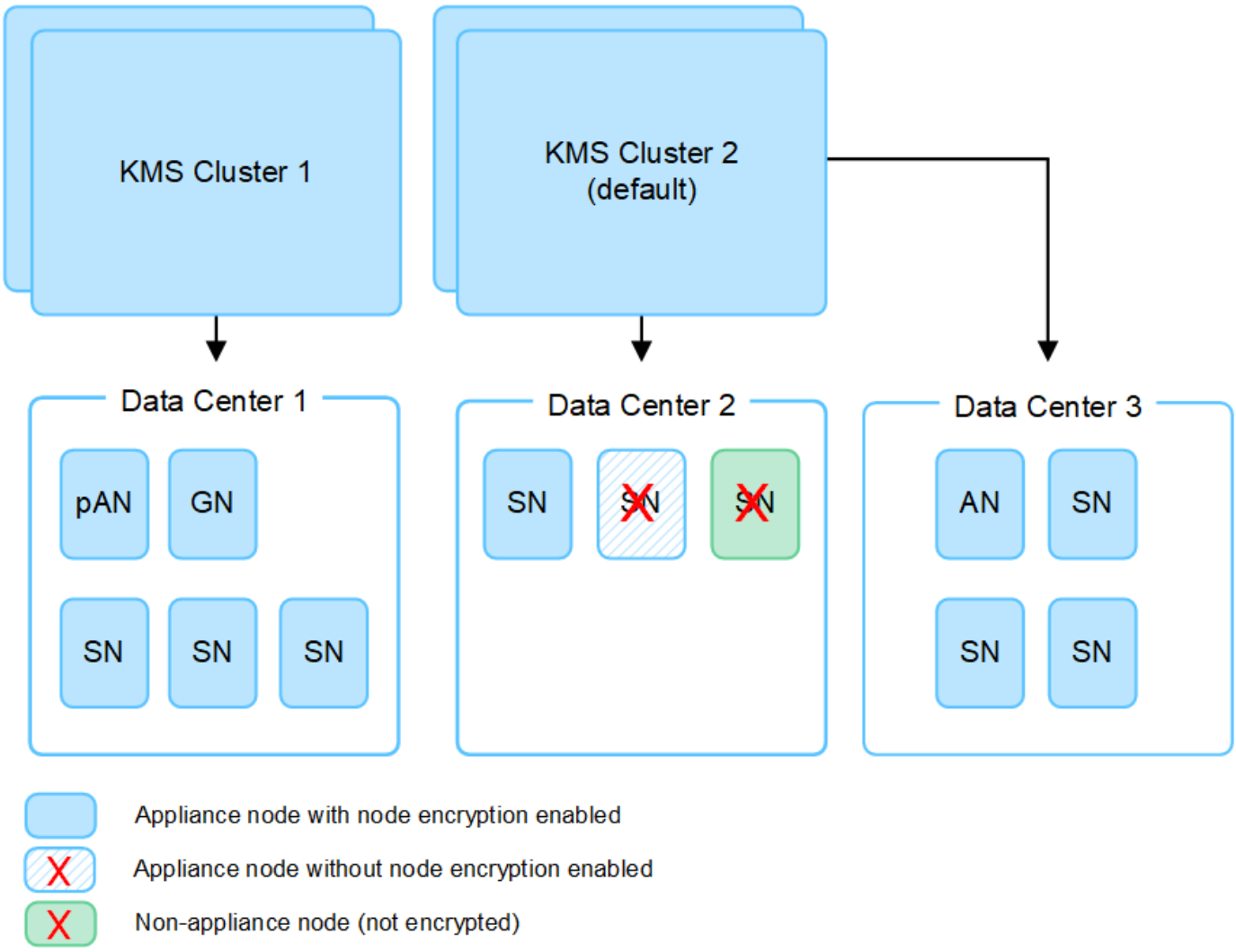
¿Cuántos servidores de gestión de claves necesito?

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

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

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

Tenga en cuenta que no puede usar un KMS para nodos que no sean del dispositivo ni para ningún nodo del dispositivo que no tenga habilitada la configuración **Node Encryption** 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 **KMS encryption key rotation failed** 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 utilizar el instalador de dispositivos de StorageGRID para "Borre 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.

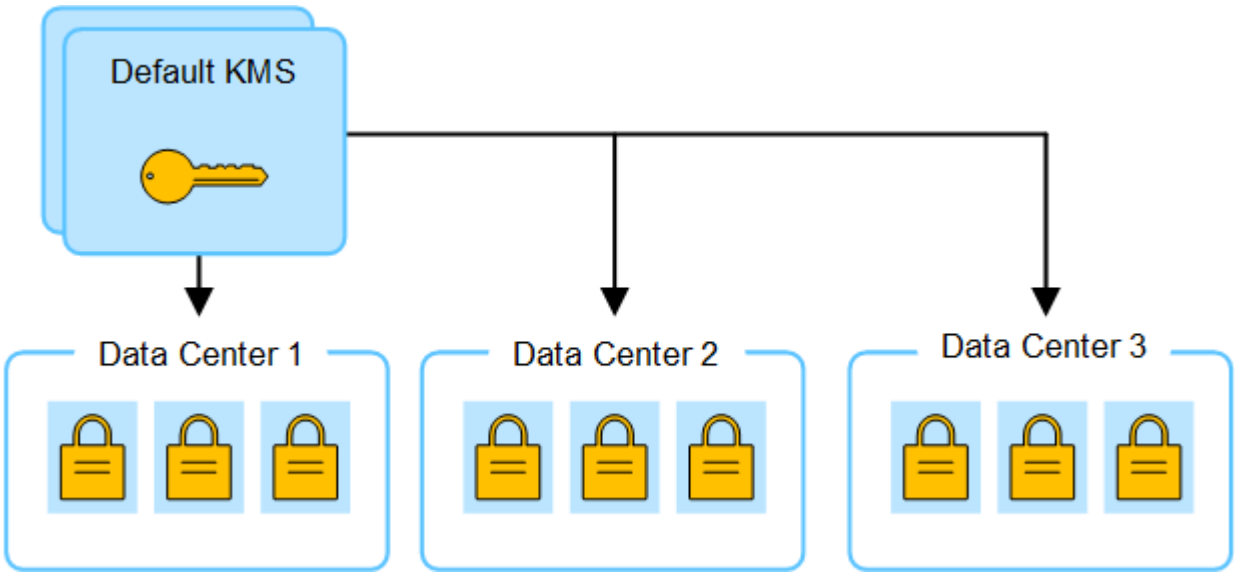
Consideraciones para cambiar el KMS de un sitio

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.

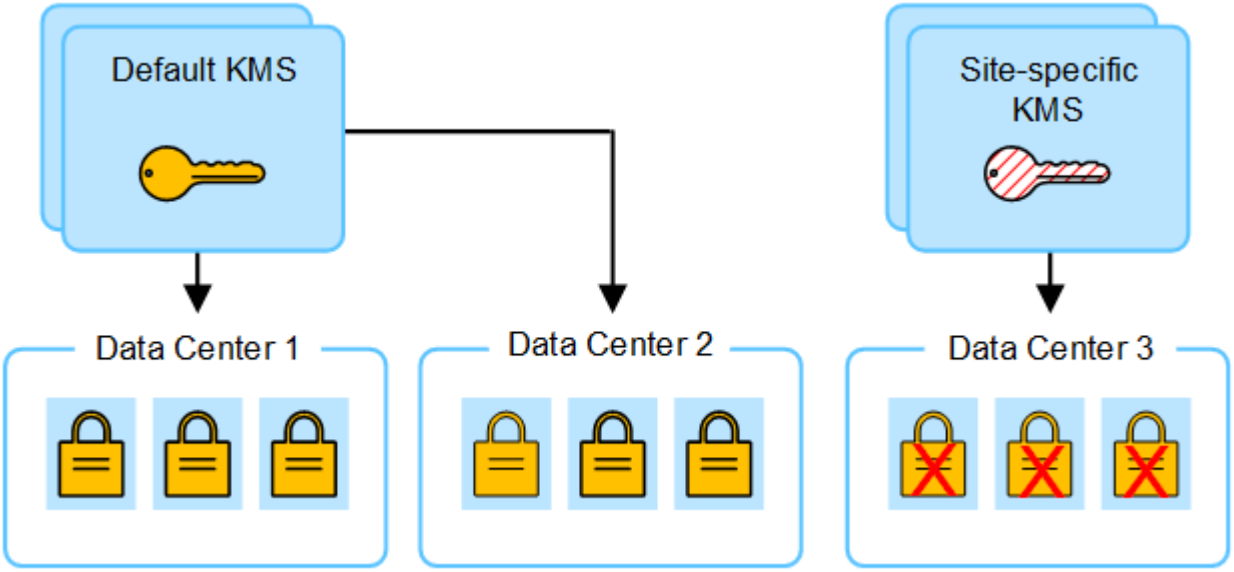
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original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

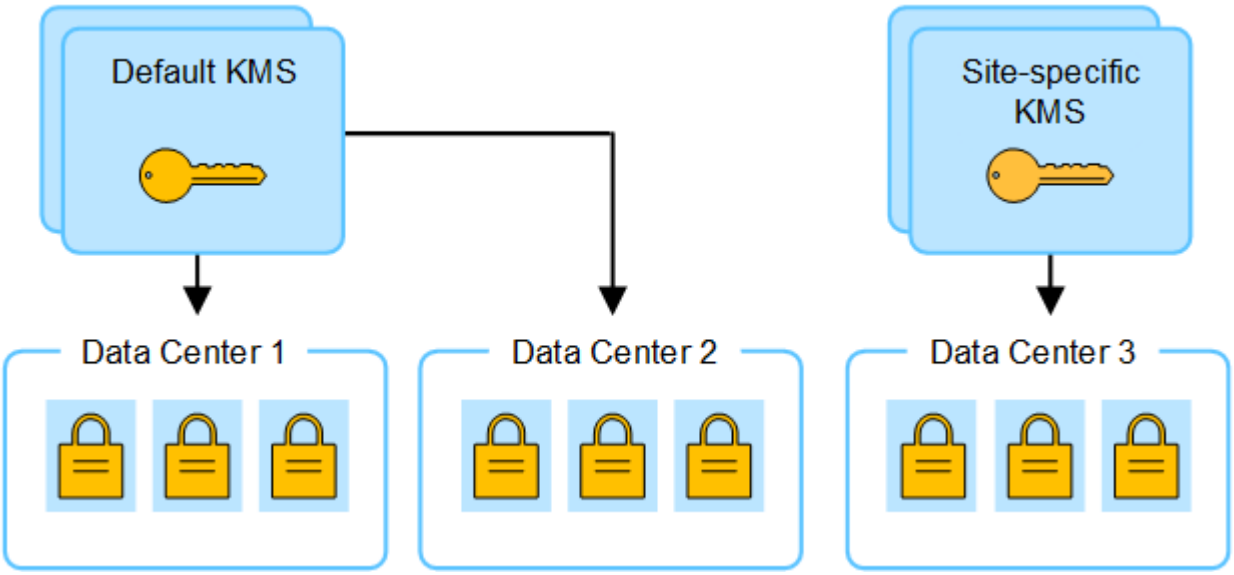
1. Inicialmente configuras un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa 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. "Editar un servidor de gestión de claves (KMS)"
Tiene un KMS predeterminado y agrega un sitio nuevo en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos del dispositivo en el sitio nuevo ya han sido cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un KMS nuevo. 2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Añadir un servidor de gestión de claves (KMS)"
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. "Añadir un servidor de gestión de claves (KMS)"

Configure StorageGRID como cliente en KMS

Debe configurar StorageGRID como cliente para cada servidor de gestión de claves externo o clúster de KMS antes de poder añadir el KMS a StorageGRID.

Acerca de esta tarea

Estas instrucciones se aplican a Thales CipherTrust Manager. Para obtener una lista de versiones compatibles, utilice "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

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 de 2.048 bits o más, y debe ser exportable.

3. Registre la siguiente información de cada clúster KMS o KMS.

   Necesitará esta información cuando agregue el KMS a StorageGRID.

- Nombre de host o dirección IP para cada servidor.
- Puerto KMIP utilizado por el KMS.
- Alias de clave para la clave de cifrado del KMS.

> La clave de cifrado ya debe existir en el KMS. StorageGRID no crea ni gestiona claves KMS.

4. Para cada clúster de KMS o KMS, obtenga un certificado de servidor firmado por una entidad de certificación (CA) o un paquete de certificado que contiene cada uno de los archivos de certificado de CA codificados con PEM, concatenado en el orden de la cadena de certificados.

   El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

   - El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.
   - El campo Nombre alternativo del asunto (SAN) de cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que se conectará StorageGRID.

     > Al configurar el KMS en StorageGRID, debe introducir las mismas FQDN o direcciones IP en el campo **Nombre de host**.

   - El certificado de servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que suele utilizar el puerto 5696.
5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada del certificado de cliente.

   El certificado de cliente permite que StorageGRID se autentique en el KMS.

Añadir un servidor de gestión de claves (KMS)

Utilice el asistente del servidor de gestión de claves de StorageGRID para agregar cada clúster KMS o KMS.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Ya tienes "Se ha configurado StorageGRID como cliente en el KMS"Y tiene la información necesaria para cada clúster KMS o KMS.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.

Acerca de esta tarea

Si es posible, configure cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS. Si crea el KMS predeterminado primero, todos los dispositivos cifrados por nodo de la cuadrícula se cifrarán con el KMS predeterminado. Si desea crear más tarde un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulte "Consideraciones para cambiar el KMS de un sitio" para obtener más detalles.

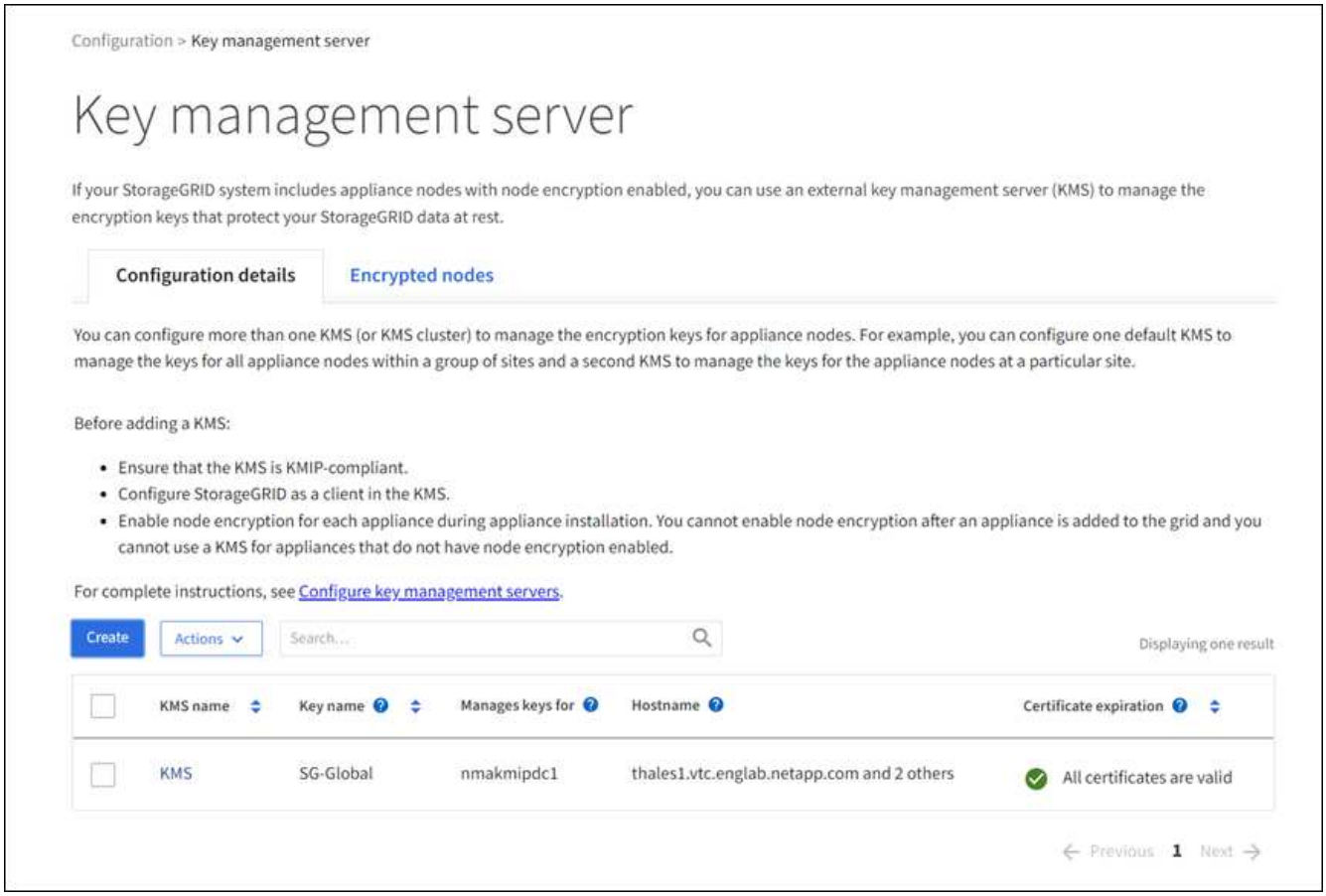
Paso 1: Detalles de KM

En el Paso 1 (detalles de KMS) del Asistente para agregar un servidor de gestión de claves, proporciona detalles sobre el clúster de KMS o KMS.

Pasos

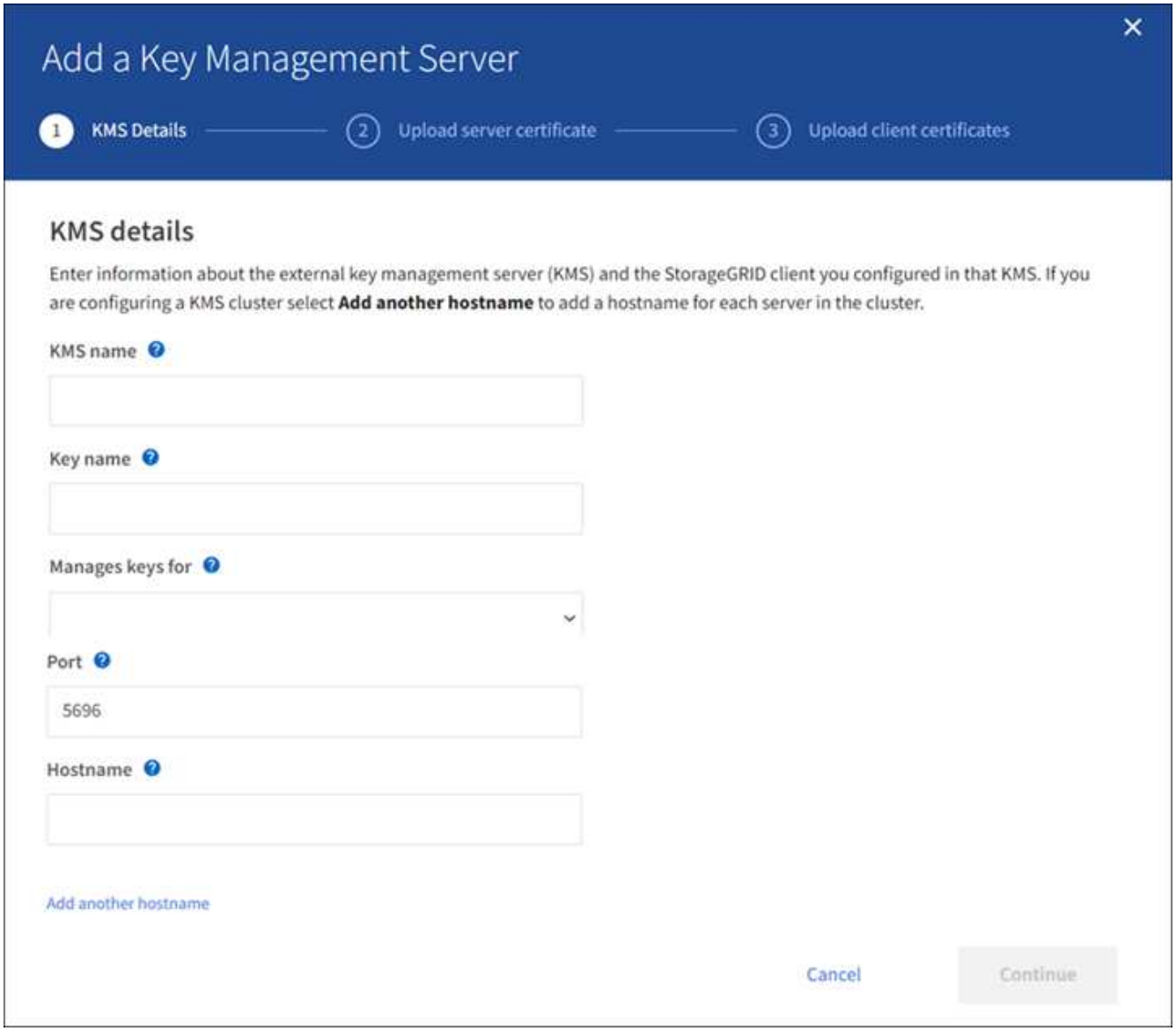
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página del servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.



2. Seleccione **Crear**.

   Paso 1 (detalles de KMS) del asistente Add a Key Management Server.



3. Introduzca la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres.

Campo	Descripción
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 gestionados por otro KMS (por defecto KMS)** 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 Nombre Alternativo del Asunto (SAN) del certificado del 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.

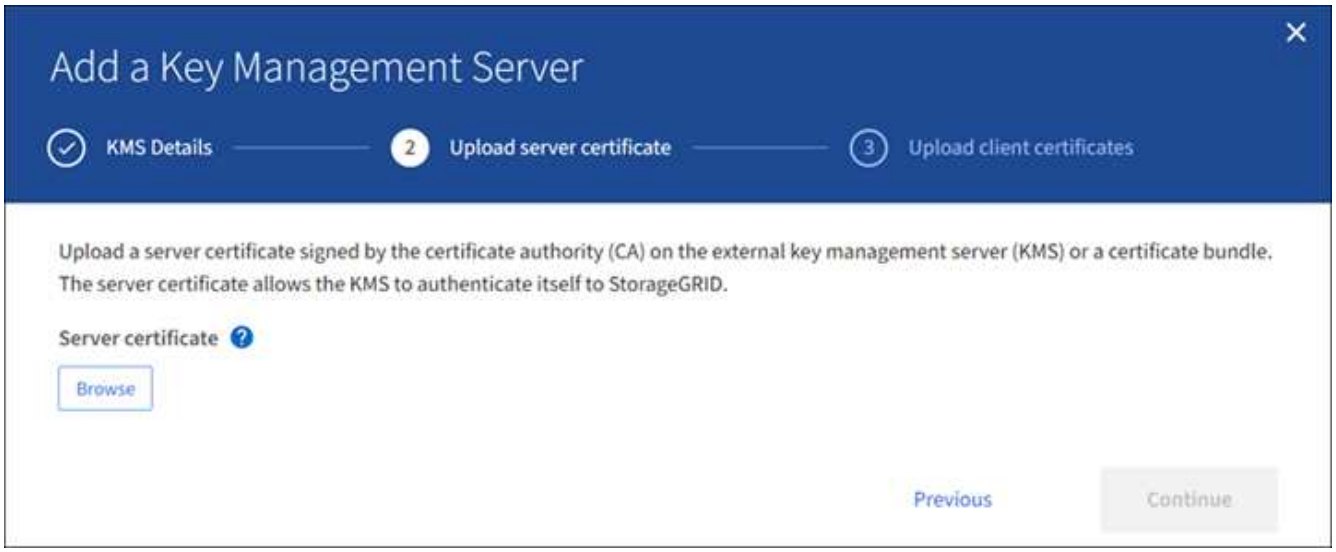
4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

Paso 2: Cargar certificado de servidor

En el paso 2 (Cargar certificado de servidor) del asistente Agregar un servidor de gestión de claves, cargue el certificado de servidor (o paquete de certificados) para el KMS. El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

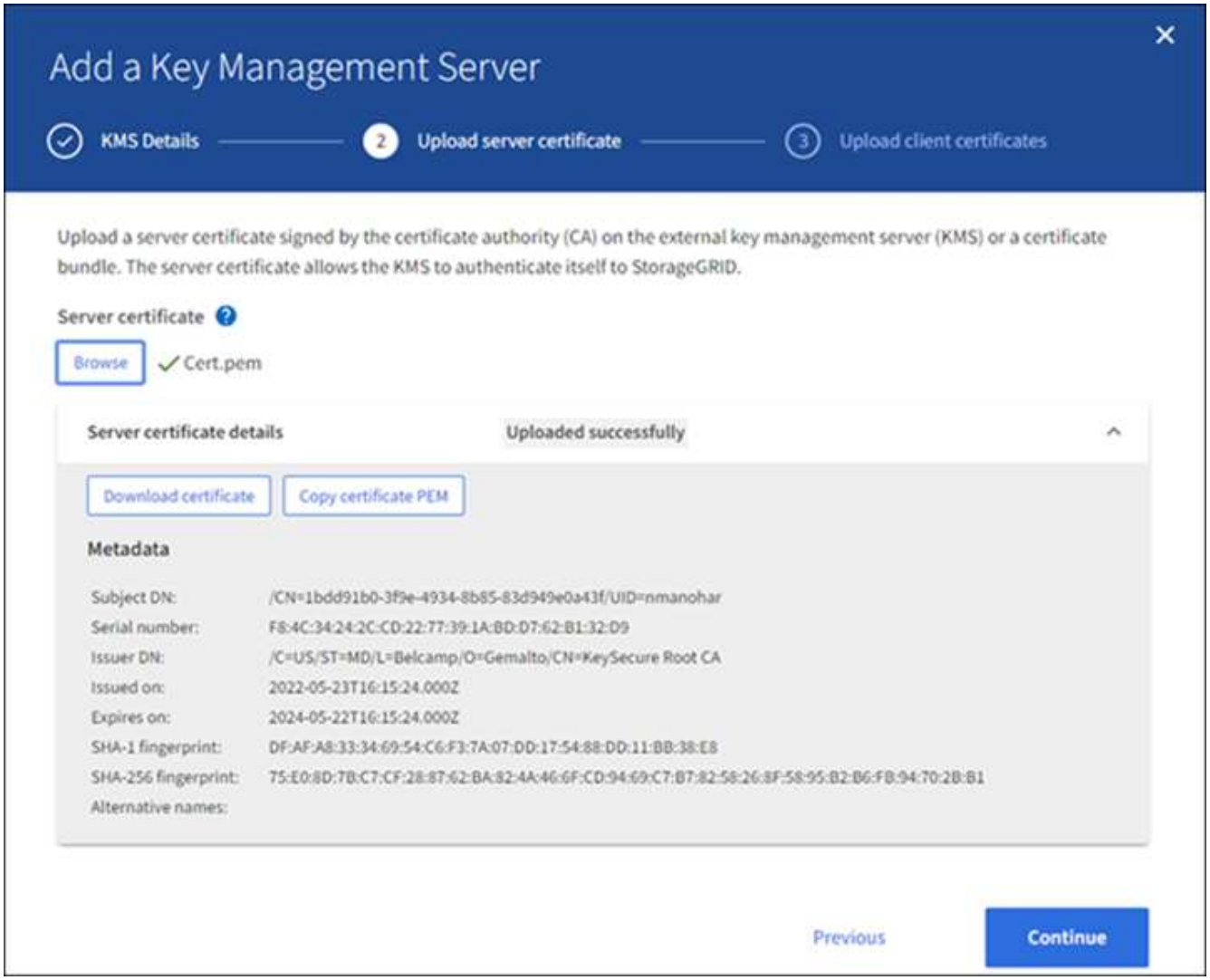
Pasos

1. Desde **Paso 2 (Cargar certificado de servidor)**, busque la ubicación del certificado de servidor guardado o el paquete de certificados.



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.

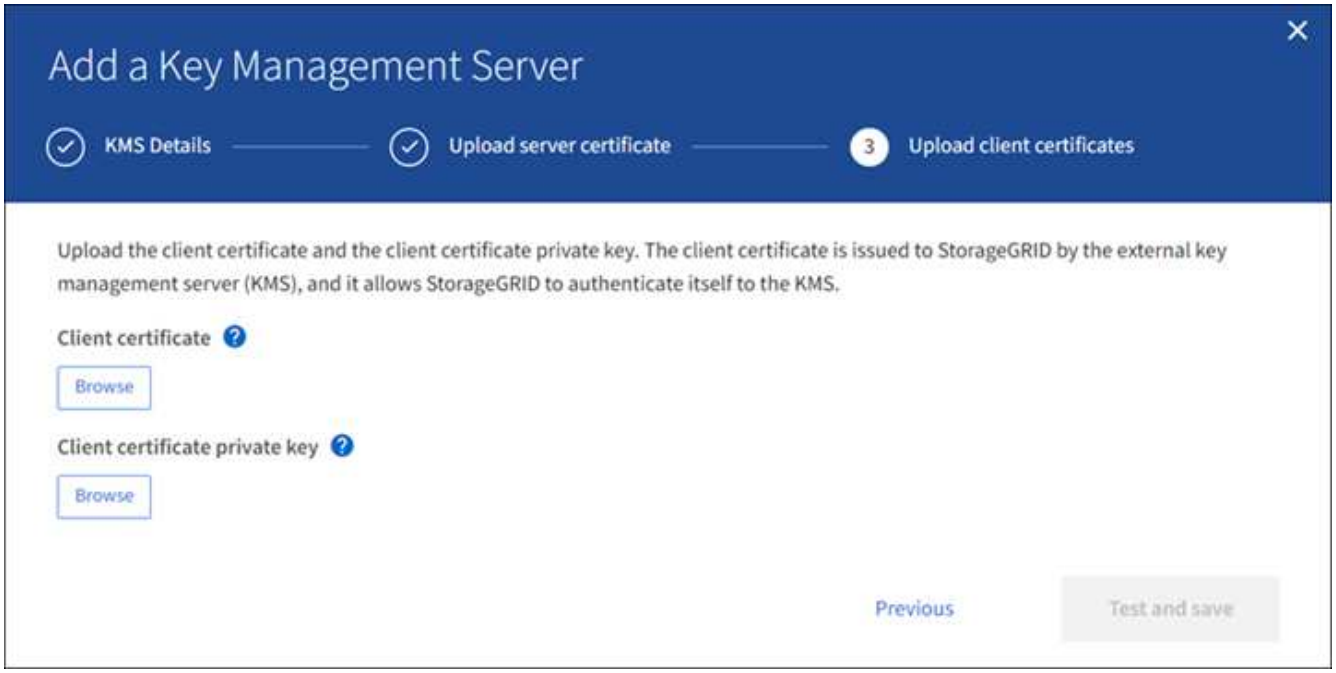
3. Seleccione **continuar**.

Paso 3: Cargar certificados de cliente

En el paso 3 (Cargar certificados de cliente) del asistente para agregar un servidor de gestión de claves, cargue el certificado de cliente y la clave privada de certificado de cliente. El certificado de cliente permite que StorageGRID se autentique en el KMS.

Pasos

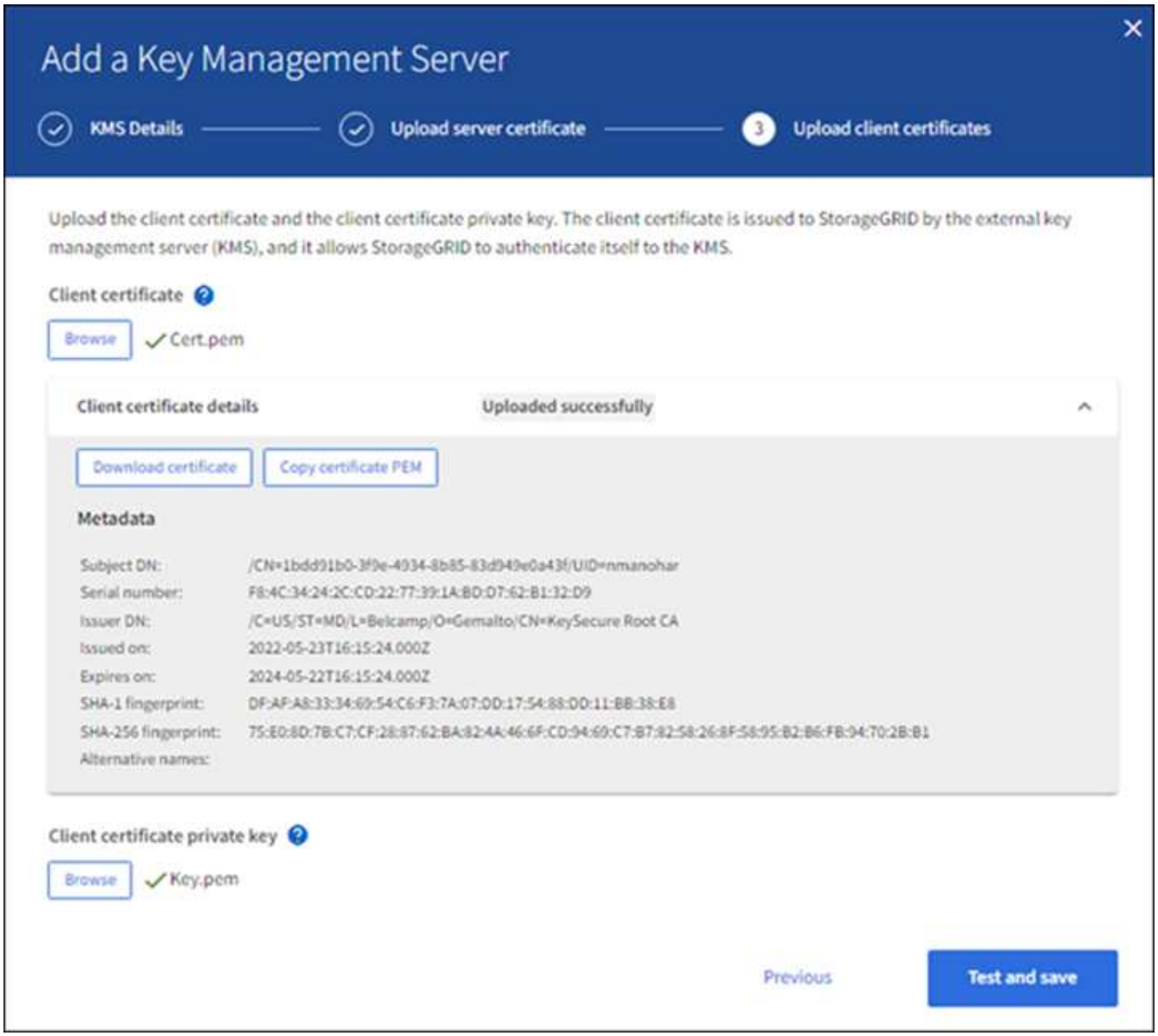
1. Desde **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.



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.



5. Selecciona **Probar y 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 **Probar y guardar**, revise los detalles del mensaje y luego 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 **Forzar guardar**.

Al seleccionar **Force save** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

8. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

   La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

Ver detalles de KMS

Puede ver información sobre cada servidor de gestión de claves (KMS) del sistema StorageGRID, incluidos el estado actual de los certificados de servidor y de cliente.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página del servidor de gestión de claves. La pestaña Detalles de configuración muestra todos los servidores de gestión de claves configurados.

2. Revise la información de la tabla de cada KMS.

Campo	Descripción
Nombre de KM	Nombre descriptivo del KMS.
Nombre de clave	El alias clave del cliente StorageGRID en el KMS.
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, abra un KMS y seleccione **Editar** o **Acciones** > **Editar**.

Campo	Descripción
Caducidad 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:** StorageGRID puede tardar hasta 30 minutos en recibir actualizaciones del vencimiento del certificado. Debe actualizar el navegador web para ver los valores actuales.

3. Si la caducidad del certificado es Desconocido, espere hasta 30 minutos y actualice el explorador web.

> Inmediatamente después de agregar un KMS, el vencimiento 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 Caducidad del certificado indica que un certificado ha caducado o está a punto de caducar, solucione el problema lo antes posible.

   Cuando se activan las alertas **KMS CA CERTIFICATION**, **KMS client certificate expiration** y **KMS server certificate expiration**, anote la descripción de cada alerta y realice las acciones recomendadas.

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

5. Para ver los detalles del certificado de este KMS, seleccione el nombre del KMS en la tabla.
6. En la página de resumen de KMS, revise los metadatos y el certificado PEM tanto para el certificado de servidor como para el certificado de cliente. Según sea necesario, seleccione **Editar certificado** para reemplazar un certificado por uno nuevo.

Vea los nodos cifrados

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra todos los servidores de gestión de claves que se configuraron.

2. En la parte superior de la página, seleccione la pestaña **Nodos encriptados**.

   La pestaña Nodos cifrados muestra los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Encriptación 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 KM	Nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Añadir un servidor de gestión de claves (KMS)"
UID de clave	El ID único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver una UID de clave completa, coloque el cursor sobre 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

   Realice las acciones recomendadas para estas alertas.

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

Editar un servidor de gestión de claves (KMS)

Es posible que deba editar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de expirar.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Si planea actualizar el sitio seleccionado para un KMS, ha revisado el "Consideraciones para cambiar el KMS de un sitio".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas editar y selecciona **Acciones** > **Editar**.

   También puede editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualice los detalles en **Paso 1 (detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de 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"

Campo	Descripción
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente **Sitios no gestionados 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 está editando el KMS predeterminado, no puede seleccionar un sitio específico.
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del 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 está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

   Paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de gestión de claves.

6. Si necesita sustituir el certificado del servidor, seleccione **examinar** y cargue el nuevo archivo.
7. Seleccione **continuar**.

   El paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de gestión de claves aparece.

8. Si necesita sustituir el certificado de cliente y la clave privada del certificado de cliente, seleccione **examinar** y cargue los nuevos archivos.
9. Selecciona **Probar y 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 guardar**.

Al seleccionar **Force save** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

Se guarda la configuración de KMS.

12. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

    La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

Quitar un servidor de gestión de claves (KMS)

En algunos casos, es posible quitar un servidor de gestión de claves. Por ejemplo, puede que desee quitar un KMS específico de un sitio si ha retirado del servicio el sitio.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.

Acerca de esta tarea

Puede eliminar un KMS en los siguientes casos:

- Puede eliminar un KMS específico de un sitio si se ha dado de baja o si el sitio incluye ningún nodo de dispositivo con cifrado de nodo activado.
- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tiene nodos de dispositivo con cifrado de nodo activado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas eliminar y selecciona **Acciones** > **Eliminar**.

   También puede eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirme que lo siguiente es verdadero:
   - Está eliminando un KMS específico del sitio para un sitio que no tiene ningún nodo de dispositivo con cifrado de nodo activado.
   - Está eliminando el KMS predeterminado, pero ya existe un KMS específico para cada sitio con cifrado de nodo.
4. Seleccione **Sí**.

   La configuración de KMS se elimina.

Administrar la configuración de proxy

Configure las opciones de proxy de almacenamiento

Si utiliza servicios de plataforma o pools de almacenamiento en cloud, puede configurar un proxy no transparente entre los nodos de almacenamiento y los extremos de S3 externos. Por ejemplo, es posible que necesite un proxy no transparente para permitir que los mensajes de servicios de plataforma se envíen a extremos externos, como un punto final en Internet.

Antes de empezar

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

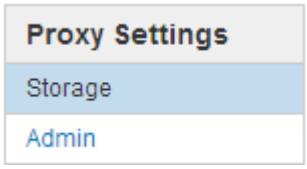
Acerca de esta tarea

Puede configurar los ajustes de un único proxy de almacenamiento.

Pasos

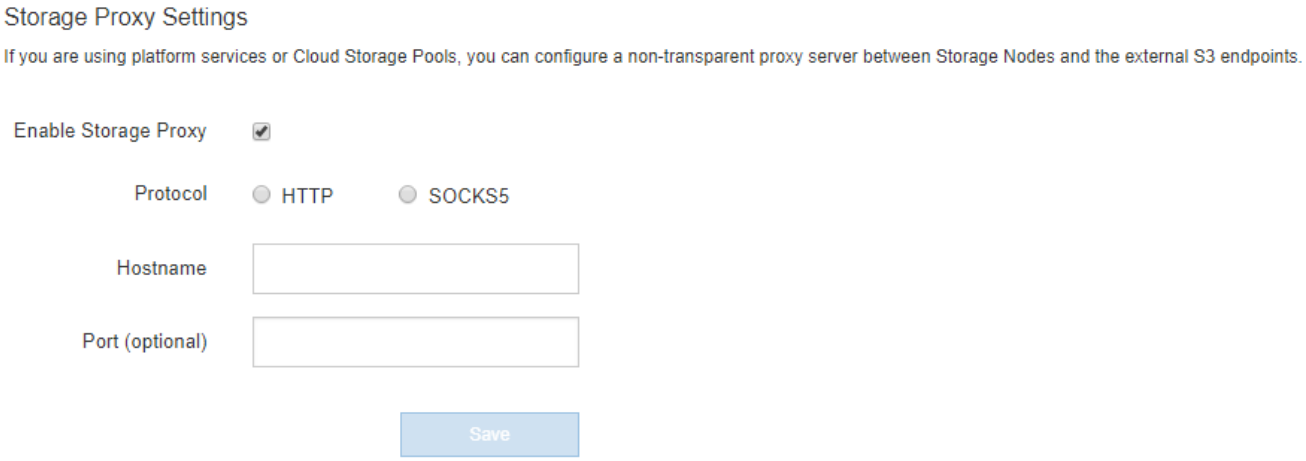
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Se muestra la página Storage Proxy Settings. De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. Seleccione la casilla de verificación **Activar proxy de almacenamiento**.

   Aparecen los campos para configurar un proxy de almacenamiento.

3. Seleccione el protocolo del proxy de almacenamiento no transparente.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. De manera opcional, introduzca el puerto utilizado para conectarse al servidor proxy.

Puede dejar este campo en blanco si utiliza el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

   Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos extremos para los servicios de plataforma o Cloud Storage Pools.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Compruebe la configuración del servidor proxy para asegurarse de que los mensajes de StorageGRID relacionados con el servicio de la plataforma no se bloqueen.

Después de terminar

Si necesita deshabilitar un proxy de almacenamiento, desactive la casilla de verificación **Habilitar proxy de almacenamiento** y seleccione **Guardar**.

Información relacionada

- "Red y puertos para servicios de plataforma"
- "Gestión de objetos con ILM"

Configure los ajustes del proxy de administración

Si envía mensajes de AutoSupport con HTTP o HTTPS (consulte "Configure AutoSupport"), puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Antes de empezar

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

Acerca de esta tarea

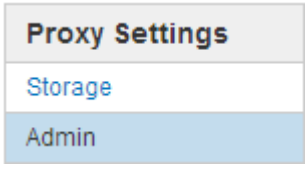
Puede configurar los ajustes de un único proxy de administración.

Pasos

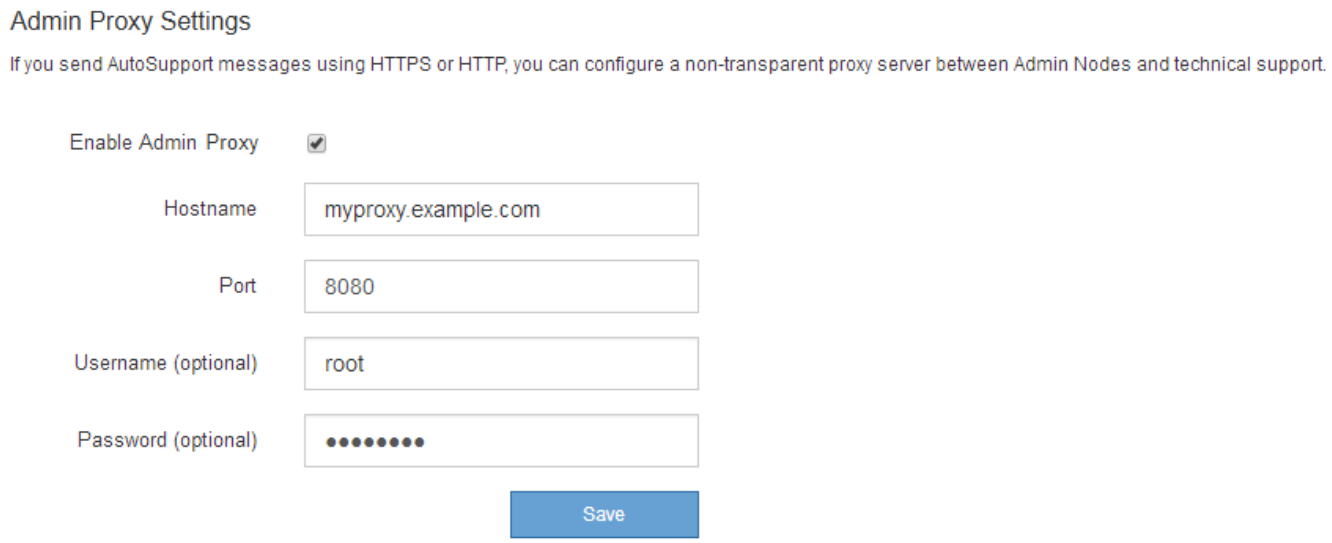
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Aparece la página Admin Proxy Settings (Configuración del proxy de administración). De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. En el menú de la barra lateral, seleccione **Admin**.



3. Seleccione la casilla de verificación **Enable Admin Proxy**.



4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Si lo desea, introduzca el nombre de usuario del proxy.

   Deje este campo en blanco si el servidor proxy no requiere un nombre de usuario.

7. De forma opcional, introduzca la contraseña del proxy.

   Deje este campo en blanco si el servidor proxy no requiere una contraseña.

8. Seleccione **Guardar**.

   Una vez guardado el proxy de administrador, se configura el servidor proxy entre los nodos de administrador y el soporte técnico.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesita deshabilitar el proxy, desactive la casilla de verificación **Habilitar proxy de administración** y seleccione **Guardar**.

Controle los firewalls

Controle el acceso a un firewall externo

Puede abrir o cerrar puertos específicos 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.

Si desea configurar el firewall interno de StorageGRID, consulte "Configure el firewall interno".

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.
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 API de gestión no pueden acceder a Grid Manager ni a la API de administración 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

- "Inicie sesión en Grid Manager"
- "Cree una cuenta de inquilino"
- "Comunicaciones externas"

Gestionar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad del grid al permitirle controlar el acceso de red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos, excepto los necesarios para su implementación de grid específica. Los cambios de configuración que realice en la página de control del firewall se despliegan en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su grid.

- **Lista de direcciones privilegiadas**: Utilice esta pestaña para permitir el acceso seleccionado a los puertos cerrados. Puede agregar direcciones IP o subredes en la notación CIDR que pueden acceder a los puertos cerrados mediante la pestaña Administrar acceso externo.
- **Administrar acceso externo**: Utilice esta pestaña para cerrar los puertos que están abiertos por defecto, o reabrir los puertos previamente cerrados.
- **Red de cliente no confiable**: Utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red cliente.

  Esta pestaña también proporciona la opción de especificar los puertos adicionales que desea abrir cuando se configura una red cliente que no sea de confianza. Estos puertos pueden proporcionar acceso a Grid Manager, al Tenant Manager o a ambos.

  La configuración de esta ficha sustituye a la configuración de la ficha Administrar acceso externo.

  - Un nodo con una red de cliente que no sea de confianza aceptará solo conexiones en los puertos de punto final del equilibrador de carga configurados en ese nodo (puntos finales enlazados de tipo de nodo, interfaz de nodo y global).
  - Los puertos adicionales abiertos en la pestaña Red de cliente sin confianza están abiertos en todas las redes de cliente que no son de confianza, incluso si no se ha configurado ningún punto final de equilibrio de carga.
  - Los puertos de punto final del equilibrador de carga y los puertos adicionales seleccionados *son los únicos puertos abiertos* en las redes de cliente que no son de confianza, independientemente de la configuración de la pestaña Administrar redes externas.
  - Cuando se confía, se puede acceder a todos los puertos abiertos en la pestaña Administrar acceso externo, así como a cualquier punto final del equilibrador de carga abierto en la red cliente.

> La configuración que realice en una pestaña puede afectar a los cambios de acceso que realice en otra pestaña. Asegúrese de comprobar la configuración en todas las pestañas para asegurarse de que su red se comporta de la forma que espera.

Para configurar los controles internos del firewall, consulte "Configurar los controles del firewall".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Lista de direcciones con privilegios y pestañas Gestionar acceso externo

El separador Lista de Direcciones con Privilegios permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de grid que están cerrados. La pestaña Administrar acceso externo permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no son de cuadrícula de forma predeterminada). Estas dos pestañas a menudo se pueden utilizar juntas para personalizar el acceso exacto a la red que necesita para su grid.

> Las direcciones IP con privilegios no tienen acceso de puerto de grid interno por defecto.

Ejemplo 1: Utilice un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host reforzado con seguridad) para la administración de la red. Puede utilizar estos pasos generales:

1. Utilice el separador Lista de Direcciones con Privilegios para agregar la dirección IP del host de salto.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

> Agregue la dirección IP con privilegios antes de bloquear los puertos 443 y 8443. Cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

Después de guardar la configuración, todos los puertos externos en el nodo de administración de la cuadrícula se bloquearán para todos los hosts excepto el host de salto. A continuación, puede utilizar el host de salto para realizar tareas de mantenimiento en la red de forma más segura.

Ejemplo 2: Limitar el acceso a Grid Manager y al administrador de inquilinos

Supongamos que desea limitar el acceso a Grid Manager y al gestor de inquilinos por motivos de seguridad. Puede utilizar estos pasos generales:

1. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 443.
2. Utilice el conmutador en la pestaña Administrar acceso externo para permitir el acceso al puerto 8443.
3. Utilice el conmutador en la pestaña Administrar acceso externo para permitir el acceso al puerto 9443.

Después de guardar la configuración, los hosts no podrán acceder al puerto 443, pero podrán acceder a Grid Manager a través del puerto 8443 y al gestor de inquilinos a través del puerto 9443.

Ejemplo 3: Bloquear puertos sensibles

Suponga que desea bloquear los puertos confidenciales y el servicio en ese puerto (por ejemplo, SSH en el puerto 22). Puede utilizar los siguientes pasos generales:

1. Utilice el separador Lista de Direcciones con Privilegios para otorgar acceso sólo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

> Agregue la dirección IP con privilegios antes de bloquear los puertos 443 y 8443. Cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

Después de guardar la configuración, el puerto 22 y el servicio SSH estarán disponibles para los hosts de la lista de direcciones con privilegios. Se denegará el acceso al servicio a todos los demás hosts sin importar de qué interfaz proviene la solicitud.

Ejemplo 4: Desactivar el acceso a los servicios no utilizados

A nivel de red, puede desactivar algunos servicios que no desea utilizar. Por ejemplo, si no proporcionará acceso Swift, debe realizar los siguientes pasos generales:

1. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 18083.
2. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 18085.

Después de guardar la configuración, el nodo de almacenamiento ya no permite la conectividad Swift, pero

sigue permitiendo el acceso a otros servicios en puertos no bloqueados.

Pestaña Redes de cliente que no son de confianza

Si está utilizando una red cliente, puede ayudar a proteger StorageGRID de ataques hostiles al aceptar el tráfico de clientes entrantes solo en puntos finales configurados explícitamente o en puertos adicionales que seleccione en esta pestaña.

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 grid en All "puertos externos disponibles".

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 cliente de un nodo no es de confianza, el nodo solo acepta conexiones entrantes en puertos configurados explícitamente como puntos finales del equilibrador de carga y cualquier puerto adicional que designe mediante la pestaña Red cliente no confiable de la página de control de firewall. Consulte "Configurar puntos finales del equilibrador de carga" y.. "Configurar los controles del firewall".

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. Desde la "Puntos finales del equilibrador de carga" Configure un punto final del equilibrador de carga para S3 sobre HTTPS en el puerto 443.
2. En la página de control de firewall, seleccione Sin confianza para especificar que la red 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

Suponga que desea habilitar el tráfico de servicios de la plataforma S3 saliente desde un nodo de almacenamiento, pero desea evitar las conexiones entrantes a ese nodo de almacenamiento en la red de clientes. Debe realizar este paso general:

- En la pestaña Redes de cliente sin confianza de la página de control de firewall, indique que la red de cliente en el 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 las solicitudes salientes a los destinos de servicios de plataforma configurados.

Ejemplo 3: Limitar el acceso a Grid Manager a una subred

Supongamos que desea permitir el acceso de Grid Manager solo en una subred específica. Debe realizar los siguientes pasos:

1. Conecte la red cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente sin confianza para configurar la red cliente como no confiable.
3. En la sección **Puertos adicionales abiertos en Red de clientes no confiables** de la pestaña, agregue el puerto 443 o 8443.

4. Utilice el separador Gestionar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP con privilegios definidas para hosts fuera de esa subred).

Después de guardar la configuración, solo los hosts de la subred especificada pueden acceder a Grid Manager. Todos los demás hosts están bloqueados.

Configure el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso a la red a puertos específicos de los nodos de StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha revisado la información de "Gestionar los controles del firewall" y.. "Directrices sobre redes".
- 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.

> Al cambiar la configuración de la red cliente, las conexiones de cliente existentes pueden fallar si no se han configurado los puntos finales del equilibrador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos del grid. Puede utilizar las pestañas de control del firewall para abrir o cerrar los puertos que están abiertos de forma predeterminada en la red de grid, la red de administración y la red de cliente. También puede crear una lista de direcciones IP con privilegios que pueden acceder a los puertos de cuadrícula que están cerrados. Si utiliza una red cliente, puede especificar si un nodo confía en el tráfico entrante de la red cliente y puede configurar el acceso de puertos específicos en la red cliente.

Limitar el número de puertos abiertos a direcciones IP fuera de su red a solo aquellos que son absolutamente necesarios mejora la seguridad de su red. Utilice la configuración en cada una de las tres pestañas de control de Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de controles de firewall, incluidos ejemplos, consulte "Gestionar los controles del firewall".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Acceda a los controles del cortafuegos

Pasos

1. Selecciona **CONFIGURACIÓN** > **Seguridad** > **Control de firewall**.

   Las tres pestañas de esta página se describen en "Gestionar los controles del firewall".

2. Seleccione cualquier pestaña para configurar los controles del firewall.

   Puede utilizar estas pestañas en cualquier orden. Las configuraciones establecidas en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña pueden cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones con privilegios

Utilice el separador Lista de Direcciones con Privilegios para otorgar a los hosts acceso a los puertos que están cerrados por defecto o cerrados por valores en el separador Gestionar Acceso Externo.

Las direcciones IP y subredes con privilegios no tienen acceso interno a la cuadrícula por defecto. Además, los puntos finales del equilibrador de carga y los puertos adicionales abiertos en la pestaña de lista de direcciones con privilegios son accesibles incluso si están bloqueados en la pestaña Gestionar acceso externo.

> La configuración de la pestaña Lista de direcciones con privilegios no puede sustituir la configuración de la pestaña Red de clientes sin confianza.

Pasos

1. En la pestaña Lista de direcciones con privilegios, introduzca la dirección o subred IP que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes con privilegios adicionales.

   > Agregue el menor número posible de direcciones a la lista de privilegios.

3. Opcionalmente, seleccione **Permitir direcciones IP privilegiadas para acceder a los puertos internos de StorageGRID**. Consulte "Puertos internos StorageGRID".

   > Esta opción elimina algunas protecciones para los servicios internos. Déjelo desactivado si es posible.

4. Seleccione **Guardar**.

Gestione el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de grid puede acceder al puerto a menos que agregue la dirección IP a la lista de direcciones con privilegios. Solo puede cerrar los puertos que están abiertos de forma predeterminada y sólo puede abrir los puertos que haya cerrado.

> La configuración de la pestaña Administrar acceso externo no puede sustituir la configuración de la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la red cliente incluso si está abierto en la pestaña Gestionar acceso externo. La configuración de la pestaña Red de cliente no confiable anula los puertos cerrados (como 443, 8443, 9443) en la red cliente.

Pasos

1. Selecciona **Administrar acceso externo**. El separador muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no son de cuadrícula por defecto) para los nodos de la cuadrícula.
2. Configure los puertos que desea abrir y cerrar mediante las siguientes opciones:
   - Utilice la palanca situada junto a cada puerto para abrir o cerrar el puerto seleccionado.
   - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.

- Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.

> Si cierra los puertos 443 o 8443 de Grid Manager, cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

> Utilice la barra de desplazamiento situada a la derecha de la tabla para asegurarse de que ha visto todos los puertos disponibles. Utilice el campo de búsqueda para buscar la configuración de cualquier puerto externo introduciendo un número de puerto. Puede introducir un número de puerto parcial. Por ejemplo, si introduce un **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Seleccione **Guardar**

Red cliente no confiable

Si la red cliente de un nodo no es de confianza, el nodo solo acepta el tráfico entrante en los puertos configurados como puntos finales de equilibrio de carga y, opcionalmente, los puertos adicionales que seleccione en esta pestaña. También puede usar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.

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

Los cambios de configuración que realice en la pestaña **Red de clientes sin confianza** anulan la configuración de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red cliente no confiable**.
2. En la sección Definir Nuevo Nodo por Defecto, especifique cuál debe ser el valor por defecto cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.

   - **De confianza** (por defecto): Cuando se agrega un nodo en una expansión, su red 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 pestaña para cambiar la configuración de un nuevo nodo específico.

   > Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de cliente solo en puntos finales del equilibrador de carga configurados explícitamente o puertos seleccionados adicionales:

   - Seleccione **Untrust on Visualized Nodes** para agregar todos los nodos mostrados en la tabla a la lista Untrusted Client Network.
   - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos mostrados en la tabla de la lista Red de clientes sin confianza.

- Utilice el conmutador situado junto a cada puerto para establecer la red cliente como de confianza o no de confianza para el nodo seleccionado.

  Por ejemplo, puede seleccionar **Untrust on displayed nodes** para agregar todos los nodos a la lista Untrusted Client Network y, a continuación, usar el conmutador junto a un nodo individual para agregar ese nodo a la lista Trusted Client Network.

> Use la barra de desplazamiento en la parte derecha de la tabla para asegurarse de que ha visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si introduce un **GW**, se mostrarán todos los nodos que tengan la cadena “GW” como parte de su nombre.

4. De manera opcional, seleccione cualquier puerto adicional que desee abrir en la red cliente que no sea de confianza. Estos puertos pueden proporcionar acceso a Grid Manager, al Tenant Manager o a ambos.

   Por ejemplo, puede que desee utilizar esta opción para asegurarse de que se puede acceder a Grid Manager en la red cliente con fines de mantenimiento.

> Estos puertos adicionales están abiertos en la red cliente, independientemente de si están cerrados en la pestaña Administrar acceso externo.

5. Seleccione **Guardar**.

   La nueva configuración del firewall se aplica y aplica inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Gestione inquilinos

Gestionar inquilinos: Información general

Como administrador de grid, debe crear y gestionar las cuentas de inquilino que utilizan los clientes S3 y Swift para almacenar y recuperar objetos.

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

¿Qué son las cuentas de inquilinos?

Una cuenta de inquilino permite usar la API DE REST de simple Storage Service (S3) o la API DE REST de Swift para almacenar y recuperar objetos en un sistema StorageGRID.

Cada cuenta de inquilino tiene grupos locales o federados, usuarios, bloques de S3 o contenedores Swift y objetos.

Las cuentas de arrendatario se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, pueden utilizarse 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 de cliente S3, puede utilizar bloques S3 y políticas de bloques para segregar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones de implementación "Bloques de S3 y políticas de bloques" si quiere 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.

Para obtener más información, consulte "Usar una cuenta de inquilino".

¿Cómo se crea una cuenta de inquilino?

Al crear una cuenta de inquilino, especifique la siguiente información:

- Información básica, incluido el nombre del inquilino, el tipo de cliente (S3 o Swift) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propio origen de identidad, usar S3 Select o usar una conexión de federación de grid.
- Acceso raíz inicial para el inquilino, basado en si el sistema StorageGRID utiliza usuarios y grupos locales, federación de identidades o inicio de sesión único (SSO).

Además, puede habilitar la configuración Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de arrendatario S3 necesitan cumplir con los requisitos normativos. Cuando se habilita el bloqueo de objetos S3, todas las cuentas de inquilinos S3 pueden crear y gestionar bloques conforme a la normativa.

¿Para qué se utiliza el gestor de inquilinos?

Después de crear la cuenta de inquilino, los usuarios de inquilino pueden iniciar sesión en el Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Utilice la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Supervise el uso del almacenamiento

Mientras que los usuarios inquilinos de S3 pueden crear y gestionar la clave de acceso y los depósitos S3 con el administrador de inquilinos, deben usar una aplicación cliente S3 para ingerir y gestionar objetos. Consulte "USE LA API DE REST DE S3" para obtener más detalles.

Los usuarios de Swift deben tener el permiso de acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso de acceso raíz no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Cree una cuenta de inquilino

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

Los pasos para crear una cuenta de inquilino varían en función de si "federación de identidades" y.. "inicio de sesión único" Están configurados y si la cuenta de Grid Manager que utiliza para crear la cuenta de arrendatario pertenece a un grupo de administración con el permiso acceso raíz.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso de acceso raíz o cuentas de inquilino.
- Si la cuenta de arrendatario utilizará el origen de identidad configurado para el Administrador de grid y desea otorgar permiso de acceso raíz para la cuenta de arrendatario a un grupo federado, ha importado ese grupo federado en el Gestor de grid. No es necesario asignar ningún permiso de Grid Manager a este grupo de administración. Consulte "Gestione los grupos de administradores".
- Si desea permitir que un inquilino de S3 clone los datos de su cuenta y replique objetos de bucket en otro grid mediante una conexión de federación de grid:
  - Ya tienes "se ha configurado la conexión de federación de grid".
  - El estado de la conexión es **Conectado**.
  - Tiene permiso de acceso raíz.
  - Ha revisado las consideraciones de "gestionar los inquilinos permitidos para la federación de grid".
  - Si la cuenta de arrendatario utilizará el origen de identidad configurado para Grid Manager, ha importado el mismo grupo federado en Grid Manager en ambas cuadrículas.

    Al crear el inquilino, seleccionará este grupo para que tenga el permiso inicial de acceso raíz para las cuentas de inquilino de origen y de destino.

    Si este grupo de administración no existe en ambas cuadrículas antes de crear el arrendatario, el arrendatario no se replica en el destino.

Acceda al asistente

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear**.

Introduzca los detalles

Pasos

1. Introduzca los detalles del arrendatario.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta único de 20 dígitos.
Descripción (opcional)	Descripción para ayudar a identificar al inquilino. Si va a crear un inquilino que utilizará una conexión de federación de grid, opcionalmente, utilice este campo para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: «Este inquilino se creó en Grid 1».
Tipo de cliente	El tipo de protocolo de cliente que usará este inquilino, ya sea **S3** o **Swift**. **Nota**: El soporte para aplicaciones cliente Swift ha sido obsoleto y será eliminado en una versión futura.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

2. Seleccione **continuar**.

Seleccione los permisos

Pasos

1. Opcionalmente, seleccione cualquier permiso que desee que tenga este inquilino.

> Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, seleccione el icono de ayuda de cada permiso.

Permiso	Si se ha seleccionado…
Permitir los servicios de plataforma	El inquilino puede usar servicios de plataforma S3 como CloudMirror. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
Usar origen de identidad propio	El inquilino puede configurar y gestionar su propio origen de identidad para usuarios y grupos federados. Esta opción está desactivada si tiene "SSO configurado" Para su sistema StorageGRID.
Permitir selección S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Consulte "Gestione S3 Select para cuentas de inquilinos". **Importante**: Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Permiso	Si se ha seleccionado…
Utilizar conexión de federación de grid	El inquilino puede utilizar una conexión de federación de grid. Seleccionando esta opción: • Hace que este arrendatario y todos los grupos de arrendatarios y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la cuadrícula *source*) a la otra cuadrícula de la conexión seleccionada (la cuadrícula *destination*). • Permite a este inquilino configurar la replicación entre grid entre bloques correspondientes en cada grid. Consulte "Gestione los inquilinos permitidos para la federación de grid". **Nota**: Solo puede seleccionar **Usar conexión de federación de grid** cuando está creando un nuevo inquilino de S3; no puede seleccionar este permiso para un inquilino existente.

2. Si seleccionó **Usar conexión de federación de grid**, seleccione una de las conexiones de federación de grid disponibles.

3. Seleccione **continuar**.

Defina el acceso raíz y cree un inquilino

Pasos

1. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza la federación de identidades, el inicio de sesión único (SSO) o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haga esto
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Seleccione **Crear arrendatario**.

   Aparece un mensaje Correcto y el nuevo arrendatario aparece en la página Inquilinos. Para saber cómo se ven los detalles de los inquilinos y se supervisa la actividad de los inquilinos, consulte "Supervise la actividad de los inquilinos".

3. Si seleccionó el permiso **Usar conexión de federación de grid** para el inquilino:

   a. Confirme que se ha replicado un inquilino idéntico en la otra cuadrícula de la conexión. Los inquilinos de ambas cuadrículas tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.

   > Si ve el mensaje de error «`El inquilino creado sin un clon`», consulte las instrucciones de "Solucionar errores de federación de grid".

   b. Si proporcionó una contraseña de usuario raíz local al definir el acceso raíz, "cambie la contraseña del usuario raíz local" para el inquilino replicado.

   > Un usuario raíz local no puede iniciar sesión en el gestor de inquilinos en la cuadrícula de destino hasta que se cambie la contraseña.

Iniciar sesión en el inquilino (opcional)

Según sea necesario, puede iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puede iniciar sesión en el inquilino más adelante. Los pasos de inicio de sesión dependen de si ha iniciado sesión en Grid Manager mediante el puerto predeterminado (443) o un puerto restringido. Consulte "Controle el acceso a un firewall externo".

Inicie sesión ahora

Si está usando…	Realice lo siguiente…
Puerto 443 y se establece una contraseña para el usuario raíz local	1. Seleccione **Iniciar sesión como root**. Al iniciar sesión, aparecen enlaces para configurar buckets, federación de identidades, grupos y usuarios. 2. Seleccione los vínculos para configurar la cuenta de arrendatario. Cada enlace abre la página correspondiente en el Administrador de arrendatarios. Para completar la página, consulte "instrucciones para el uso de cuentas de inquilino".

Si está usando…	Realice lo siguiente…
Puerto 443 y no ha establecido una contraseña para el usuario raíz local	Seleccione **Iniciar sesión** e introduzca las credenciales de un usuario en el grupo federado de acceso raíz.
Un puerto restringido	1. Selecciona **Finalizar** 2. Seleccione **Restringido** en la tabla de arrendatarios para obtener más información sobre el acceso 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

Inicie sesión más tarde

Si está usando…	Realice una de estas…
Puerto 443	• En Grid Manager, seleccione **ARRENDATARIOS** y seleccione **Iniciar sesión** a la derecha del nombre del arrendatario. • 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
Un puerto restringido	• En Grid Manager, seleccione **ARRENDATARIOS** y seleccione **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

Configure el inquilino

Siga las instrucciones de "Usar una cuenta de inquilino" Para gestionar usuarios y grupos de inquilinos, claves de acceso S3, bloques, servicios de plataforma, y clonación de cuentas y replicación entre grid.

Edite la cuenta de inquilino

Una cuenta de inquilino se puede editar para cambiar el nombre para mostrar, la cuota de almacenamiento o los permisos de inquilino.

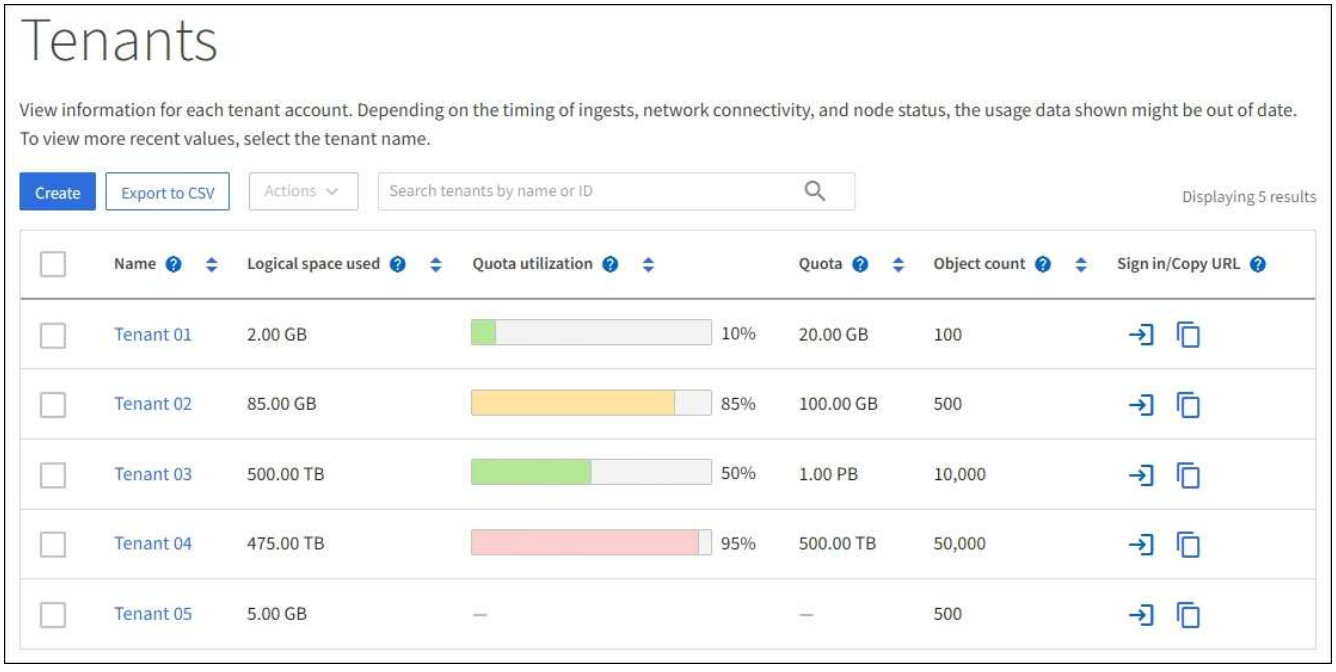
> Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puede editar los detalles del inquilino desde cualquier cuadrícula en la conexión. Sin embargo, los cambios que realice en una cuadrícula de la conexión no se copiarán en la otra cuadrícula. Si desea mantener los detalles del arrendatario exactamente sincronizados entre las cuadrículas, realice las mismas modificaciones en ambas cuadrículas. Consulte "Gestione los inquilinos permitidos para la conexión de federación de grid".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso de acceso raíz o cuentas de inquilino.

Pasos

1. Seleccione **ARRENDATARIOS**.



2. Localice la cuenta de inquilino que desea editar.

   Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.

3. Seleccione el inquilino. Puede realizar una de las siguientes acciones:
   - Selecciona la casilla de verificación para el inquilino y selecciona **Acciones** > **Editar**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Editar**.

4. Si lo desea, cambie los valores de estos campos:
   - **Nombre**
   - **Descripción**
   - **Cuota de almacenamiento**
5. Seleccione **continuar**.
6. Seleccione o borre los permisos para la cuenta de inquilino.
   - Si deshabilita **Servicios de plataforma** para un arrendatario que ya los está utilizando, los servicios que han configurado para sus cubos S3 dejarán de funcionar. No se envía ningún mensaje de error al inquilino. Por ejemplo, si el inquilino ha configurado la replicación de CloudMirror para un bloque de S3, podrán seguir almacenando objetos en el bloque, pero las copias de esos objetos ya no se realizarán en el bloque S3 externo que se hayan configurado como extremo. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
   - Cambie la configuración de **Uses own identity source** para determinar si la cuenta de inquilino utilizará su propia fuente de identidad o la fuente de identidad que se configuró para Grid Manager.

     Si **usa su propia fuente de identidad** 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.
     - Desactivado y no seleccionado, SSO está activado para el sistema StorageGRID. El inquilino debe utilizar el origen de identidad configurado para el administrador de grid.
   - Seleccione o desactive el permiso **Permitir S3 Select** según sea necesario. Consulte "Gestione S3 Select para cuentas de inquilinos".
   - Para eliminar el permiso **Use grid federation connection**, siga las instrucciones de "quitar el permiso de un inquilino para usar la federación de grid".

Cambiar la contraseña del usuario raíz local del inquilino

Puede que necesite cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz está bloqueado en la cuenta.

Antes de empezar

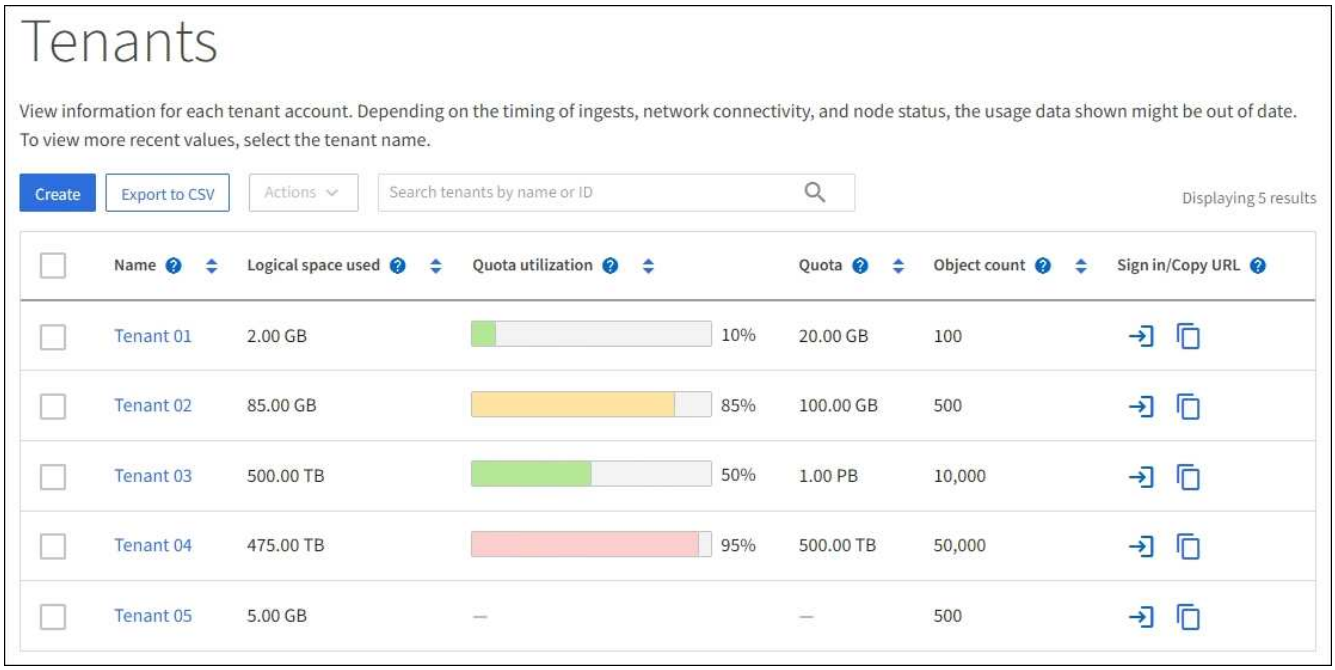
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta de inquilino. Para realizar tareas de usuario raíz, los usuarios deben pertenecer a un grupo federado que tenga el permiso acceso raíz para el arrendatario.

Pasos

1. Seleccione **ARRENDATARIOS**.



2. Seleccione la cuenta de inquilino. Puede realizar una de las siguientes acciones:
   - Selecciona la casilla de verificación para el inquilino y selecciona **Acciones** > **Cambiar contraseña raíz**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Acciones** > **Cambiar contraseña raíz**.
3. Introduzca la nueva contraseña de la cuenta de inquilino.
4. Seleccione **Guardar**.

Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar de forma permanente el acceso del inquilino al sistema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Quitó todos los bloques (S3), los contenedores (Swift) y los objetos asociados con la cuenta de inquilino.
- Si el inquilino puede usar una conexión de federación de grid, ha revisado las consideraciones para "Eliminación de un inquilino con el permiso de conexión Usar federación de grid".

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Localice la cuenta de inquilino o las cuentas que desea eliminar.

   Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.
3. Para eliminar varios inquilinos, selecciona las casillas de verificación y selecciona **Acciones** > **Eliminar**.
4. Para suprimir un solo inquilino, realice una de las siguientes acciones:
   - Selecciona la casilla de verificación y selecciona **Acciones** > **Eliminar**.

- Seleccione el nombre del inquilino para mostrar la página de detalles y, a continuación, seleccione * Acciones * > * Eliminar *.

5. Seleccione **Sí**.

Gestione los servicios de la plataforma

Gestionar servicios de plataforma para inquilinos: Información general

Si habilita los servicios de plataforma para cuentas de inquilino de S3, debe configurar su grid para que los inquilinos puedan acceder a los recursos externos necesarios para usar estos servicios.

¿Qué son los servicios de plataforma?

Los servicios de plataforma incluyen la replicación de CloudMirror, las notificaciones de eventos y el servicio de integración de búsqueda.

Estos servicios permiten a los inquilinos utilizar la siguiente funcionalidad con sus bloques S3:

- **Duplicación de CloudMirror**: El servicio de replicación de CloudMirror de StorageGRID se utiliza para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

  Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

  > La replicación de CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

  > 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 depósito se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon Simple Notification Service™ (Amazon SNS) externo especificado.

  Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

  > Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

- **Servicio de integración de búsqueda**: El servicio de integración de búsqueda se usa para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos utilizando el servicio externo.

  Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma ofrecen a los inquilinos la capacidad de usar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis con sus datos. Puesto que la ubicación objetivo para los servicios de plataforma suele ser externa a la implementación de StorageGRID, debe decidir si desea permitir a los inquilinos utilizar estos servicios. Si lo hace, debe habilitar el uso de servicios de plataforma al crear o editar cuentas de inquilino. También debe configurar la red de modo que los mensajes de servicios de plataforma que generan los inquilinos puedan llegar a sus destinos.

Recomendaciones para el uso de servicios de plataformas

Antes de utilizar los servicios de plataforma, tenga en cuenta las siguientes recomendaciones:

- Si un bloque de S3 del sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, también debe habilitar el control de versiones de bloques de S3 para el extremo de destino. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el extremo.
- No debe usar más de 100 inquilinos activos con solicitudes S3 que requieran la replicación, las notificaciones y la integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede dar como resultado un rendimiento del cliente S3 más lento.
- Las solicitudes a un punto final que no se puedan completar se pondrán en cola a un máximo de 500.000 solicitudes. Este límite se comparte por igual entre los inquilinos activos. Los nuevos inquilinos pueden exceder temporalmente este límite de 500.000 para que los nuevos inquilinos no sean penalizados injustamente.

Información relacionada

- "Usar una cuenta de inquilino"
- "Configure las opciones de proxy de almacenamiento"
- "Supervisar StorageGRID"

Red y puertos para servicios de plataforma

Si permite que un inquilino de S3 utilice los servicios de plataforma, debe configurar las redes para el grid para garantizar que los mensajes de servicios de plataforma se puedan entregar a sus destinos.

Puede habilitar los servicios de plataforma para una cuenta de inquilino de S3 al crear o actualizar la cuenta de inquilino. Si se habilitan los servicios de plataforma, el inquilino puede crear extremos que sirvan como destino para la replicación de CloudMirror, notificaciones de eventos o mensajes de integración de búsqueda desde sus bloques de S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los extremos de destino.

Por ejemplo, los inquilinos pueden configurar los siguientes tipos de extremos de destino:

- Un clúster de Elasticsearch alojado localmente
- Aplicación local que admite la recepción de mensajes de Simple Notification Service (Amazon SNS)
- Un bloque de S3 alojado localmente en la misma instancia de StorageGRID u otra

- Un extremo externo, como un extremo en Amazon Web Services.

Para garantizar que los mensajes de servicios de plataforma se puedan entregar, debe configurar la red o las redes que contienen los nodos de almacenamiento ADC. Debe asegurarse de que se pueden utilizar los siguientes puertos para enviar mensajes de servicios de plataforma a los extremos de destino.

De forma predeterminada, los mensajes de servicios de plataforma se envían a los siguientes puertos:

- **80**: Para los URI de punto final que comienzan con http
- **443**: Para los URI de punto final que comienzan con https

Los inquilinos pueden especificar un puerto diferente cuando crean o editan un extremo.

> Si se usa una puesta en marcha de StorageGRID como destino de la replicación de CloudMirror, podrían recibirse mensajes de replicación en un puerto distinto de 80 o 443. Compruebe que el puerto que se utiliza para S3 en la implementación de StorageGRID de destino se especifique en el extremo.

Si utiliza un servidor proxy no transparente, también debe hacerlo "Configure las opciones de proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

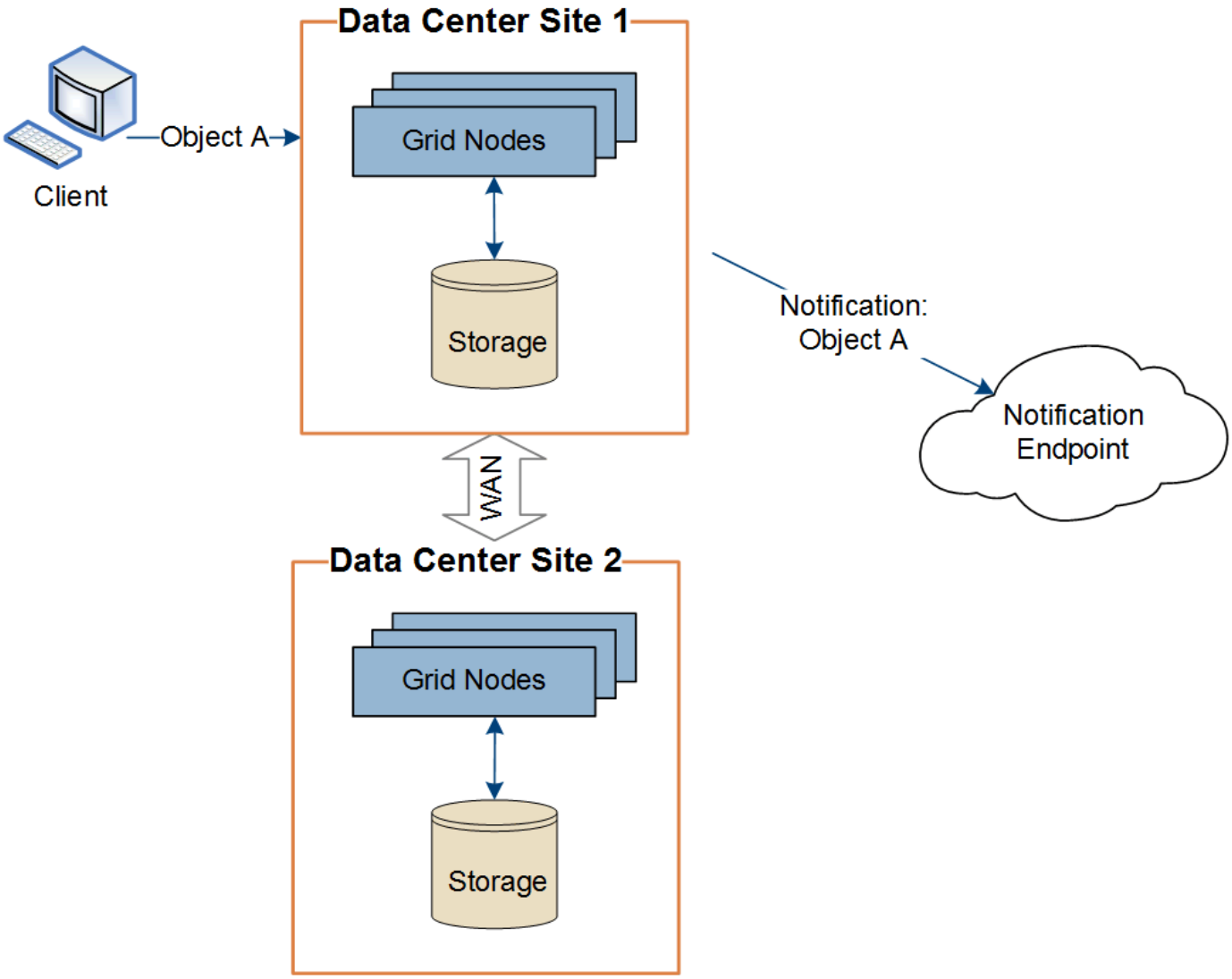
Información relacionada

- "Usar una cuenta de inquilino"

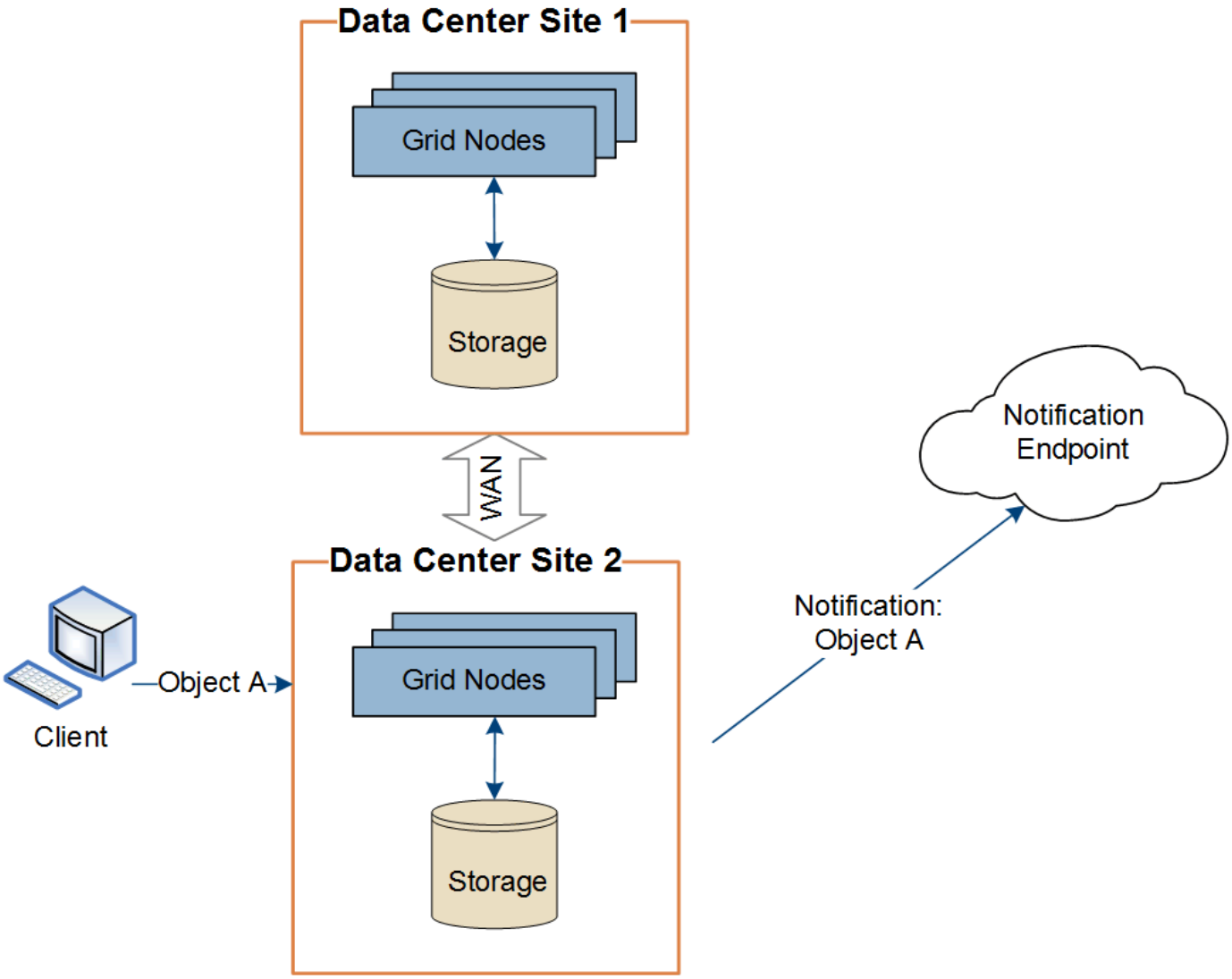
Entrega de mensajes de servicios de plataforma por sitio

Todas las operaciones de servicios de plataforma se realizan in situ.

Es decir, si un inquilino utiliza un cliente para realizar una operación S3 API Create en un objeto conectando a un nodo de puerta de enlace en el sitio 1 del centro de datos, se activa y envía la notificación acerca de esa acción desde el sitio 1 del centro de datos.



Si el cliente realiza posteriormente una operación de eliminación de API de S3 en ese mismo objeto desde el centro de datos Sitio 2, se activa y envía la notificación sobre la acción de eliminación desde el centro de datos Sitio 2.



Asegúrese de que la red de cada sitio esté configurada de modo que los mensajes de servicios de la plataforma se puedan entregar a sus destinos.

Solucione problemas de servicios de plataforma

Los extremos utilizados en los servicios de plataforma los crean y mantienen los usuarios de arrendatarios en el Administrador de arrendatarios; sin embargo, si un arrendatario tiene problemas al configurar o utilizar servicios de plataforma, puede utilizar el Administrador de grid para ayudar a resolver el problema.

Problemas con nuevos extremos

Para que un inquilino pueda utilizar los servicios de plataforma, deben crear uno o varios extremos mediante el administrador de inquilinos. Cada extremo representa un destino externo para un servicio de plataforma, como un bloque de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple o un clúster de Elasticsearch alojado localmente o en AWS. Cada extremo incluye la ubicación del recurso externo y las credenciales que se necesitan para acceder a ese recurso.

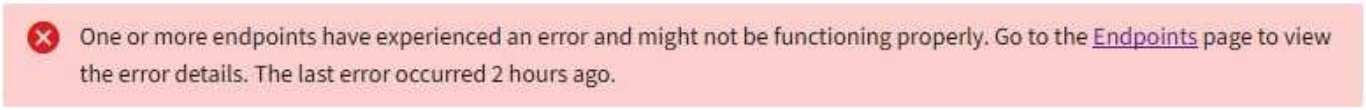
Cuando un inquilino crea un extremo, el sistema StorageGRID valida que existe el extremo y que se puede acceder a él utilizando las credenciales que se han especificado. La conexión con el extremo se valida desde un nodo en cada sitio.

Si falla la validación del punto final, un mensaje de error explica por qué falló la validación del punto final. El usuario inquilino debe resolver el problema y, a continuación, intentar crear el extremo de nuevo.

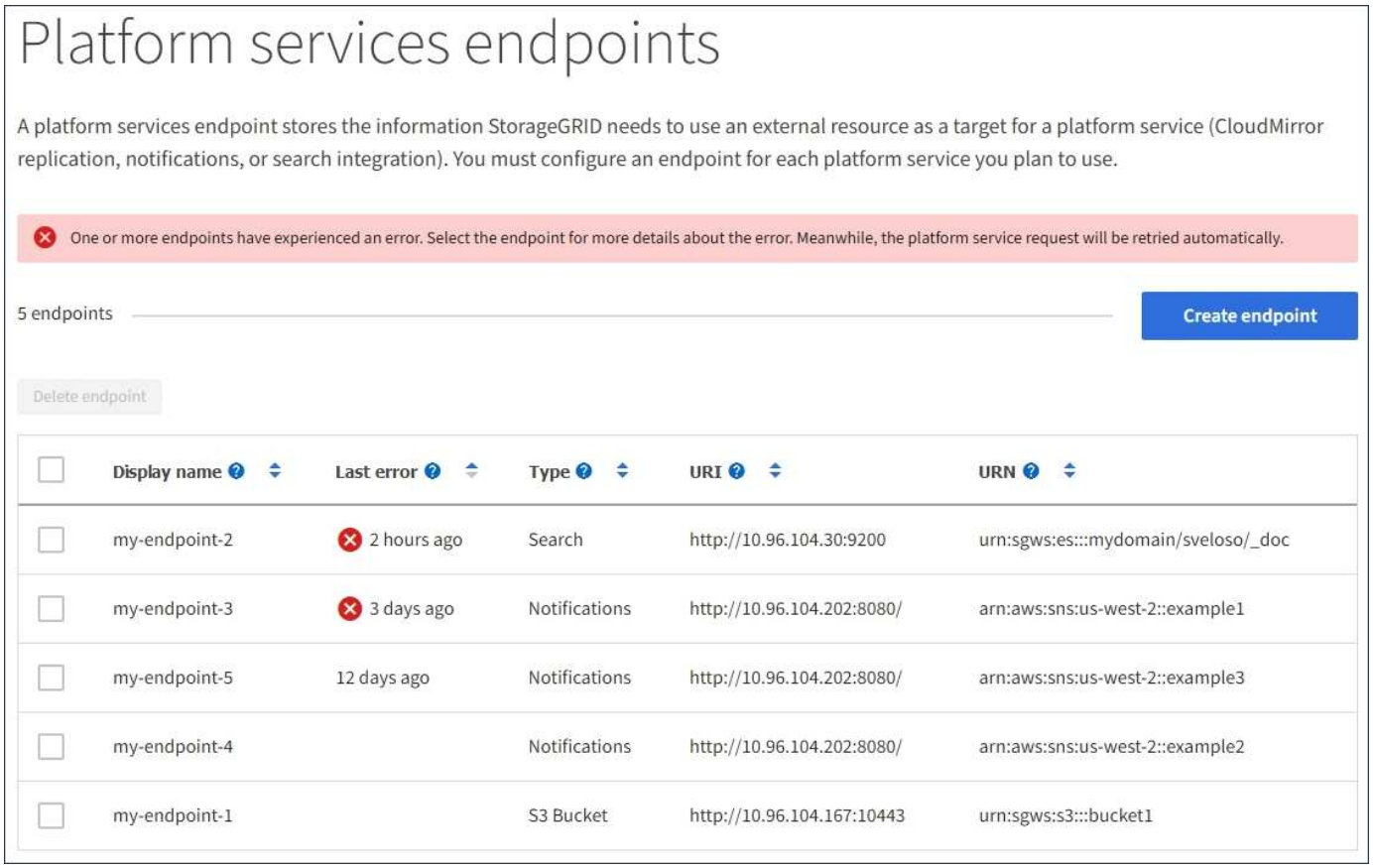
La creación de punto final fallará si los servicios de plataforma no están activados para la cuenta de inquilino.

Problemas con los extremos existentes

Si se produce un error cuando StorageGRID intenta llegar a un punto final existente, se muestra un mensaje en el panel de control del gestor de inquilinos.



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 ha configurado un "Proxy de almacenamiento" Entre los nodos de almacenamiento y los extremos del servicio de plataforma, se podrían producir errores si el servicio de proxy no permite mensajes de StorageGRID. Para resolver estos problemas, compruebe la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determine si se ha producido un error

Si se ha producido algún error de punto final en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página endpoints para ver más detalles sobre el error.

Error en las operaciones del cliente

Algunos problemas de los servicios de plataforma pueden provocar errores en las operaciones del cliente en el bloque de S3. Por ejemplo, las operaciones del cliente S3 fallarán si se detiene el servicio interno Replicated State Machine (RSM) o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node*** > **SSM** > **Servicios**.

Errores de punto final recuperables e irrecuperables

Una vez creados los extremos, los errores de solicitud de servicio de la plataforma pueden producirse por varios motivos. Algunos errores se pueden recuperar con la intervención del usuario. Por ejemplo, pueden producirse errores recuperables por los siguientes motivos:

- Las credenciales del usuario se han eliminado o han caducado.
- El bloque de destino no existe.
- No se puede entregar la notificación.

Si StorageGRID encuentra un error recuperable, la solicitud de servicio de la plataforma se reintentará hasta que se complete correctamente.

Otros errores son irrecuperables. Por ejemplo, se produce un error irrecuperable si se elimina el extremo.

Si StorageGRID encuentra un error de punto final irrecuperable, la alarma heredada total de eventos (SMTT) se activa en el Administrador de grid. Para ver la alarma de legado total de eventos:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***node*** > **SSM** > **Eventos**.
3. Ver último evento en la parte superior de la tabla.

   Los mensajes de eventos también se muestran en la `/var/local/log/bycast-err.log`.

4. Siga las instrucciones proporcionadas en el contenido de la alarma SMTT para corregir el problema.
5. Seleccione la ficha **Configuración** para restablecer los recuentos de eventos.
6. Notifique al inquilino los objetos cuyos mensajes de servicios de plataforma no se han entregado.

7. Indique al inquilino que vuelva a activar la replicación o notificación fallida actualizando los metadatos o las etiquetas del objeto.

   El arrendatario puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

Los mensajes de servicios de 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 los mensajes de servicios de plataforma no se pueden entregar debido a un error irrecuperable, la alarma de legado de Total Events (SMTT) se activa en Grid Manager.

Rendimiento más lento para las solicitudes de servicio de la plataforma

El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino.

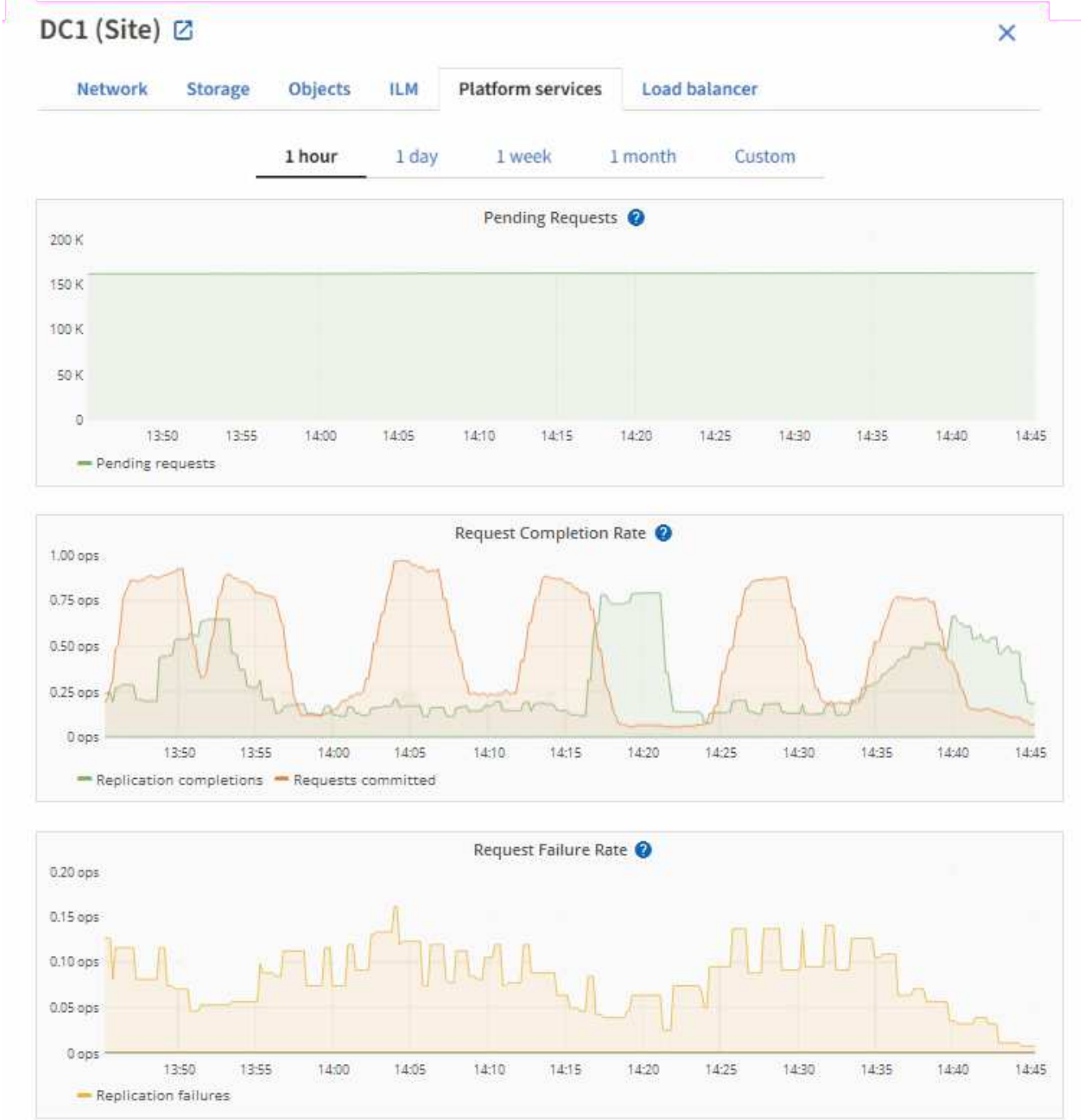
El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro.

Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Las solicitudes de servicio de la plataforma fallan

Para ver la tasa de fallos de solicitud para servicios de plataforma:

1. Seleccione **NODES**.
2. Seleccione ***site*** > **Servicios de plataforma**.
3. Vea el gráfico de tasa de errores de solicitud.



Alerta de servicios de plataforma no disponibles

La alerta **Servicios de plataforma no disponibles** indica que no se pueden realizar operaciones de servicio de plataforma en un sitio porque hay demasiados nodos de almacenamiento con el servicio RSM en ejecución o disponibles.

El servicio RSM garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos extremos.

Para resolver esta alerta, determine qué nodos de almacenamiento del sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC). A continuación, asegúrese de que la mayoría simple de estos nodos de almacenamiento esté en funcionamiento y disponible.

Si se produce un error en más de un nodo de almacenamiento que contiene el servicio RSM de un sitio, perderá las solicitudes de servicio de plataforma pendientes para ese sitio.

Orientación adicional para la solución de problemas para extremos de servicios de la plataforma

Para obtener información adicional, consulte **Use una cuenta de inquilino › Solucionar problemas de los extremos de servicios de la plataforma**.

Información relacionada

- "Solucionar los problemas del sistema StorageGRID"

Gestione S3 Select para cuentas de inquilinos

Puede permitir que determinados inquilinos S3 usen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select proporciona una forma eficiente de buscar en grandes cantidades de datos sin tener que implementar una base de datos y recursos asociados para permitir las búsquedas. También reduce el coste y la latencia de la recuperación de datos.

¿Qué es S3 Select?

S3 Select permite que los clientes S3 utilicen solicitudes SelectObjectContent para filtrar y recuperar solo los datos necesarios de un objeto. La implementación de StorageGRID de S3 Select incluye un subconjunto de comandos y funciones de S3 Select.

Consideraciones y requisitos para usar S3 Select

Requisitos de administración de grid

El administrador de grid debe conceder a los inquilinos la Capacidad Select S3. Seleccione **permitir selección de S3** cuando "crear un inquilino" o. "edición de un arrendatario".

Requisitos de formato de objeto

El objeto que desea consultar debe tener uno de los siguientes formatos:

- **CSV**. Se puede utilizar tal cual o comprimir en archivos GZIP o bzip2.
- **Parquet**. Requisitos adicionales para objetos de parquet:
  - S3 Select solo admite la compresión en columnas usando GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos de parquet.
  - S3 La selección no es compatible con la salida de parquet. Debe especificar el formato de salida como CSV o JSON.
  - El tamaño máximo del grupo de filas sin comprimir es de 512 MB.
  - Debe utilizar los tipos de dato especificados en el esquema del objeto.
  - No puede utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.

Requisitos de los extremos

La solicitud SelectObjectContent debe enviarse a un "Extremo del equilibrador de carga de StorageGRID".

Los nodos de administración y puerta de enlace utilizados por el punto final deben ser uno de los siguientes:

- Nodo de dispositivo SG100 o SG1000
- Nodo de software basado en VMware
- Nodo bare metal que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

Las consultas no pueden enviarse directamente a los nodos de almacenamiento.

> Las solicitudes SelectObjectContent pueden reducir el rendimiento de equilibrio de carga de todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Consulte "Instrucciones para usar S3 Select".

Para ver "Gráficos Grafana" Para las operaciones de S3 Select a lo largo del tiempo, seleccione **SUPPORT** > **Tools** > **Metrics** en Grid Manager.

Configurar conexiones de cliente

Configurar las conexiones del cliente S3 y Swift: Información general

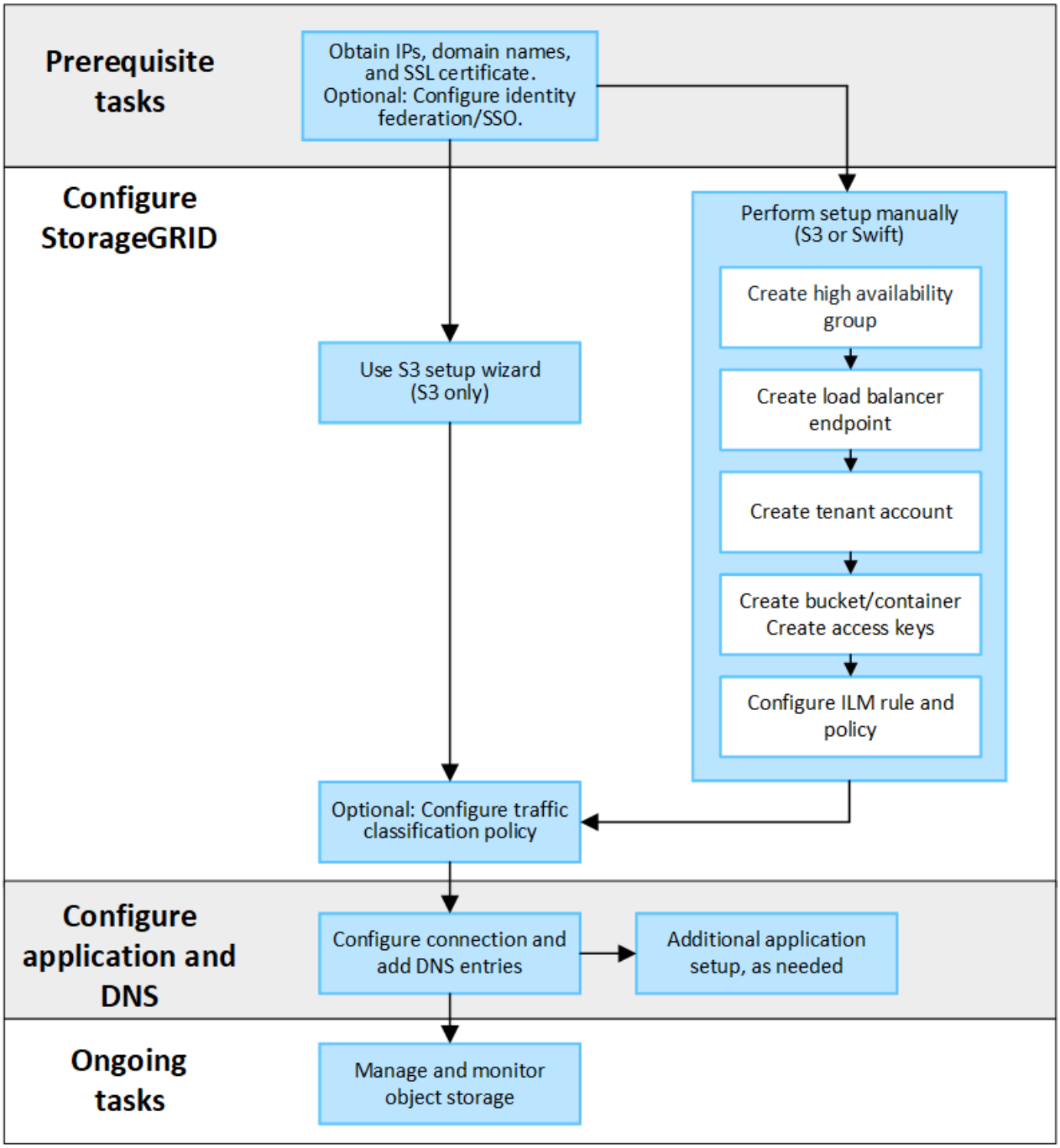
Como administrador de grid, puede gestionar las opciones de configuración que controlan cómo las aplicaciones cliente S3 y Swift se conectan al sistema StorageGRID para almacenar y recuperar los datos.

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Flujo de trabajo de configuración

Como se muestra en el diagrama de flujo de trabajo, hay cuatro pasos principales para conectar StorageGRID a cualquier aplicación S3 o Swift:

1. Realice tareas de requisitos previos en StorageGRID, según cómo se conectará la aplicación cliente a StorageGRID.
2. Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la cuadrícula. Puede utilizar el asistente de configuración de S3 o configurar cada entidad de StorageGRID manualmente.
3. Use la aplicación S3 o Swift para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que desee utilizar.
4. Realice tareas continuas en la aplicación y en StorageGRID para gestionar y supervisar el almacenamiento de objetos a lo largo del tiempo.



Información necesaria para asociar StorageGRID a una aplicación cliente

Para poder asociar StorageGRID a una aplicación cliente S3 o Swift, debe realizar pasos de configuración en StorageGRID y obtener cierto valor.

¿Qué valores necesito?

La tabla siguiente muestra los valores que debe configurar en StorageGRID y donde los utiliza la aplicación S3 o Swift y el servidor DNS.

Valor	Donde se configura el valor	Donde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del equilibrador de carga	Aplicación cliente
Certificado SSL	StorageGRID > Punto final del equilibrador de carga	Aplicación cliente
Nombre del servidor (FQDN)	StorageGRID > Punto final del equilibrador de carga	• Aplicación cliente • Entrada DNS
S3 ID de clave de acceso y clave de acceso secreta	StorageGRID > inquilino y bloque	Aplicación cliente
Nombre de cubo/contenedor	StorageGRID > inquilino y bloque	Aplicación cliente

¿Cómo obtengo estos valores?

Dependiendo de sus requisitos, puede hacer cualquiera de los siguientes pasos para obtener la información que necesita:

- * Utilice el "S3 Asistente de configuración"*. El asistente de configuración de S3 le ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puede utilizar al configurar la aplicación S3. El asistente le guiará por los pasos necesarios y le ayudará a garantizar que la configuración cumple las prácticas recomendadas de StorageGRID.

  Si está configurando una aplicación S3, se recomienda utilizar el asistente de configuración de S3 a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- * Utilice el "Asistente de configuración de FabricPool"*. De forma similar al asistente de configuración de S3, el asistente de configuración de FabricPool ayuda a configurar rápidamente los valores necesarios y genera un archivo que se puede usar al configurar un nivel de cloud de FabricPool en ONTAP.

  Si va a utilizar StorageGRID como sistema de almacenamiento de objetos para un nivel cloud de FabricPool, se recomienda utilizar el asistente de configuración de FabricPool, a menos que sepa que tiene requisitos especiales o que su implementación requerirá una gran personalización.

- **Configurar artículos manualmente**. Si se conecta a una aplicación Swift (o se conecta a una aplicación S3 y prefiere no utilizar el asistente de configuración S3), puede obtener los valores requeridos realizando la configuración manualmente. Siga estos pasos:

  a. Configure el grupo de alta disponibilidad (HA) que desee utilizar para la aplicación S3 o Swift. Consulte "Configuración de grupos de alta disponibilidad".

  b. Cree el extremo del equilibrador de carga que utilizará la aplicación S3 o Swift. Consulte "Configurar puntos finales del equilibrador de carga".

c. Cree la cuenta de inquilino que utilizará la aplicación S3 o Swift. Consulte "Cree una cuenta de inquilino".

d. Para un inquilino de S3, inicie sesión en la cuenta de inquilino y genere un ID de clave de acceso y una clave de acceso secreta para cada usuario que acceda a la aplicación. Consulte "Cree sus propias claves de acceso".

e. Cree uno o varios bloques de S3 o contenedores Swift dentro de la cuenta de inquilino. Para S3, consulte "Crear bloque de S3". En el caso de Swift, utilice el "Solicitud de contenedor PUT".

f. Para agregar instrucciones de ubicación específicas para los objetos que pertenecen al inquilino o bloque/contenedor nuevo, cree una regla de ILM nueva y active una nueva política de ILM para utilizar esa regla. Consulte "Cree la regla de ILM" y.. "Cree una política de ILM".

Utilice el asistente de configuración de S3

Utilice el asistente de configuración de S3: Consideraciones y requisitos

Puede usar el asistente de configuración de S3 para configurar StorageGRID como el sistema de almacenamiento de objetos de una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 le guiará en cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargará archivos que puede utilizar para introducir valores en la aplicación S3. Utilice el asistente para configurar su sistema con mayor rapidez y asegurarse de que su configuración cumple las prácticas recomendadas de StorageGRID.

Si tiene el permiso de acceso de raíz, puede completar el asistente de configuración de S3 cuando empiece a utilizar el Administrador de grid de StorageGRID, o bien puede acceder al asistente y completarlo en cualquier momento posterior. En función de los requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y, a continuación, utilizar el asistente para ensamblar los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, confirme que ha completado estos requisitos previos.

Obtenga direcciones IP y configure interfaces VLAN

Si va a configurar un grupo de alta disponibilidad (HA), sabrá a qué nodos se conectará la aplicación S3 y a qué red StorageGRID se utilizará. También sabe qué valores introducir para la subred CIDR, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de la aplicación S3, ya ha configurado la interfaz VLAN. Consulte "Configure las interfaces VLAN".

Configurar la federación de identidades y SSO

Si tiene pensado utilizar la federación de identidades o el inicio de sesión único (SSO) para el sistema StorageGRID, tiene activadas estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará la aplicación S3. Consulte "Usar la federación de identidades" y.. "Configurar el inicio de sesión único".

Obtener y configurar nombres de dominio

Sabe qué nombre de dominio completo (FQDN) debe utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree con el asistente.

Si tiene pensado utilizar S3 solicitudes virtuales de estilo hospedado, debería tener "Nombres de dominio de punto final S3 configurados". Se recomienda utilizar solicitudes virtuales de estilo alojado.

Revisión de los requisitos del equilibrio de carga y del certificado de seguridad

Si tiene pensado utilizar el equilibrador de carga de StorageGRID, ha revisado las consideraciones generales sobre el equilibrio de carga. Tiene los certificados que cargará o los valores necesarios para generar un certificado.

Si planea utilizar un punto final de equilibrio de carga externo (de terceros), tiene el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Configure cualquier conexión de federación de grid

Si desea permitir que el inquilino S3 clone los datos de la cuenta y replique objetos del bloque en otra cuadrícula mediante una conexión de federación de grid, antes de iniciar el asistente confirme lo siguiente:

- Ya tienes "se ha configurado la conexión de federación de grid".
- El estado de la conexión es **Conectado**.
- Tiene permiso de acceso raíz.

Acceda al asistente de configuración de S3 y complete este

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID para su uso con una aplicación S3. El asistente de configuración proporciona los valores que la aplicación necesita para acceder a un bucket de StorageGRID y guardar objetos.

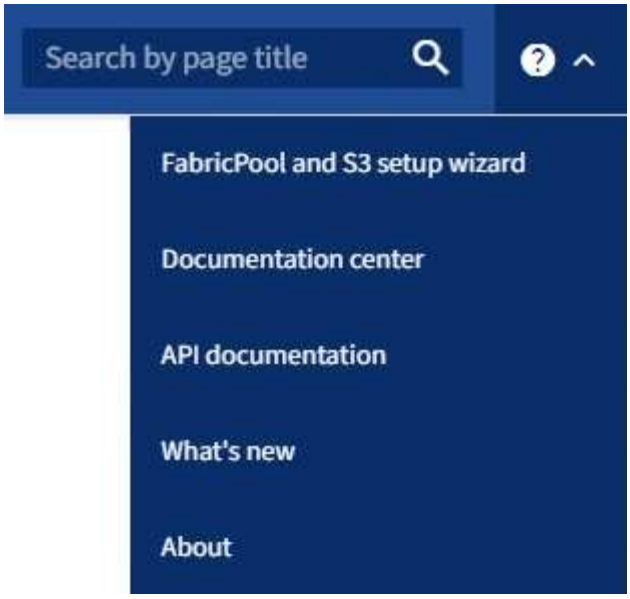
Antes de empezar

- Usted tiene la "Permiso de acceso raíz".
- Ha revisado el "consideraciones y requisitos" para utilizar el asistente.

Acceda al asistente

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Si el banner del asistente de configuración **FabricPool y S3** aparece en el panel de control, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el icono de ayuda en la barra de encabezado del Administrador de cuadrículas y seleccione **FabricPool y el asistente de configuración S3**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Paso 1 de 6: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contiene cada uno de ellos el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela, nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener las conexiones de datos de S3 GbE disponibles. Si falla la interfaz activa del grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad".

Pasos

1. Si va a utilizar un equilibrador de carga externo, no es necesario crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a. Paso 2 de 6: Configurar punto final de equilibrio de carga.
2. Para usar el equilibrador de carga de StorageGRID, es posible crear un grupo de alta disponibilidad nuevo o usar un grupo de alta disponibilidad existente.

Crear grupo de alta disponibilidad

a. Para crear un nuevo grupo HA, selecciona **Crear grupo HA**.

b. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

d. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

e. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en la notación CIDR — una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para volver al asistente de configuración S3.

g. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Use el grupo de alta disponibilidad existente

a. Para usar un grupo HA existente, seleccione el nombre del grupo HA en el **Seleccione un grupo HA**.

b. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Paso 2 de 6: Configurar punto final de equilibrio de carga

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Puede usar el servicio de equilibrador de carga de StorageGRID, que existe en todos los nodos de administración y puerta de enlace, o puede conectarse a un equilibrador de carga externo (de terceros). Se recomienda utilizar el equilibrador de carga de StorageGRID.

Para obtener más detalles sobre esta tarea, consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Para usar el servicio de Equilibrador de Carga de StorageGRID, seleccione la pestaña **Equilibrador de Carga de StorageGRID** y, a continuación, cree o seleccione el punto final del equilibrador de carga que desea utilizar. Para usar un equilibrador de carga externo, selecciona la pestaña **Equilibrador de carga externo** y proporciona detalles sobre el sistema que ya has configurado.

Crear punto final

Pasos

1. Para crear un punto final de equilibrio de carga, selecciona **Crear punto final**.
2. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que estos puertos están reservados en los nodos de Admin. **Nota:** Los puertos utilizados por otros servicios de red no están permitidos. Consulte"Referencia de puerto de red".
Tipo de cliente	Debe ser **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

3. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final—utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Opción	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.

Opción	Descripción
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

4. Para el paso de acceso de arrendatario, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

5. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener detalles sobre lo que se debe introducir.
Usar certificado StorageGRID S3 y Swift	Utilice esta opción solo si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados API S3 y Swift" para obtener más detalles.

6. Seleccione **Finalizar** para volver al asistente de configuración de S3.
7. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

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

Utilizar punto final de equilibrio de carga existente

Pasos

1. Para usar un punto final existente, seleccione su nombre en el **Seleccione un punto final de equilibrio de carga**.
2. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Utilizar equilibrador de carga externo

Pasos

1. Para utilizar un equilibrador de carga externo, complete los siguientes campos.

Campo	Descripción
FQDN	Nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	Número de puerto que utilizará la aplicación S3 para conectarse al equilibrador de carga externo.
Certificado	Copie el certificado del servidor para el equilibrador de carga externo y péguelo en este campo.

2. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Paso 3 de 6: Crear inquilino y bloque

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, bloques, objetos y un conjunto específico de funcionalidades. Debe crear el arrendatario antes de crear el depósito que utilizará la aplicación S3 para almacenar sus objetos.

Un bucket es un contenedor que se usa para almacenar los objetos y los metadatos de objetos de un inquilino. Aunque es posible que algunos inquilinos tengan muchos buckets, el asistente le ayuda a crear un inquilino y un bloque de la forma más rápida y sencilla. Puede utilizar el Gestor de inquilinos más adelante para agregar los depósitos adicionales que necesite.

Puede crear un nuevo inquilino para que lo utilice esta aplicación S3. De forma opcional, también puede crear un bucket para el nuevo arrendatario. Por último, puede permitir al asistente crear las claves de acceso S3 para el usuario raíz del inquilino.

Para obtener más detalles sobre esta tarea, consulte "Cree una cuenta de inquilino" y.."Crear bloque de S3".

Pasos

1. Seleccione **Crear arrendatario**.
2. Para los pasos Enter details, introduzca la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.

Campo	Descripción
Descripción (opcional)	Descripción para ayudar a identificar al inquilino.
Tipo de cliente	El tipo de protocolo de cliente que utilizará este inquilino. Para el asistente de configuración S3, se selecciona **S3** y el campo está desactivado.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

3. Seleccione **continuar**.
4. Opcionalmente, seleccione cualquier permiso que desee que tenga este inquilino.

> Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, seleccione el icono de ayuda de cada permiso.

Permiso	Si se ha seleccionado…
Permitir los servicios de plataforma	El inquilino puede usar servicios de plataforma S3 como CloudMirror. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
Usar origen de identidad propio	El inquilino puede configurar y gestionar su propio origen de identidad para usuarios y grupos federados. Esta opción está desactivada si tiene "SSO configurado" Para su sistema StorageGRID.
Permitir selección S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Consulte "Gestione S3 Select para cuentas de inquilinos". **Importante**: Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Permiso	Si se ha seleccionado…
Utilizar conexión de federación de grid	El inquilino puede utilizar una conexión de federación de grid. Seleccionando esta opción: • Hace que este arrendatario y todos los grupos de arrendatarios y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la cuadrícula *source*) a la otra cuadrícula de la conexión seleccionada (la cuadrícula *destination*). • Permite a este inquilino configurar la replicación entre grid entre bloques correspondientes en cada grid. Consulte "Gestione los inquilinos permitidos para la federación de grid". **Nota**: Solo puede seleccionar **Usar conexión de federación de grid** cuando está creando un nuevo inquilino de S3; no puede seleccionar este permiso para un inquilino existente.

5. Si seleccionó **Usar conexión de federación de grid**, seleccione una de las conexiones de federación de grid disponibles.
6. Defina el acceso raíz para la cuenta de inquilino en función de si utiliza el sistema StorageGRID "federación de identidades", "Inicio de sesión único (SSO)", o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

7. Si desea que el asistente cree el ID de clave de acceso y la clave de acceso secreta para el usuario root, seleccione **Crear clave de acceso S3 de usuario root automáticamente**.

Seleccione esta opción si el único usuario para el arrendatario será el usuario root. Si otros usuarios usarán este inquilino, use el Gestor de inquilinos para configurar claves y permisos.

8. Seleccione **continuar**.
9. Para el paso de creación de depósito, opcionalmente cree un depósito para los objetos del inquilino. De lo contrario, seleccione **Crear inquilino sin cubo** para ir al paso de descarga de datos.

Si S3 Object Lock está habilitado para la cuadrícula, el depósito creado en este paso no tiene S3 Object Lock habilitado. Si necesita usar un cubo de bloqueo de objetos S3 para esta aplicación S3, seleccione **Crear inquilino sin cubo**. A continuación, utilice Gestor de inquilinos para "cree el cucharón" en su lugar.

a. Introduzca el nombre del depósito que utilizará la aplicación S3. Por ejemplo: `S3-bucket`.

No puede cambiar el nombre del bloque después de crear el bloque.

b. Seleccione la **Región** para este cubo.

Utilice la región predeterminada (us-east-1) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del bloque.

c. Seleccione **Activar el control de versiones de objetos** si desea almacenar cada versión de cada objeto en este depósito.

d. Seleccione **Crear inquilino y cubo** y vaya al paso de descarga de datos.

Paso 4 de 6: Descargar datos

En el paso de descarga de datos, puede descargar uno o dos archivos para guardar los detalles de lo que acaba de configurar.

Pasos

1. Si seleccionó **Crear clave de acceso S3 de usuario root automáticamente**, realice una o ambas de las siguientes acciones:
   - Selecciona **Descargar claves de acceso** para descargar a. `.csv` El archivo que contiene el nombre de la cuenta de inquilino, el ID de clave de acceso y la clave de acceso secreta.
   - Seleccione el icono de copia ( ) Para copiar el ID de clave de acceso y la clave de acceso secreta en el portapapeles.
2. Seleccione **Descargar valores de configuración** para descargar a. `.txt` archivo que contiene la configuración del extremo del balanceador de carga, el inquilino, el bloque y el usuario raíz.
3. Guarde esta información en una ubicación segura.

No cierre esta página hasta que haya copiado ambas claves de acceso. Las teclas no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura, ya que se puede utilizar para obtener datos de su sistema StorageGRID.

4. Si se le solicita, seleccione la casilla de verificación para confirmar que ha descargado o copiado las claves.
5. Seleccione **Continuar** para ir a la regla de ILM y paso de política.

Paso 5 de 6: Revise la regla de ILM y la política de ILM para S3

Las reglas de gestión de la vida útil de la información controlan la ubicación, la duración y el comportamiento de procesamiento de todos los objetos del sistema StorageGRID. La política de ILM incluida con StorageGRID hace dos copias replicadas de todos los objetos. Esta política está en vigor hasta que cree una nueva política propuesta y la active.

Pasos

1. Revise la información proporcionada en la página.
2. Si desea agregar instrucciones específicas para los objetos que pertenecen al nuevo arrendatario o depósito, cree una nueva regla y una nueva política. Consulte "Cree la regla de ILM" y.. "Cree una política de ILM: Descripción general".
3. Seleccione **He revisado estos pasos y entiendo lo que tengo que hacer**.
4. Seleccione la casilla de verificación para indicar que comprende qué hacer a continuación.
5. Selecciona **Continuar** para ir a **Resumen**.

Paso 6 de 6: Resumen de la revisión

Pasos

1. Revise el resumen.
2. Anote los detalles en los siguientes pasos, que describen la configuración adicional que puede ser necesaria antes de conectarse al cliente S3. Por ejemplo, si selecciona **Iniciar sesión como root**, accederá al gestor de inquilinos, donde podrá agregar usuarios de inquilinos, crear depósitos adicionales y actualizar la configuración del depósito.
3. Seleccione **Finalizar**.
4. Configure la aplicación mediante el archivo descargado de StorageGRID o los valores obtenidos manualmente.

Gestionar grupos de alta disponibilidad

Gestionar grupos de alta disponibilidad: Descripción general

Puede agrupar las interfaces de red de varios nodos de administrador y puerta de enlace en un grupo de alta disponibilidad (ha). Si la interfaz activa del grupo de alta disponibilidad falla, una interfaz de backup puede administrar la carga de trabajo.

¿Qué es un grupo de alta disponibilidad?

Puede usar grupos de alta disponibilidad para proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift o proporcionar conexiones de alta disponibilidad a Grid Manager y Tenant Manager.

Cada grupo de alta disponibilidad proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de ALTA DISPONIBILIDAD que incluyen nodos de puerta de enlace, nodos de administrador o ambos proporcionan conexiones de datos con alta disponibilidad para los clientes S3 y Swift.
- Los grupos DE ALTA DISPONIBILIDAD que incluyen solo los nodos de administrador proporcionan conexiones de alta disponibilidad con el administrador de grid y el administrador de inquilinos.
- Un grupo de alta disponibilidad que sólo incluye dispositivos SG100 o SG1000 y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad "Inquilinos de S3 que usan S3 Select". Se recomienda a los grupos de ALTA DISPONIBILIDAD cuando se usa S3 Select, pero no es obligatorio.

¿Cómo se crea un grupo de alta disponibilidad?

1. Debe seleccionar una interfaz de red para uno o más nodos de administrador o nodos de puerta de enlace. Puede usar una interfaz de red de cuadrícula (eth0), una interfaz de red de cliente (eth2), una

interfaz VLAN o una interfaz de acceso que haya agregado al nodo.

> No puede agregar una interfaz a un grupo de alta disponibilidad si tiene una dirección IP asignada por DHCP.

2. Se especifica una interfaz para ser la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.
3. El orden de prioridad de las interfaces de copia de seguridad se determina.
4. Asigne una a 10 direcciones IP virtuales (VIP) al grupo. Las aplicaciones cliente pueden utilizar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para ver instrucciones, consulte "Configuración de grupos de alta disponibilidad".

¿Cuál es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo ha se añaden a la interfaz principal, que es la primera interfaz en el orden de prioridad. Siempre que la interfaz principal siga estando disponible, se utiliza cuando los clientes se conectan a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz primaria es la interfaz "'activa'" del grupo.

Del mismo modo, durante el funcionamiento normal, cualquier interfaz con menor prioridad para el grupo ha actúa como interfaces «'backup'». Estas interfaces de copia de seguridad no se utilizan a menos que la interfaz primaria (actualmente activa) deje de estar disponible.

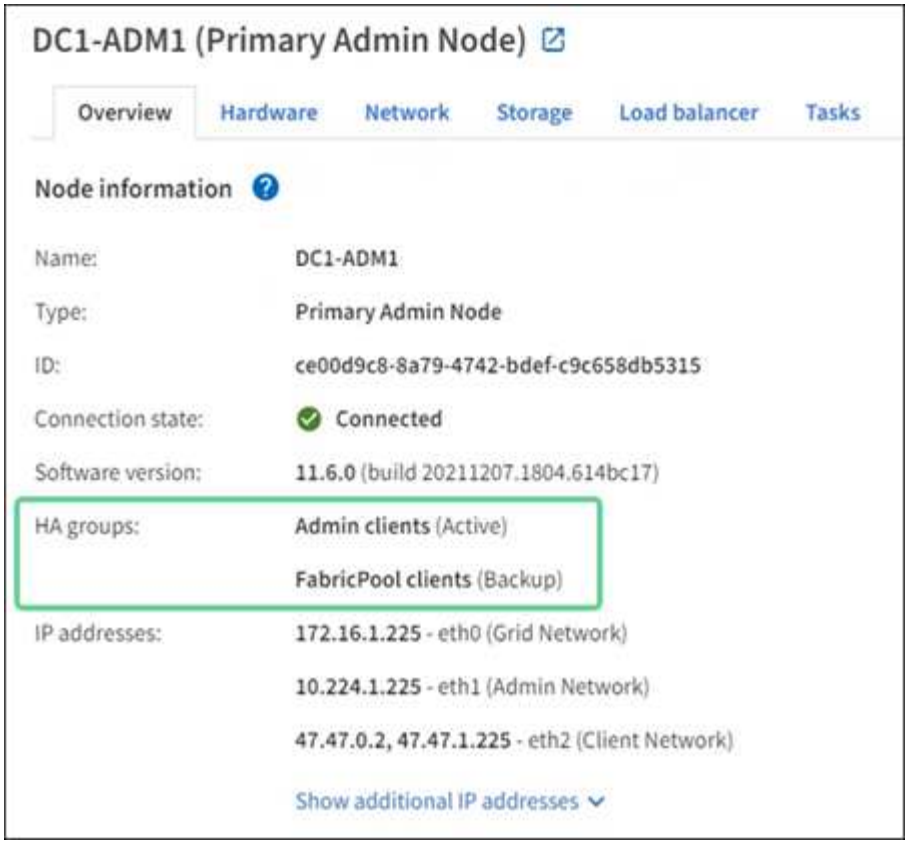
Ver el estado actual del grupo de alta disponibilidad de un nodo

Para ver si un nodo está asignado a un grupo ha y determinar su estado actual, seleccione **NODES** > ***node***.

Si la ficha **Descripción general** incluye una entrada para **grupos ha**, el nodo se asigna a los grupos ha enumerados. El valor después de que el nombre del grupo sea el estado actual del nodo del grupo de alta disponibilidad:

- **Activo**: El grupo ha se está alojando actualmente en este nodo.
- **Copia de seguridad**: El grupo ha no está utilizando actualmente este nodo; se trata de una interfaz de copia de seguridad.
- **Detenido**: El grupo HA no se puede alojar en este nodo porque el servicio High Availability (Keepalived) se ha detenido manualmente.
- **Fallo**: El grupo HA no se puede alojar en este nodo debido a uno o más de los siguientes:
  - El servicio Load Balancer (nginx-gw) no se está ejecutando en el nodo.
  - La interfaz eth0 o VIP del nodo está inactiva.
  - El nodo está inactivo.

En este ejemplo, el nodo de administración principal se ha añadido a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa del grupo de clientes de administración y una interfaz de respaldo del grupo de clientes de FabricPool.



¿Qué ocurre cuando falla la interfaz activa?

La interfaz que aloja actualmente las direcciones VIP es la interfaz activa. Si el grupo ha incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se mueven a la primera interfaz de respaldo disponible en el orden de prioridad. Si falla esa interfaz, las direcciones VIP se mueven a la siguiente interfaz de respaldo disponible, etc.

La conmutación por error puede activarse por cualquiera de estas razones:

- El nodo en el que se configura la interfaz se desactiva.
- El nodo en el que se configura la interfaz pierde la conectividad con los demás nodos durante al menos 2 minutos.
- La interfaz activa se desactiva.
- El servicio Load Balancer se detiene.
- El servicio de alta disponibilidad se detiene.

> Es posible que la conmutación al respaldo no se active por errores de red externos al nodo que aloja la interfaz activa. Del mismo modo, los servicios para Grid Manager o el Gestor de inquilinos no activan la conmutación por error.

Por lo general, el proceso de recuperación tras fallos sólo se realiza en unos pocos segundos y es lo suficientemente rápido como para que las aplicaciones cliente tengan un impacto escaso y puedan confiar en los comportamientos normales de reintento para continuar con el funcionamiento.

Cuando se resuelve un fallo y hay una interfaz de mayor prioridad disponible de nuevo, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad disponible.

¿Cómo se utilizan los grupos de alta disponibilidad?

Puede usar grupos de alta disponibilidad para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo de alta disponibilidad puede proporcionar conexiones administrativas de alta disponibilidad al administrador de grid o al administrador de inquilinos.
- Un grupo de alta disponibilidad puede proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift.
- Un grupo de alta disponibilidad que contiene una sola interfaz le permite proporcionar muchas direcciones VIP y establecer explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo proporcionan los mismos servicios. Cuando crea un grupo de alta disponibilidad, añada interfaces desde los tipos de nodos que proporcionan los servicios necesarios.

- **Admin Nodes**: Incluye el servicio Load Balancer y permite el acceso al Grid Manager o al arrendatario Manager.
- * Nodos de Gateway*: Incluye el servicio de Equilibrador de Carga.

Objetivo del grupo de alta disponibilidad	Añada nodos de este tipo al grupo de alta disponibilidad
Acceso a Grid Manager	• Nodo de administración principal (**primario**) • Nodos de administrador no primario **Nota:** el nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.
Acceso solo al administrador de inquilinos	• Nodos de administrador primario o no primario
Acceso al cliente de S3 o Swift: Servicio Load Balancer	• Nodos de administración • Nodos de puerta de enlace
Acceso de clientes S3 para "S3 Select"	• Aparatos SG100 o SG1000 • Nodos de software basados en VMware **Nota**: Se recomiendan los grupos DE HA cuando se usa S3 Select, pero no es necesario.

Limitaciones en el uso de grupos de alta disponibilidad con Grid Manager o Intenant Manager

Si falla un servicio de Grid Manager o de arrendatario Manager, no se activa la conmutación por error del grupo de alta disponibilidad.

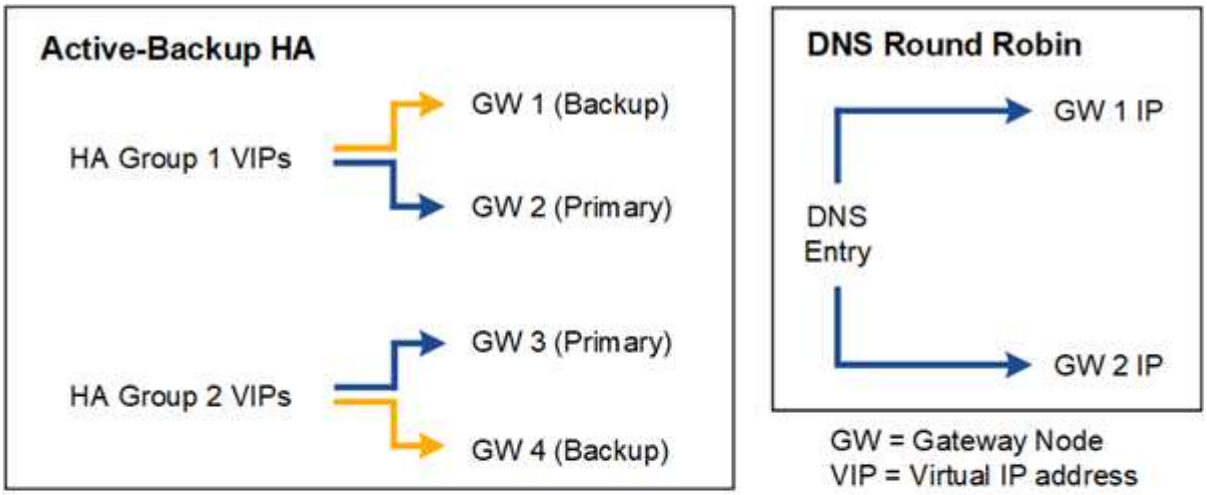
Si ha iniciado sesión en Grid Manager o en el arrendatario Manager cuando se produce la conmutación por error, ha cerrado sesión y debe volver a iniciar sesión para reanudar la tarea.

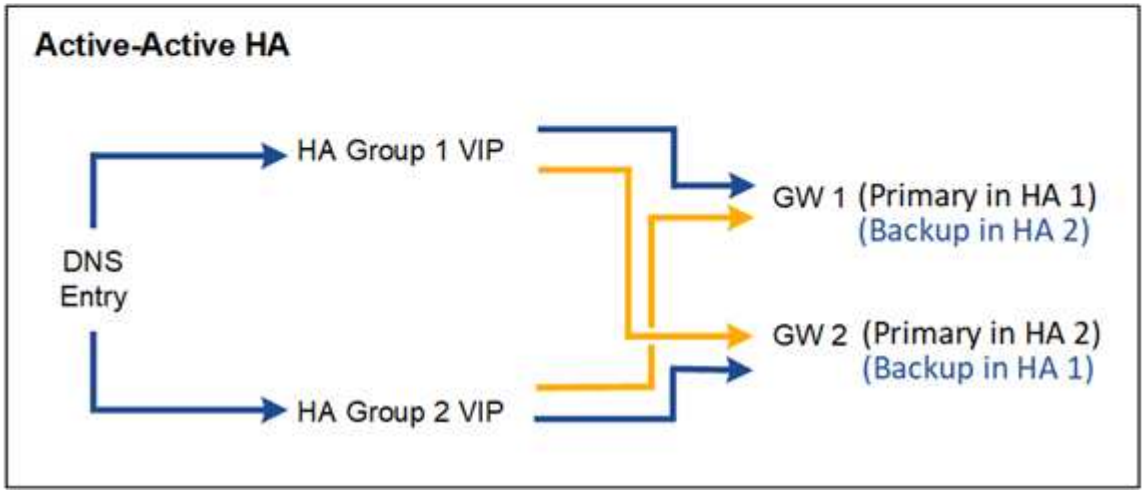
Algunos procedimientos de mantenimiento no se pueden realizar cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puede utilizar Grid Manager para supervisar el sistema StorageGRID.

Opciones de configuración para grupos de alta disponibilidad

Los diagramas siguientes proporcionan ejemplos de diferentes formas de configurar grupos de alta disponibilidad. Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz primaria del grupo de alta disponibilidad y el amarillo indica la interfaz de backup del grupo de alta disponibilidad.





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.
Alta disponibilidad activo-activo	• 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.

Configuración de grupos de alta disponibilidad

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Si piensa utilizar una interfaz VLAN en un grupo de alta disponibilidad, ha creado la interfaz VLAN. Consulte "Configure las interfaces VLAN".
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
  - **Red Hat Enterprise Linux o CentOS (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Linux (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"
  - **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"

Crear un grupo de alta disponibilidad

Cuando crea un grupo de alta disponibilidad, selecciona una o varias interfaces y las organiza por orden de prioridad. A continuación, debe asignar una o varias direcciones VIP al grupo.

Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administrador se incluyan en un grupo de alta disponibilidad. Un grupo de alta disponibilidad solo puede usar una interfaz para cualquier nodo concreto; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de alta disponibilidad.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca los detalles del grupo de alta disponibilidad

Pasos

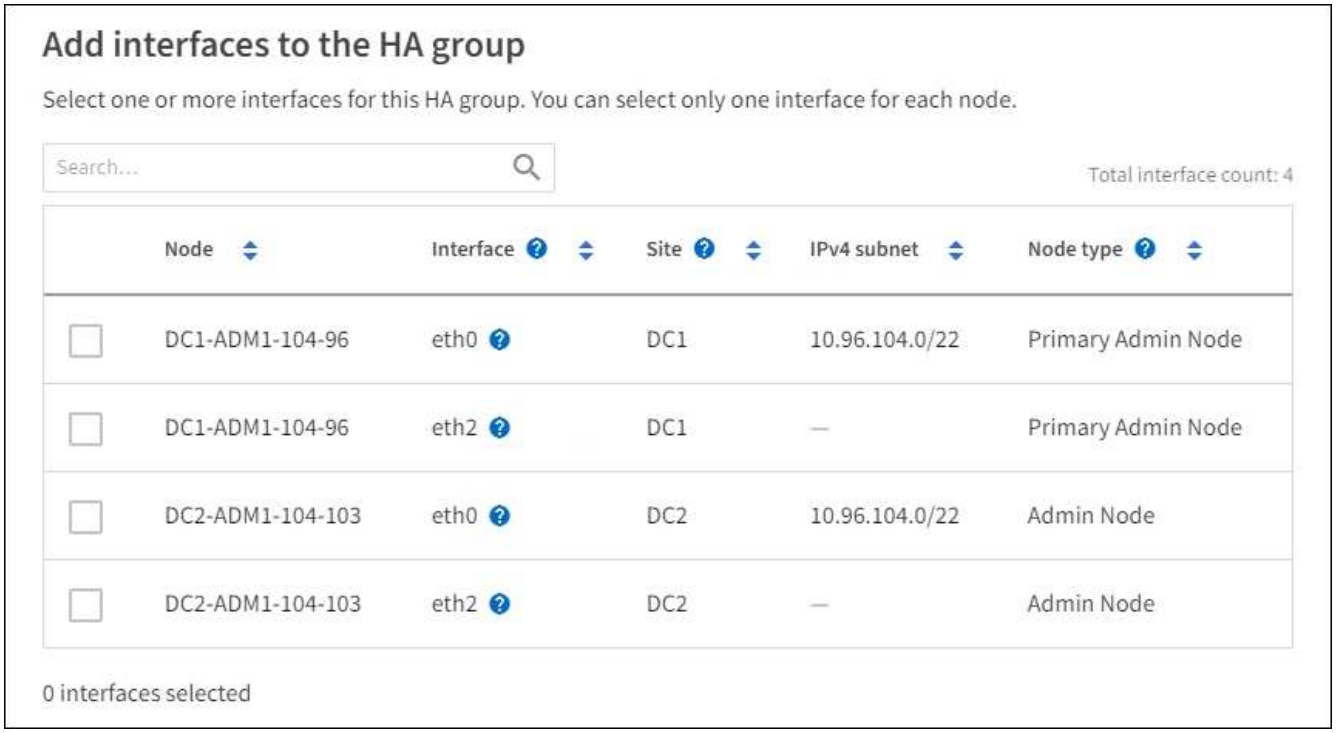
1. Proporcione un nombre único para el grupo de alta disponibilidad.
2. De forma opcional, puede introducir una descripción para el grupo de alta disponibilidad.
3. Seleccione **continuar**.

Añada interfaces al grupo de alta disponibilidad

Pasos

1. Seleccione una o varias interfaces para añadirlas a este grupo de alta disponibilidad.

   Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

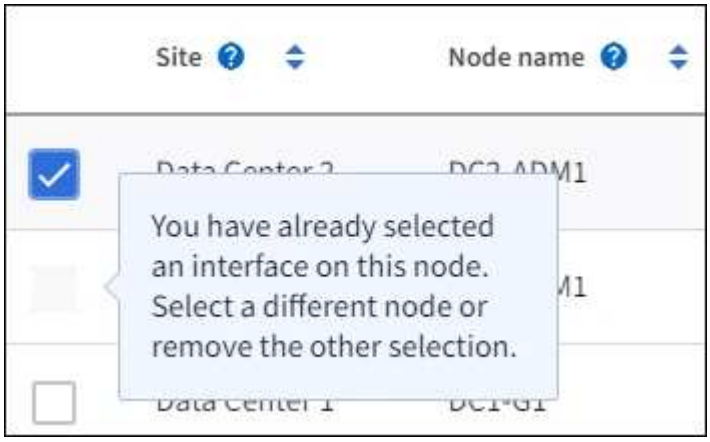


> Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para seleccionar interfaces

- Debe seleccionar al menos una interfaz.
- Solo puede seleccionar una interfaz para un nodo.
- Si el grupo ha es para la protección de alta disponibilidad de los servicios Admin Node, que incluyen Grid Manager y el inquilino Manager, seleccione interfaces sólo en nodos de administrador.

- Si el grupo de alta disponibilidad está para la protección de alta disponibilidad de tráfico de cliente S3 o Swift, seleccione interfaces en nodos de administrador, nodos de puerta de enlace o ambos.
- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación al respaldo, los servicios que proporciona el nodo que antes estaba activo podrían no estar disponibles en el nodo recién activo. Por ejemplo, un nodo de puerta de enlace de backup no puede ofrecer una protección de alta disponibilidad de los servicios de nodo de administración. Del mismo modo, un nodo de administración de copia de seguridad no puede realizar todos los procedimientos de mantenimiento que puede proporcionar el nodo de administración primario.
- Si no puede seleccionar una interfaz, su casilla de verificación está desactivada. La sugerencia de herramienta proporciona más información.



- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **continuar**.

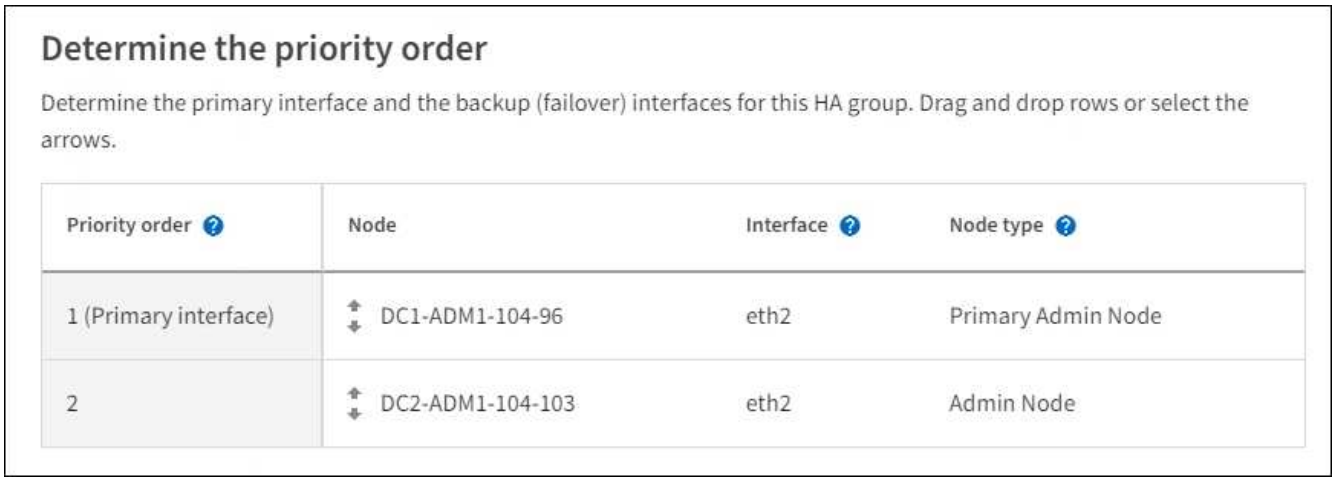
Determinar el orden de prioridad

Si el grupo HA incluye más de una interfaz, puede determinar cuál es la interfaz principal y cuáles son las interfaces de backup (failover). Si la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad que está disponible. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, etc.

Pasos

1. Arrastre filas en la columna **Orden de prioridad** para determinar la interfaz principal y cualquier interfaz de respaldo.

   La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.



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

2. Seleccione **continuar**.

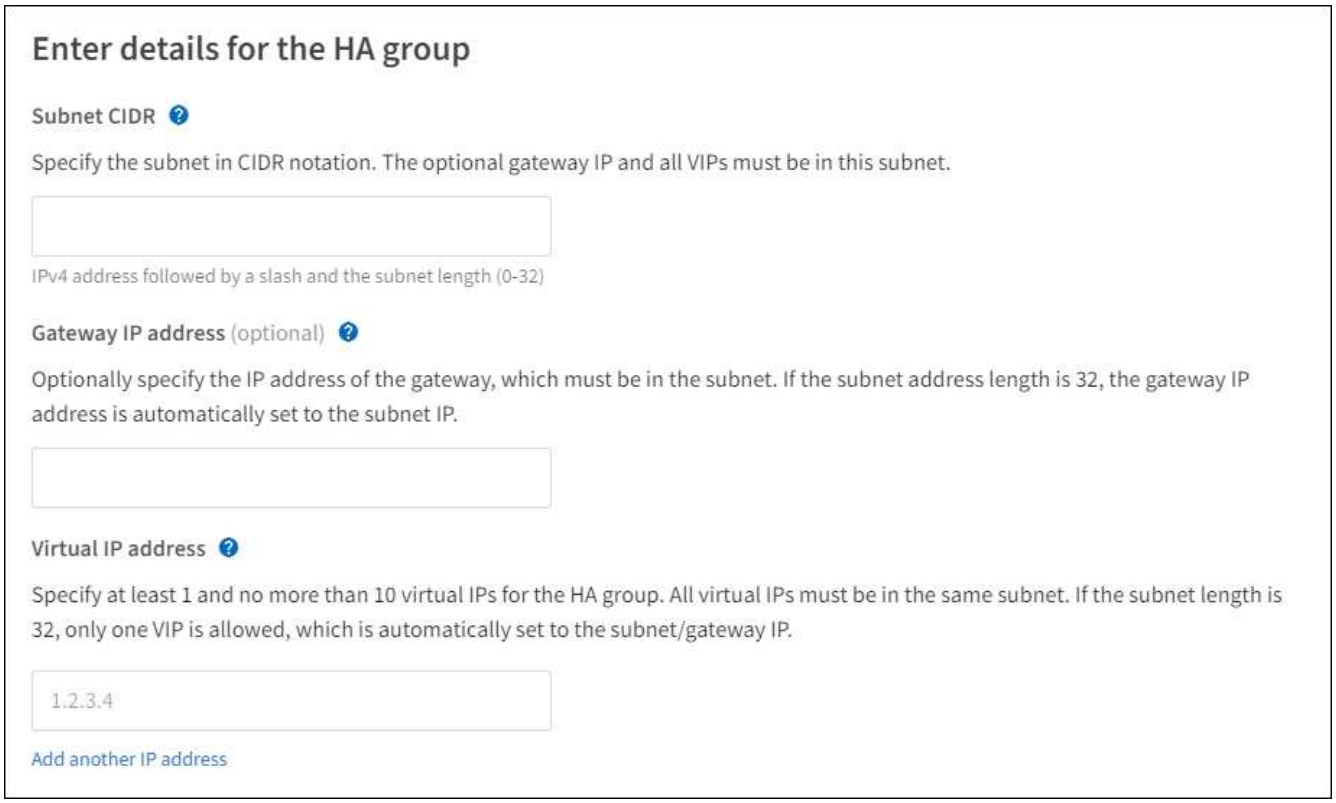
Introduzca las direcciones IP

Pasos

1. En el campo **CIDR de subred**, especifique la subred VIP en notación CIDR --una dirección IPv4 seguida de una barra y la longitud de subred (0-32).

   La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.

   Si utiliza un prefijo de 32 bits, la dirección de red VIP también funciona como dirección de puerta de enlace y dirección VIP.



2. De manera opcional, si alguno de los clientes S3, Swift, administrativos o de arrendatario accederá a estas direcciones VIP desde una subred diferente, introduzca la **dirección IP de la puerta de enlace**. La dirección de la puerta de enlace debe estar en la subred VIP.

   Los usuarios de cliente y administrador utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

3. Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

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

4. Seleccione **Crear grupo ha** y seleccione **Finalizar**.

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

> Espere hasta 15 minutos para que los cambios en un grupo de alta disponibilidad se apliquen a todos los nodos.

Siguientes pasos

Si utilizará este grupo de ha para el equilibrio de carga, cree un extremo de equilibrio de carga para determinar el puerto y el protocolo de red y para conectar los certificados necesarios. Consulte "Configurar puntos finales del equilibrador de carga".

Editar un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que deba editar un grupo de alta disponibilidad si desea quitar el nodo asociado a una interfaz seleccionada en un procedimiento de retirada del sitio o nodo.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.

   La página grupos de alta disponibilidad muestra todos los grupos de alta disponibilidad existentes.

2. Seleccione la casilla de comprobación del grupo de alta disponibilidad que desea editar.
3. Realice una de las siguientes acciones, según lo que desee actualizar:
   - Seleccione **acciones** > **Editar dirección IP virtual** para agregar o eliminar direcciones VIP.
   - Seleccione **acciones** > **Editar grupo ha** para actualizar el nombre o la descripción del grupo, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o quitar direcciones VIP.
4. Si ha seleccionado **Editar dirección IP virtual**:
   a. Actualice las direcciones IP virtuales del grupo de alta disponibilidad.
   b. Seleccione **Guardar**.
   c. Seleccione **Finalizar**.
5. Si ha seleccionado **Editar grupo ha**:
   a. Si lo desea, actualice el nombre o la descripción del grupo.
   b. Opcionalmente, seleccione o desactive las casillas de verificación para agregar o eliminar interfaces.

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

   c. Opcionalmente, arrastre Filas para cambiar el orden de prioridad de la interfaz principal y cualquier interfaz de backup de este grupo de alta disponibilidad.
   d. De manera opcional, actualice las direcciones IP virtuales.
   e. Seleccione **Guardar** y, a continuación, seleccione **Finalizar**.

Espere hasta 15 minutos para que los cambios en un grupo de alta disponibilidad se apliquen a todos los nodos.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o varios grupos de alta disponibilidad al mismo tiempo.

No puede eliminar un grupo de alta disponibilidad si está vinculado a un extremo de equilibrador de carga. Para eliminar un grupo de alta disponibilidad, debe eliminarlo de los extremos de equilibrio de carga que lo utilicen.

Para evitar que se produzcan interrupciones en el cliente, actualice las aplicaciones cliente S3 o Swift

afectadas antes de quitar un grupo de alta disponibilidad. Actualice cada cliente para que se conecte mediante otra dirección IP, por ejemplo, la dirección IP virtual de un grupo ha diferente o la dirección IP configurada para una interfaz durante la instalación.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Revise la columna **Load Balancer Endpoints** para cada grupo HA que desee eliminar. Si se muestra algún punto final del equilibrador de carga:
   a. Vaya a **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
   b. Seleccione la casilla de verificación para el punto final.
   c. Seleccione **acciones** > **Editar modo de enlace de punto final**.
   d. Actualice el modo de enlace para eliminar el grupo HA.
   e. Seleccione **Guardar cambios**.
3. Si no aparece ningún punto final del equilibrador de carga, seleccione la casilla de verificación de cada grupo de alta disponibilidad que desee quitar.
4. Selecciona **Acciones** > **Eliminar grupo HA**.
5. Revise el mensaje y seleccione **Eliminar grupo ha** para confirmar su selección.

   Se eliminan todos los grupos de alta disponibilidad seleccionados. Aparecerá un banner verde de éxito en la página grupos de alta disponibilidad.

Gestione el equilibrio de carga

Consideraciones que tener en cuenta al equilibrio de carga

Es posible utilizar el balanceo de carga para manejar cargas de trabajo de procesamiento y recuperación de clientes S3 y Swift.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo de ingesta y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión mediante la distribución de la carga de trabajo entre varios nodos de almacenamiento.

El servicio de equilibrador de carga de StorageGRID se instala en todos los nodos de administrador y en todos los nodos de puerta de enlace, y ofrece balanceo de carga de capa 7. Realiza la terminación de las solicitudes de cliente de Seguridad de capa de transporte (TLS), inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento.

El servicio Load Balancer de cada nodo funciona de forma independiente cuando se reenvía tráfico de clientes 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.

> Aunque el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, puede que en su lugar desee integrar un equilibrador de carga de terceros. Si quiere más información, póngase en contacto con su representante de cuenta de NetApp o consulte "TR-4626: Equilibradores de carga globales y de terceros de StorageGRID".

¿Cuántos nodos de equilibrio de carga se necesitan?

Como práctica recomendada general, cada sitio del sistema StorageGRID debe incluir dos o más nodos con el servicio de equilibrador de carga. Por ejemplo, un sitio puede incluir dos nodos de puerta de enlace, o bien un nodo de administrador y un nodo de puerta de enlace. Asegúrese de que dispone de una infraestructura adecuada de red, hardware o virtualización para cada nodo de equilibrio de carga, ya sea para dispositivos de servicios SG100 o SG1000, nodos de configuración básica o nodos basados en máquinas virtuales (VM).

¿Qué es un extremo de equilibrador de carga?

Un punto final de equilibrio de carga define el puerto y el protocolo de red (HTTPS o HTTP) que utilizarán las solicitudes de aplicación cliente entrantes y salientes para acceder a los nodos que contienen el servicio de equilibrio de carga. El extremo también define el tipo de cliente (S3 o Swift), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados.

Para crear un punto final de equilibrio de carga, seleccione **CONFIGURACIÓN** > **Red** > **Puntos finales de equilibrio de carga** o complete el asistente de configuración de FabricPool y S3. Para obtener instrucciones:

- "Configurar puntos finales del equilibrador de carga"
- "Use el asistente de configuración de S3"
- "Use el asistente de configuración de FabricPool"

Consideraciones para el puerto

El puerto para un punto final de equilibrio de carga es por defecto 10433 para el primer punto final que cree, pero puede especificar cualquier puerto externo no utilizado entre 1 y 65535. Si utiliza el puerto 80 o 443, el punto final utilizará el servicio Equilibrador de Carga sólo en los nodos de Gateway. Estos puertos están reservados en los nodos de administrador. Si utiliza el mismo puerto para más de un punto final, debe especificar un modo de enlace diferente para cada punto final.

Los puertos utilizados por otros servicios de grid no están permitidos. Consulte "Referencia de puerto de red".

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado de seguridad de la capa de transporte (TLS). Aunque no se recomienda la conexión a StorageGRID sin cifrado TLS, especialmente en entornos de producción. Al seleccionar el protocolo de red para el punto final del equilibrador de carga StorageGRID, debe seleccionar **HTTPS**.

Consideraciones sobre los certificados de punto final del equilibrador de carga

Si selecciona **HTTPS** como protocolo de red para el punto final del equilibrador de carga, debe proporcionar un certificado de seguridad. Puede utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Sube un certificado firmado (recomendado)**. Este certificado puede estar firmado por una entidad de certificación (CA) de confianza pública o una entidad de certificación (CA) privada. El uso de un certificado de servidor de CA de confianza pública para proteger la conexión es la práctica recomendada. A diferencia de los certificados generados, los certificados firmados por una CA pueden rotarse de forma no disruptiva, lo que puede ayudar a evitar problemas de caducidad.

  Debe obtener los siguientes archivos antes de crear el punto final del equilibrador de carga:

  - El archivo de certificado del servidor personalizado.

    - El archivo de claves privadas del certificado de servidor personalizado.
    - De manera opcional, un paquete de CA de los certificados de cada entidad emisora intermedia.
- **Generar un certificado autofirmado**.
- **Utilice el certificado global StorageGRID S3 y Swift**. Debe cargar o generar una versión personalizada de este certificado antes de poder seleccionarlo para el punto final del equilibrador de carga. Consulte "Configure los certificados API S3 y Swift".

¿Qué valores necesito?

Para crear el certificado, debe conocer todos los nombres de dominio y las direcciones IP que utilizarán las aplicaciones cliente S3 o Swift para acceder al extremo.

La entrada **Subject DN** (Nombre Distinguido) para el certificado debe incluir el nombre de dominio completo que la aplicación cliente utilizará para StorageGRID. Por ejemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede utilizar comodines para representar los nombres de dominio totalmente cualificados de todos los nodos de administración y nodos de gateway que ejecutan el servicio de equilibrio de carga. Por ejemplo: `*.storagegrid.example.com` utiliza el comodín * que se va a representar `adm1.storagegrid.example.com` y.. `gn1.storagegrid.example.com`.

Si planea utilizar S3 solicitudes virtuales de estilo hospedado, el certificado también debe incluir una entrada **Nombre Alternativo** para cada una "Nombre de dominio de punto final S3" ha configurado, incluidos los nombres comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Si utiliza caracteres comodín para los nombres de dominio, revise la "Directrices de refuerzo para certificados de servidor".

También debe definir una entrada DNS para cada nombre en el certificado de seguridad.

¿Cómo se gestionan los certificados que caducan?

Si el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID caduca, la aplicación podría perder temporalmente el acceso a StorageGRID.

Para evitar problemas de caducidad de certificados, siga las siguientes prácticas recomendadas:

- Monitoree cuidadosamente cualquier alerta que advierta de fechas de vencimiento de certificados que se acercan, como el **Caducidad del certificado de punto final del equilibrador de carga** y **Caducidad del certificado de servidor global para las alertas S3 y Swift API**.
- Mantenga siempre sincronizadas las versiones del certificado de la aplicación StorageGRID y S3. Si reemplaza o renueva el certificado utilizado para un punto final de equilibrio de carga, debe reemplazar o renovar el certificado equivalente utilizado por la aplicación S3.

- Utilice un certificado de CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede sustituir certificados próximos a caducar de forma no disruptiva.
- Si generó un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe reemplazar manualmente el certificado tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado existente.

Consideraciones sobre el modo de enlace

El modo de enlace le permite controlar qué direcciones IP se pueden utilizar para acceder a un punto final de equilibrio de carga. Si un punto final utiliza un modo de enlace, las aplicaciones cliente solo pueden acceder al punto final si utilizan una dirección IP permitida o su nombre de dominio completo (FQDN) correspondiente. Las aplicaciones cliente que utilizan cualquier otra dirección IP o FQDN no pueden acceder al punto final.

Puede especificar cualquiera de los siguientes modos de enlace:

- **Global** (por defecto): Las aplicaciones cliente pueden acceder al punto final utilizando la dirección IP de cualquier Nodo de Gateway o Nodo de Administración, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o un FQDN correspondiente. Utilice esta configuración a menos que necesite restringir la accesibilidad de un punto final.
- **IPs virtuales de grupos HA**. Las aplicaciones cliente deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace.

Consideraciones para el acceso de inquilinos

El acceso de inquilino es una función de seguridad opcional que le permite controlar qué cuentas de inquilino de StorageGRID pueden usar un extremo de equilibrador de carga para acceder a sus buckets. Puede permitir que todos los inquilinos accedan a un punto final (valor predeterminado) o puede especificar una lista de los inquilinos permitidos o bloqueados para cada punto final.

Puede utilizar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus extremos. Por ejemplo, puede utilizar esta función para asegurarse de que los materiales de alto secreto o altamente clasificados propiedad de un arrendatario permanezcan completamente inaccesibles para otros arrendatarios.

> Para fines de control de acceso, el inquilino se determina a partir de las claves de acceso utilizadas en la solicitud del cliente, si no se proporcionan claves de acceso como parte de la solicitud (como con acceso anónimo), el propietario del depósito se utiliza para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para entender cómo funciona esta característica de seguridad, considere el siguiente ejemplo:

1. Ha creado dos puntos finales de equilibrio de carga, de la siguiente manera:
   - **Punto final público**: Utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
   - **Top SECRET** punto final: Utiliza el puerto 10444 y permite el acceso al inquilino **Top SECRET**

solamente. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.

2. La `top-secret.pdf` Está en un cubo propiedad del inquilino **Top secret**.

Para acceder al `top-secret.pdf`, Un usuario en el inquilino **Top secret** puede emitir una solicitud GET a. `https://w.x.y.z:10444/top-secret.pdf`. Como este inquilino puede usar el extremo 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario que pertenece a cualquier otro arrendatario emite la misma solicitud a la misma URL, recibe un mensaje de acceso denegado inmediato. Se deniega el acceso aunque las credenciales y la firma sean válidas.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente cuando se reenvía tráfico de S3 o Swift a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio Load Balancer envía más solicitudes a los nodos de almacenamiento con una mayor disponibilidad de CPU. La información de carga de CPU del nodo se actualiza cada pocos minutos, pero es posible que la ponderación se actualice con mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa de un uso del 100 % o no informa de su uso.

En algunos casos, la información acerca de la disponibilidad de CPU se limita al sitio donde se encuentra el servicio Load Balancer.

Configurar puntos finales del equilibrador de carga

Los extremos de equilibrador de carga determinan los puertos y los protocolos de red que los clientes S3 y Swift pueden utilizar al conectarse al equilibrador de carga StorageGRID en los nodos de puerta de enlace y administración.

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Ha revisado el "consideraciones que tener en cuenta al equilibrio de carga".
- Si anteriormente ha reasignado un puerto que tiene intención de utilizar para el extremo de equilibrio de carga, tiene "se ha eliminado el mapa de puertos".
- Ha creado cualquier grupo de alta disponibilidad que desee utilizar. Se recomiendan los grupos de ALTA DISPONIBILIDAD, pero no es obligatorio. Consulte "Gestión de grupos de alta disponibilidad".
- Si el punto final del equilibrador de carga será utilizado por "Inquilinos de S3 para S3 Select", No debe utilizar las direcciones IP ni las FQDN de ningún nodo de configuración básica. Sólo se permiten los dispositivos SG100 o SG1000 y los nodos de software basados en VMware para los extremos de equilibrador de carga utilizados para S3 Select.
- Ha configurado las interfaces VLAN que desea utilizar. Consulte "Configure las interfaces VLAN".
- Si crea un extremo de HTTPS (recomendado), tiene la información del certificado de servidor.

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

- Para cargar un certificado, necesita el certificado de servidor, la clave privada de certificado y, opcionalmente, un bundle de CA.
- Para generar un certificado, se necesitan todos los nombres de dominio y las direcciones IP que utilizarán los clientes S3 o Swift para acceder al extremo. También debe conocer el asunto (nombre distintivo).
- Si desea usar el certificado API de StorageGRID S3 y Swift (que también se puede usar para conexiones directamente a nodos de almacenamiento), ya sustituyó el certificado predeterminado por un certificado personalizado firmado por una autoridad de certificado externa. Consulte"Configure los certificados API S3 y Swift".

Cree un extremo de equilibrador de carga

Cada extremo de equilibrio de carga especifica un puerto, un tipo de cliente (S3 o Swift) y un protocolo de red (HTTP o HTTPS).

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Seleccione **Crear**.

Introduzca los detalles de los extremos

Pasos

1. Introduzca los detalles del extremo.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado entre 1 y 65535. Si introduce **80** o **443**, el punto final sólo se configura en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administrador.
Tipo de cliente	Tipo de aplicación cliente que utilizará este extremo, ya sea **S3** o **Swift**.
Protocolo de red	El protocolo de red que utilizarán los clientes al conectarse a este extremo. • Seleccione **HTTPS** para una comunicación segura cifrada con TLS (recomendado). Debe asociar un certificado de seguridad para poder guardar el extremo. • Seleccione **HTTP** para una comunicación no cifrada y menos segura. Utilice HTTP sólo para una cuadrícula que no sea de producción.

2. Seleccione **continuar**.

Seleccione un modo de enlace

Pasos

1. Seleccione un modo de enlace para el punto final para controlar cómo se accede al punto final—Utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Opción	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

> Si más de un punto final utiliza el mismo puerto, StorageGRID utiliza este orden de prioridad para decidir qué punto final utilizar: **IP virtuales de grupos HA** > **Interfaces de nodo** > **Tipo de nodo** > **Global**.

2. Si ha seleccionado **IP virtuales de grupos ha**, seleccione uno o más grupos ha.
3. Si ha seleccionado **interfaces de nodo**, seleccione una o más interfaces de nodo para cada nodo de administración o nodo de puerta de enlace que desee asociar con este extremo.
4. Si seleccionó **Tipo de nodo**, seleccione Nodos de administración, que incluye tanto el nodo de administración principal como cualquier nodo de administración no principal, o Nodos de puerta de enlace.

Controle el acceso de inquilinos

Pasos

1. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de arrendatario. Después de agregar cuentas de arrendatario, puede editar el punto final del equilibrador de carga para permitir o bloquear cuentas específicas.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

2. Si está creando un punto final **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el nuevo punto final del equilibrador de carga. A continuación, vaya a. Después de terminar. De lo contrario, seleccione **continuar** para adjuntar el certificado.

Adjunte el certificado

Pasos

1. Si está creando un extremo **HTTPS**, seleccione el tipo de certificado de seguridad que desea asociar al extremo.

   El certificado protege las conexiones entre los clientes S3 y Swift y el servicio Load Balancer en los nodos de Admin Node o de Gateway.

   - **Cargar certificado**. Seleccione esta opción si tiene certificados personalizados para cargar.
   - **Generar certificado**. Seleccione esta opción si tiene los valores necesarios para generar un certificado personalizado.
   - **Utilice los certificados StorageGRID S3 y Swift**. Seleccione esta opción si desea usar el certificado API global S3 y Swift, que también se puede usar para las conexiones directamente con nodos de almacenamiento.

     No puede seleccionar esta opción a menos que haya sustituido el certificado de API S3 y Swift predeterminado, firmado por la CA de grid, por un certificado personalizado firmado por una entidad de certificación externa. Consulte"Configure los certificados API S3 y Swift".

2. Si no está usando los certificados StorageGRID S3 y Swift, cargue o genere el certificado.

Cargue el certificado

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor**: El archivo de certificado de servidor personalizado en codificación PEM.
- **Clave privada de certificado**: Archivo de clave privada de certificado de servidor personalizado (`.key`).

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

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

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

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

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

  Por ejemplo: `storagegrid_certificate.pem`

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

d. Seleccione **Crear**. + se crea el punto final del equilibrador de carga. El certificado personalizado se usa en todas las conexiones nuevas posteriores entre los clientes de S3 y Swift y el extremo.

Generar certificado

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).

Campo	Descripción
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

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

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

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

     Por ejemplo: `storagegrid_certificate.pem`

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

e. Seleccione **Crear**.

   Se crea el punto final del equilibrador de carga. El certificado personalizado se usa para todas las conexiones nuevas posteriores entre los clientes de S3 y Swift y este extremo.

Después de terminar

Pasos

1. Si utiliza un DNS, asegúrese de que el DNS incluya un registro para asociar el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que utilizarán los clientes para realizar conexiones.

   La dirección IP que introduzca en el registro DNS depende de si se utiliza un grupo de alta disponibilidad de nodos con balanceo de carga:

   - Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de dicho grupo de alta disponibilidad.
   - Si no está utilizando un grupo HA, los clientes se conectarán al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de un nodo de puerta de enlace o nodo de administración.

     También debe asegurarse de que el registro DNS hace referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.

2. Proporcione a los clientes S3 y Swift la información necesaria para conectarse al extremo:

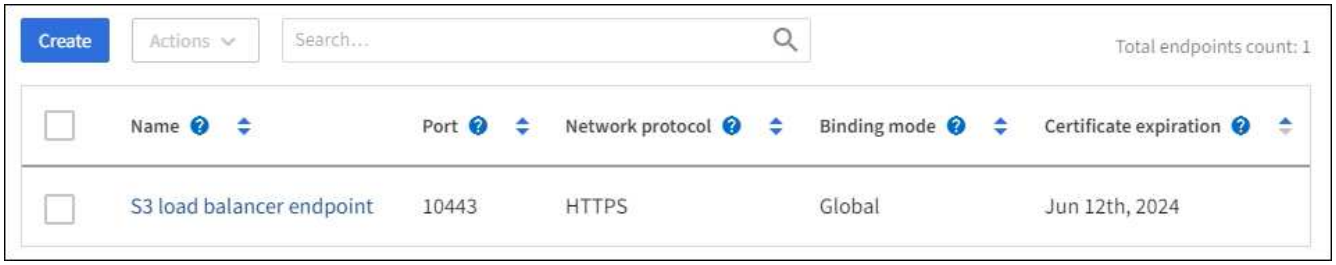
- Número de puerto
- Nombre de dominio o dirección IP completos
- Los detalles de certificado necesarios

Ver y editar puntos finales del equilibrador de carga

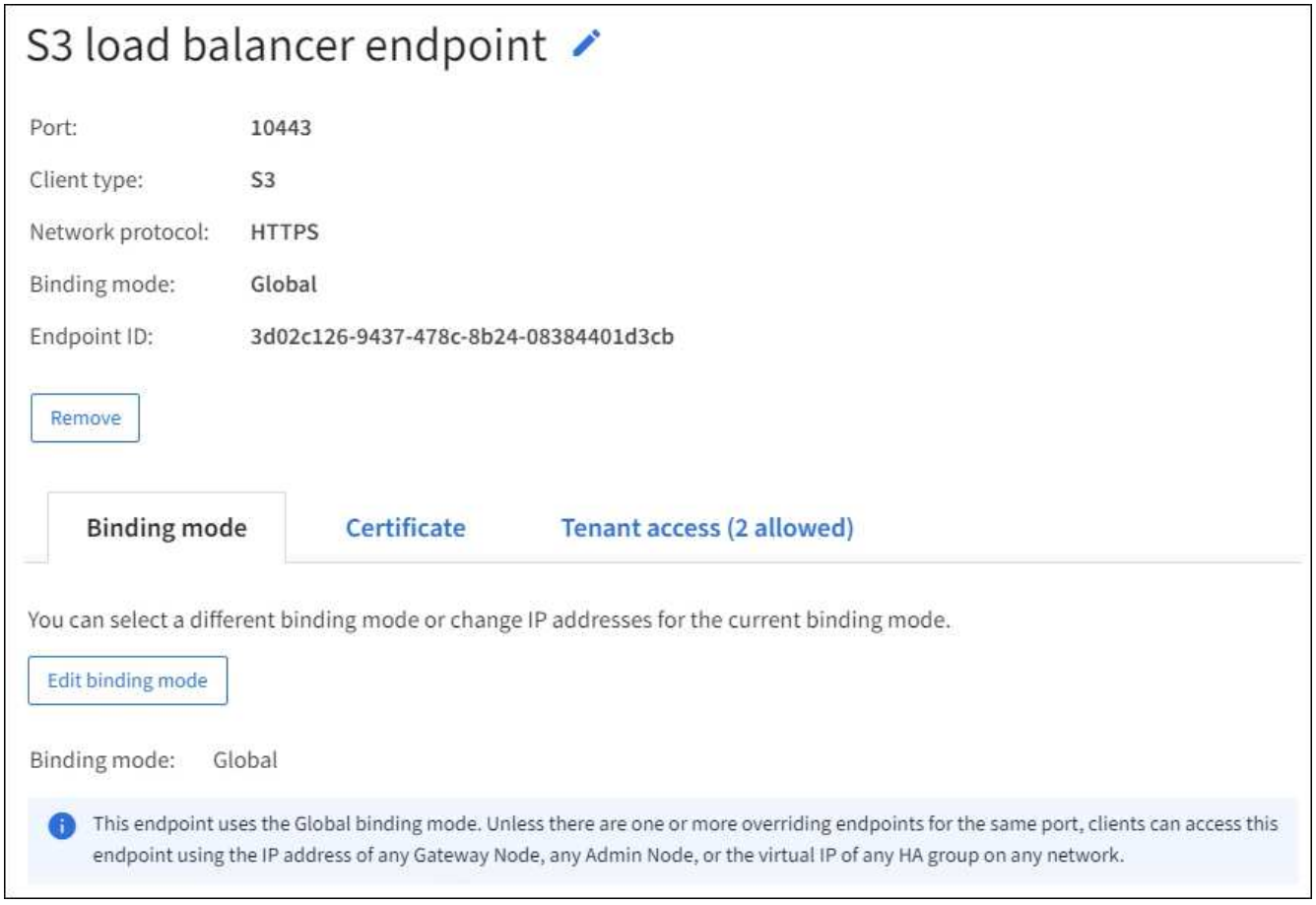
Puede ver detalles de los extremos de equilibrador de carga existentes, incluidos los metadatos de certificado para un extremo protegido. También puede cambiar el nombre de un extremo o el modo de enlace y actualizar los certificados asociados.

No puede cambiar el tipo de servicio (S3 o Swift), el puerto ni el protocolo (HTTP o HTTPS).

- Para ver información básica de todos los puntos finales del equilibrador de carga, revise la tabla de la página puntos finales del equilibrador de carga.



- Para ver todos los detalles acerca de un extremo específico, incluidos los metadatos del certificado, seleccione el nombre del extremo en la tabla.



- Para editar un punto final, utilice el menú **acciones** de la página puntos finales del equilibrador de carga o la página de detalles de un punto final específico.

> Después de editar un extremo, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú Actions	Detalles
Editar el nombre del extremo	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar nombre de punto final**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar**.
Edite el modo de enlace de punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar modo de enlace de punto final**. c. Actualice el modo de enlace según sea necesario. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione **Editar modo de enlace**. c. Actualice el modo de enlace según sea necesario. d. Seleccione **Guardar cambios**.
Editar certificado de extremo	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar certificado de punto final**. c. Cargue o genere un nuevo certificado personalizado o comience a usar el certificado global S3 y Swift, según sea necesario. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione la ficha **Certificado**. c. Seleccione **Editar certificado**. d. Cargue o genere un nuevo certificado personalizado o comience a usar el certificado global S3 y Swift, según sea necesario. e. Seleccione **Guardar cambios**.
Editar el acceso de inquilinos	a. Seleccione la casilla de verificación para el punto final. b. Selecciona **Acciones** > **Editar acceso de inquilino**. c. Elija una opción de acceso diferente, seleccione o elimine arrendatarios de la lista, o realice ambas acciones. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione la pestaña **Acceso de inquilino**. c. Selecciona **Editar acceso de inquilino**. d. Elija una opción de acceso diferente, seleccione o elimine arrendatarios de la lista, o realice ambas acciones. e. Seleccione **Guardar cambios**.

Retire los extremos del equilibrador de carga

Puede eliminar uno o varios puntos finales mediante el menú **acciones** o puede eliminar un único punto final de la página de detalles.

> Para evitar que se produzcan interrupciones en el cliente, actualice las aplicaciones cliente S3 o Swift afectadas antes de eliminar un extremo de equilibrio de carga. Actualice cada cliente para que se conecte utilizando un puerto asignado a otro extremo de equilibrador de carga. Asegúrese de actualizar también la información de certificado necesaria.

- Para eliminar uno o varios puntos finales:
  a. En la página Equilibrador de Carga, seleccione la casilla de verificación de cada punto final que desee eliminar.
  b. Seleccione **acciones** > **Quitar**.
  c. Seleccione **OK**.
- Para eliminar un extremo de la página de detalles:
  a. Desde la página Load equilibrador. seleccione el nombre del extremo.
  b. Seleccione **Quitar** en la página de detalles.
  c. Seleccione **OK**.

Configure los nombres de dominio de punto final S3

Para admitir S3 solicitudes de estilo hospedado virtual, debe utilizar Grid Manager para configurar la lista de S3 nombres de dominio de punto final a los que se conectan los clientes S3.

> El uso de una dirección IP para un nombre de dominio de punto final no es compatible. Las próximas versiones impedirán esta configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha confirmado que no hay una actualización de grid en curso.

> No realice ningún cambio en la configuración del nombre de dominio cuando haya una actualización de cuadrícula en curso.

Acerca de esta tarea

Para habilitar a los clientes que usen nombres de dominio extremo de S3, debe realizar todas las siguientes acciones:

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el "Certificado que el cliente utiliza para las conexiones HTTPS a StorageGRID" está firmado para todos los nombres de dominio que el cliente requiere.

  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 los clientes utilizan para realizar conexiones y asegúrese de que los registros hacen referencia a todos los nombres de dominio de punto final S3 necesarios, incluidos los nombres comodín.

> Los clientes se pueden conectar a StorageGRID mediante la dirección IP de un nodo de puerta de enlace, un nodo de administrador o un nodo de almacenamiento, o bien mediante la conexión a la dirección IP virtual de un grupo de alta disponibilidad. Debe comprender cómo se conectan las aplicaciones cliente a la cuadrícula para que incluya las direcciones IP correctas en los registros DNS.

Los clientes que usan conexiones HTTPS (recomendadas) a la cuadrícula pueden usar cualquiera de los siguientes certificados:

- Los clientes que se conectan a un extremo de equilibrador de carga pueden utilizar un certificado personalizado para ese extremo. Cada punto final de equilibrio de carga se puede configurar para reconocer diferentes nombres de dominio de punto final S3.
- Los clientes que se conectan a un extremo de balanceador de carga o directamente a un nodo de almacenamiento pueden personalizar el certificado de API global S3 y Swift para que incluya todos los nombres de dominio de extremo S3 requeridos.

> Si no agrega nombres de dominio de punto final S3 y la lista está vacía, se deshabilitará el soporte para S3 solicitudes de estilo hospedado virtual.

Agregue un nombre de dominio de punto final S3

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **S3 nombres de dominio de punto final**.
2. Introduzca el nombre de dominio en el campo **Nombre de dominio 1**. Seleccione **Agregar otro nombre de dominio** para agregar más nombres de dominio.
3. Seleccione **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de punto final S3 necesarios.
   - Si los clientes se conectan a un punto final del equilibrador de carga que utiliza su propio certificado, "actualice el certificado asociado al punto final".
   - Si los clientes se conectan a un extremo de balanceador de carga que utiliza el certificado de API S3 y Swift global o directamente a los nodos de almacenamiento, "Actualice el certificado de API global S3 y Swift".
5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombres de dominio de extremo.

Resultado

Ahora, cuando los clientes utilizan el extremo *`bucket.s3.company.com`*, El servidor DNS resuelve el punto final correcto y el certificado autentica el punto final como se esperaba.

Cambie el nombre de un nombre de dominio de punto final S3

Si cambia un nombre utilizado por las aplicaciones S3, las solicitudes de estilo hospedado virtual fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **S3 nombres de dominio de punto final**.
2. Seleccione el campo de nombre de dominio que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.
4. Selecciona **Sí** para confirmar tu cambio.

Suprimir un nombre de dominio de punto final S3

Si elimina un nombre utilizado por las aplicaciones S3, las solicitudes de estilo hospedado virtual fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **S3 nombres de dominio de punto final**.
2. Seleccione el icono de eliminar ✕ junto al nombre de dominio.
3. Seleccione **Sí** para confirmar la eliminación.

Información relacionada

- "USE LA API DE REST DE S3"
- "Ver direcciones IP"
- "Configuración de grupos de alta disponibilidad"

Resumen: Direcciones IP y puertos para conexiones cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 y Swift se conectan al servicio de equilibrio de carga, que se incluye en todos los nodos de administración y de puerta de enlace, o al servicio de enrutador de distribución local (LDR), que se incluye en todos los nodos de almacenamiento.

Las aplicaciones cliente se pueden conectar a StorageGRID mediante la dirección IP de un nodo de cuadrícula y el número de puerto del servicio en ese nodo. Opcionalmente, puede crear grupos de alta disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones altamente disponibles que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID con un nombre de dominio completo (FQDN) en lugar de una dirección IP o VIP, puede configurar entradas de DNS.

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. Si ya ha creado extremos del balanceador de carga y grupos de alta disponibilidad (HA), consulte Dónde encontrar direcciones IP Para localizar estos valores en Grid Manager.

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 asignado al punto final del equilibrador de carga
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	Puerto asignado al 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	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	Puerto asignado al punto final del equilibrador de carga
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

URL de ejemplo

Para conectar una aplicación cliente al punto final del equilibrador de carga de un grupo 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 HA es 192.0.2.5 y el número de puerto del extremo del equilibrador de carga es 10443, una aplicación podría utilizar la siguiente URL para conectarse a StorageGRID:

`https://192.0.2.5:10443`

Dónde encontrar direcciones IP

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Para encontrar la dirección IP de un nodo de grid:
   a. Seleccione **NODES**.
   b. Seleccione el nodo de administrador, Gateway Node o Storage Node al que desea conectarse.
   c. Seleccione la ficha **Descripción general**.
   d. En la sección Node Information, tenga en cuenta las direcciones IP del nodo.
   e. Seleccione **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaz.

      Puede establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

      - **Eth0:** Red Grid
      - **Eth1:** Red de administración (opcional)
      - **Eth2:** Red cliente (opcional)

Si va a ver un nodo de administrador o un nodo de puerta de enlace y es el nodo activo de un grupo de alta disponibilidad, en eth2 se muestra la dirección IP virtual del grupo de alta disponibilidad.

3. Para buscar la dirección IP virtual de un grupo de alta disponibilidad:
   a. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
   b. En la tabla, tenga en cuenta la dirección IP virtual del grupo ha.
4. Para buscar el número de puerto de un extremo Load Balancer:
   a. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
   b. Tenga en cuenta el número de puerto del punto final que desea utilizar.

   Si el número de puerto es 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que esos puertos están reservados en los nodos Admin. Todos los demás puertos están configurados tanto en los nodos de puerta de enlace como en los de administración.

   c. Seleccione el nombre del punto final de la tabla.
   d. Confirme que el **Client type** (S3 o Swift) coincide con la aplicación cliente que utilizará el punto final.

Administrar redes y conexiones

Configurar ajustes de red: Información general

Puede configurar varios ajustes de red desde el Gestor de cuadrícula para ajustar el funcionamiento del sistema StorageGRID.

Configure las interfaces VLAN

Puede hacerlo "Cree interfaces de LAN virtual (VLAN)" para aislar y crear particiones del tráfico con el fin de mejorar la seguridad, la flexibilidad y el rendimiento. Cada interfaz de VLAN está asociada con una o varias interfaces principales en los nodos de administración y de puerta de enlace. Puede utilizar interfaces VLAN en grupos de alta disponibilidad y en extremos de equilibrador de carga para segregar el tráfico cliente o administrador por aplicación o inquilino.

Directivas de clasificación de tráfico

Puede utilizar "políticas de clasificación de tráfico" para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con buckets específicos, inquilinos, subredes de cliente o extremos de equilibrador de carga. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Directrices para redes StorageGRID

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

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

Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Para obtener más información acerca de la topología de red, consulte "Directrices sobre redes".

Red Grid

Obligatorio. La red de red se utiliza para todo el tráfico interno de StorageGRID. Proporciona conectividad entre todos los nodos de la cuadrícula, en todos los sitios y subredes.

Red de administración

Opcional. La red de administración suele utilizarse para la administración y el mantenimiento del sistema. También se puede utilizar para el acceso a protocolos de cliente. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios.

Red cliente

Opcional. La red cliente es una red abierta que se suele utilizar para proporcionar acceso a aplicaciones cliente S3 y Swift, de modo que la red Grid se pueda aislar y proteger. La red de cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

Directrices

- Cada nodo de grid StorageGRID requiere una interfaz de red dedicada, una dirección IP, una máscara de subred y una puerta de enlace para cada red a la que está asignado.
- Un nodo de grid no puede tener más de una interfaz en una red.
- Se admite una sola puerta de enlace, por red y cada nodo de grid, y debe estar en la misma subred que el nodo. Si es necesario, puede implementar un enrutamiento más complejo en la puerta de enlace.
- En cada nodo, cada red asigna una interfaz de red específica.

Red	Nombre de la interfaz
Cuadrícula	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Si el nodo está conectado a un dispositivo StorageGRID, se utilizan puertos específicos para cada red. Para obtener más información, consulte las instrucciones de instalación del dispositivo.
- La ruta predeterminada se genera automáticamente, por nodo. Si eth2 está habilitado, 0.0.0.0/0 utiliza la red cliente en eth2. Si eth2 no está habilitado, 0.0.0.0/0 utiliza la red de cuadrícula en eth0.
- La red cliente no se pone en funcionamiento hasta que el nodo de grid se ha Unido a la cuadrícula
- La red de administrador se puede configurar durante la puesta en marcha del nodo de grid para permitir el acceso a la interfaz de usuario de la instalación antes de que la cuadrícula esté totalmente instalada.

Interfaces opcionales

Opcionalmente, se pueden añadir interfaces adicionales a un nodo. Por ejemplo, puede agregar una interfaz troncal a un nodo de administración o de puerta de enlace, para poder utilizar "Interfaces VLAN" para segregar el tráfico que pertenece a diferentes aplicaciones o arrendatarios. O bien, puede que desee añadir una interfaz de acceso para utilizarla en un "Grupo de alta disponibilidad".

Para añadir enlaces troncales o interfaces de acceso, consulte lo siguiente:

- **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"
  - **RHEL o CentOS (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **RHEL, CentOS, Ubuntu o Debian (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"

Ver direcciones IP

Puede ver la dirección IP de cada nodo de grid en el sistema StorageGRID. Luego, puede usar esta dirección IP para iniciar sesión en el nodo de la cuadrícula en la línea de comandos y realizar diversos procedimientos de mantenimiento.

Antes de empezar

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

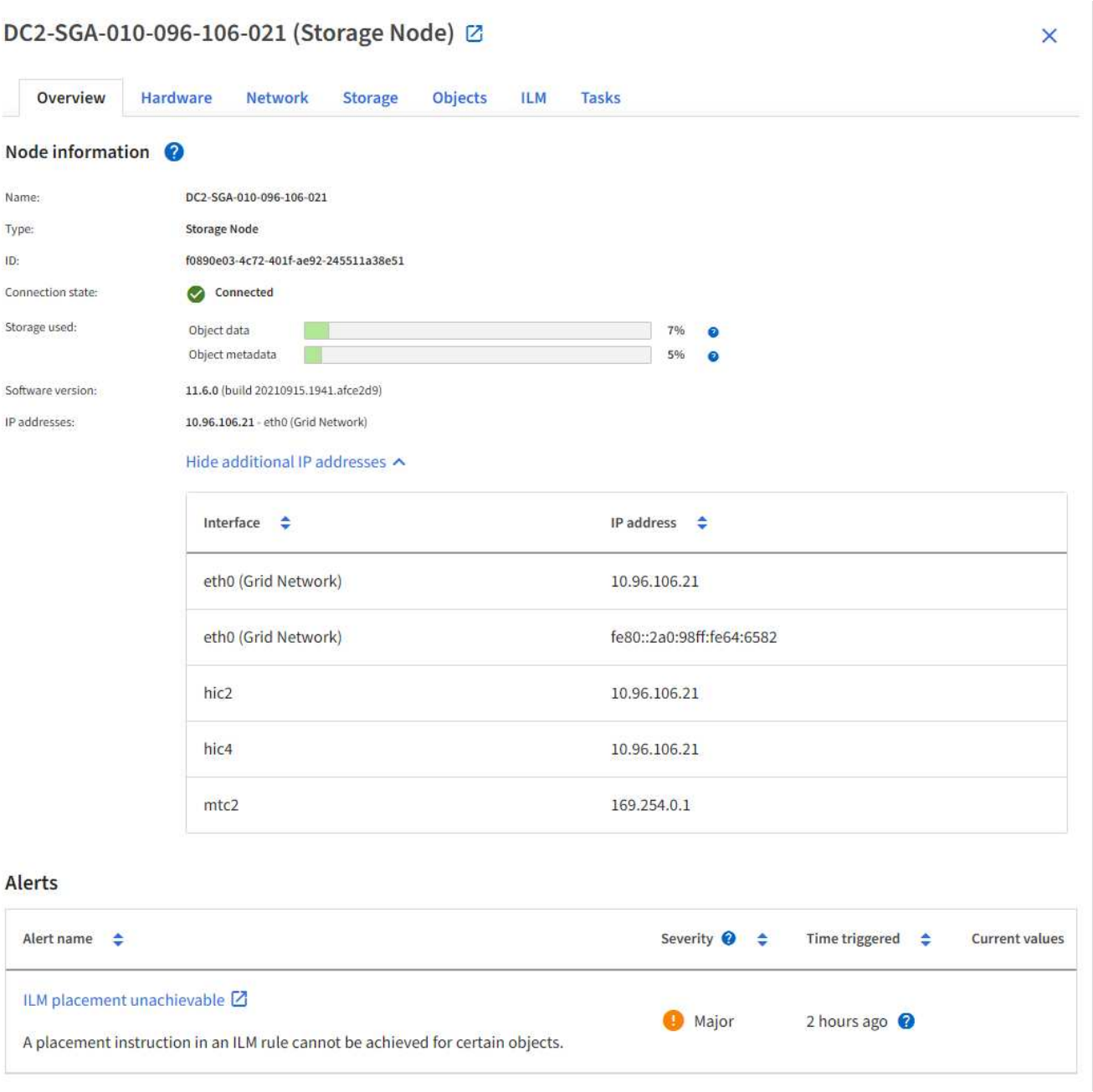
Acerca de esta tarea

Para obtener más información sobre cómo cambiar direcciones IP, consulte "Configurar las direcciones IP".

Pasos

1. Seleccione **NODES** > ***grid node*** > **Descripción general**.
2. Seleccione **Mostrar más** a la derecha del título direcciones IP.

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



Cifrados compatibles para conexiones TLS salientes

El sistema StorageGRID es compatible con un conjunto limitado de conjuntos de cifrado para conexiones TLS (seguridad de la capa de transporte) con los sistemas externos utilizados para la federación de identidades y los pools de almacenamiento en cloud.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3 para conexiones a sistemas externos que se utilizan para la federación de identidades y los pools de almacenamiento en cloud.

Se han seleccionado los cifrados TLS compatibles con sistemas externos para garantizar la compatibilidad con una gama de sistemas externos. La lista supera la lista de cifrados que se admiten con aplicaciones cliente S3 o Swift. Para configurar los cifrados, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** y seleccione **Políticas TLS y SSH**.

Las opciones de configuración de TLS, como las versiones de protocolos, 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.

Configure las interfaces VLAN

Puede crear interfaces de LAN virtual (VLAN) en nodos de administrador y de puerta de enlace, y usarlas en grupos de alta disponibilidad y extremos de equilibrador de carga para aislar y dividir el tráfico para garantizar la seguridad, la flexibilidad y el rendimiento.

Consideraciones sobre las interfaces VLAN

- Para crear una interfaz de VLAN, introduzca un ID de VLAN y elija una interfaz principal en uno o varios nodos.
- Se debe configurar una interfaz padre como interfaz troncal en el conmutador.
- Una interfaz principal puede ser Grid Network (eth0), Client Network (eth2) o una interfaz troncal adicional para la máquina virtual o el host con configuración básica (por ejemplo, ens256).
- Para cada interfaz de VLAN, solo puede seleccionar una interfaz principal para un nodo determinado. Por ejemplo, no puede utilizar la interfaz de red de grid y la interfaz de red de cliente en el mismo nodo de gateway que la interfaz principal para la misma VLAN.
- Si la interfaz de VLAN es para el tráfico del nodo de administración, que incluye tráfico relacionado con el administrador de grid y el administrador de inquilinos, seleccione interfaces sólo en nodos de administración.
- Si la interfaz de VLAN es para el tráfico de clientes S3 o Swift, seleccione interfaces en nodos de administrador o nodos de puerta de enlace.
- Si necesita agregar interfaces de línea externa, consulte lo siguiente para obtener más información:
  - **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"
  - **RHEL o CentOS (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **RHEL, CentOS, Ubuntu o Debian (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"

Cree una interfaz VLAN

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Se ha configurado una interfaz de línea externa en la red y está conectada al nodo de máquina virtual o Linux. Conoce el nombre de la interfaz troncal.
- Conoce el ID de la VLAN que desea configurar.

Acerca de esta tarea

El administrador de red podría haber configurado una o más interfaces troncales y una o varias VLAN para separar el tráfico de administración o cliente que pertenezca a diferentes aplicaciones o inquilinos. Cada VLAN se identifica por un ID o etiqueta numéricos. Por ejemplo, la red puede utilizar VLAN 100 para el tráfico FabricPool y VLAN 200 para una aplicación de archivado.

Puede utilizar Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando se crean interfaces VLAN, se especifica el identificador de VLAN y se seleccionan las interfaces principales (troncales) en uno o varios nodos.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione **Crear**.

Introduzca los detalles de las interfaces de VLAN

Pasos

1. Especifique el ID de la VLAN en la red. Puede introducir cualquier valor entre 1 y 4094.

   Los ID de VLAN no tienen por qué ser únicos. Por ejemplo, puede utilizar el identificador de VLAN 200 para el tráfico de administración en un sitio y el mismo identificador de VLAN para el tráfico de cliente en otro sitio. Puede crear interfaces VLAN independientes con diferentes conjuntos de interfaces principales en cada sitio. Sin embargo, dos interfaces de VLAN con el mismo ID no pueden compartir la misma interfaz en un nodo. Si especifica un ID que ya se ha utilizado, aparecerá un mensaje.

2. De manera opcional, introduzca una breve descripción para la interfaz de VLAN.
3. Seleccione **continuar**.

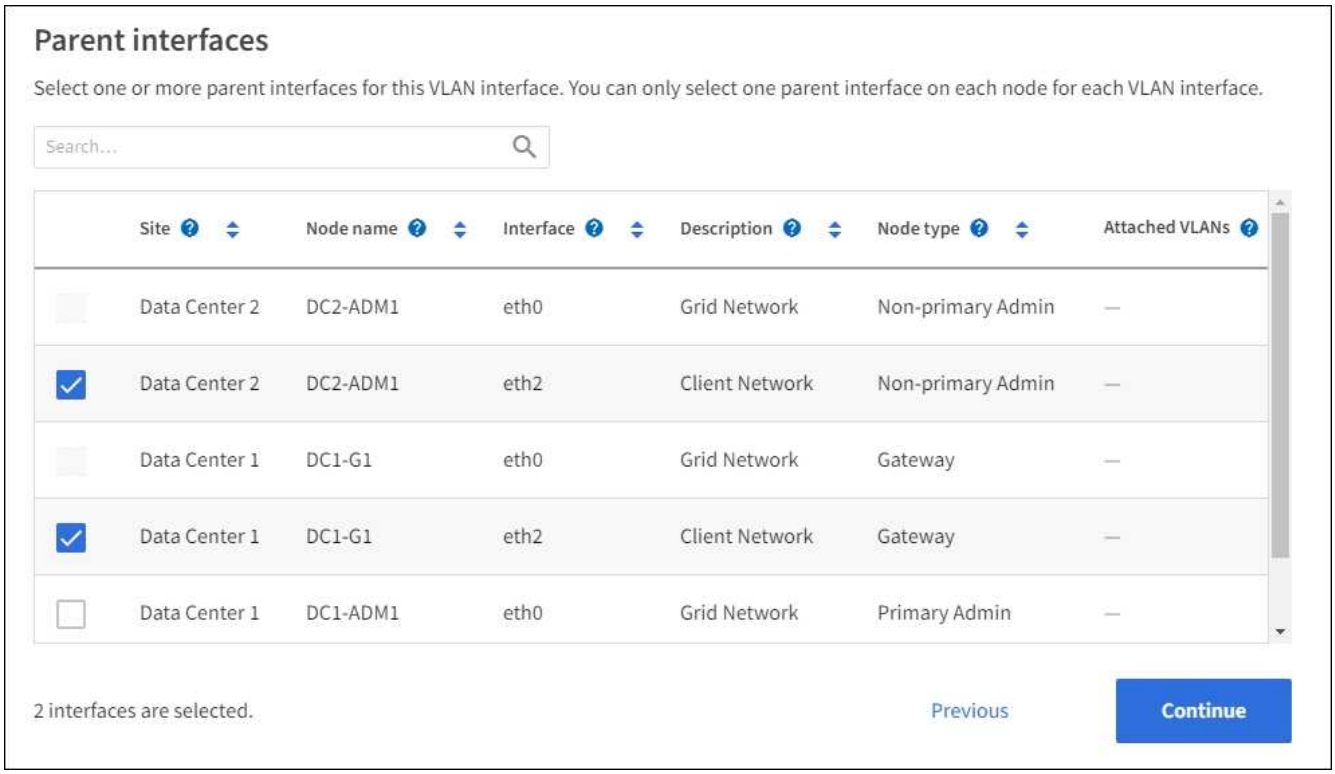
Elija interfaces padre

En la tabla, se enumeran las interfaces disponibles para todos los nodos de administrador y los nodos de puerta de enlace en cada sitio del grid. Las interfaces de la red de administración (eth1) no se pueden utilizar como interfaces principales y no se muestran.

Pasos

1. Seleccione una o varias interfaces primarias para asociar esta VLAN.

   Por ejemplo, es posible que desee conectar una VLAN a la interfaz de red de cliente (eth2) para un nodo de puerta de enlace y un nodo de administrador.



2. Seleccione **continuar**.

Confirme la configuración

Pasos

1. Revise la configuración y realice cualquier cambio.
   - Si necesita cambiar el ID de VLAN o la descripción, seleccione **introducir detalles de VLAN** en la parte superior de la página.
   - Si necesita cambiar una interfaz padre, seleccione **elegir interfaces padre** en la parte superior de la página o seleccione **anterior**.
   - Si necesita quitar una interfaz principal, seleccione la papelera .
2. Seleccione **Guardar**.
3. Espere hasta 5 minutos para que la nueva interfaz aparezca como una selección en la página grupos de alta disponibilidad y aparezca en la tabla * interfaces de red* para el nodo (**NODES** > ***nodo de interfaz principal*** > **Red**).

Edite una interfaz VLAN

Cuando edite una interfaz de VLAN, puede realizar los siguientes tipos de cambios:

- Cambie el ID o la descripción de la VLAN.
- Agregar o quitar interfaces principales.

Por ejemplo, es posible que desee quitar una interfaz principal de una interfaz VLAN si va a retirar el nodo asociado.

Tenga en cuenta lo siguiente:

- No puede cambiar un ID de VLAN si la interfaz VLAN se utiliza en un grupo de alta disponibilidad.
- No puede quitar una interfaz principal si se utiliza esa interfaz principal en un grupo de alta disponibilidad.

  Por ejemplo, supongamos que la VLAN 200 está conectada a las interfaces principales de los nodos A y B. Si un grupo de alta disponibilidad utiliza la interfaz VLAN 200 para el nodo A y la interfaz eth2 para el nodo B, puede quitar la interfaz principal sin usar para el nodo B, pero no puede quitar la interfaz principal utilizada para el nodo A.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione la casilla de comprobación de la interfaz de VLAN que desea editar. A continuación, seleccione **acciones** > **Editar**.
3. Si lo desea, actualice el ID de VLAN o la descripción. A continuación, seleccione **continuar**.

   No se puede actualizar un identificador de VLAN si la VLAN se utiliza en un grupo de alta disponibilidad.

4. Opcionalmente, active o desactive las casillas de verificación para agregar interfaces principales o para eliminar las interfaces no utilizadas. A continuación, seleccione **continuar**.
5. Revise la configuración y realice cualquier cambio.
6. Seleccione **Guardar**.

Quite una interfaz VLAN

Puede eliminar una o varias interfaces VLAN.

No puede quitar una interfaz VLAN si actualmente se utiliza en un grupo de alta disponibilidad. Para poder eliminarlo, debe quitar la interfaz VLAN del grupo ha.

Para evitar cualquier interrupción en el tráfico de cliente, considere realizar una de las siguientes acciones:

- Añada una nueva interfaz VLAN al grupo de alta disponibilidad antes de eliminar esta interfaz de VLAN.
- Cree un nuevo grupo de alta disponibilidad que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que desea quitar tiene actualmente la interfaz activa, edite el grupo de alta disponibilidad. Mueva la interfaz de VLAN que desea quitar a la parte inferior de la lista de prioridades. Espere hasta que se establezca la comunicación en la nueva interfaz principal y, a continuación, quite la interfaz antigua del grupo de alta disponibilidad. Por último, elimine la interfaz de VLAN en ese nodo.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione la casilla de comprobación de cada interfaz de VLAN que desea quitar. A continuación, seleccione **acciones** > **Eliminar**.
3. Seleccione **Sí** para confirmar su selección.

   Se eliminan todas las interfaces VLAN seleccionadas. Se muestra un banner verde de éxito en la página de interfaces de VLAN.

Administrar directivas de clasificación de tráfico

Para mejorar sus ofertas de calidad de servicio (QoS), puede crear normativas de clasificación del tráfico para identificar y supervisar distintos tipos de tráfico de red. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Las políticas de clasificación del tráfico se aplican a los extremos en el servicio StorageGRID Load Balancer para los nodos de puerta de enlace y los nodos de administración. Para crear directivas de clasificación de tráfico, debe haber creado ya puntos finales de equilibrador de carga.

Reglas de coincidencia

Cada directiva de clasificación de tráfico contiene una o más reglas coincidentes para identificar el tráfico de red relacionado con una o varias de las siguientes entidades:

- Cucharones
- Subred
- Inquilino
- Puntos finales del equilibrador de carga

StorageGRID supervisa el tráfico que coincide con cualquier regla dentro de la política de acuerdo con los objetivos de la regla. Cualquier tráfico que coincida con cualquier regla de una directiva se gestiona mediante dicha directiva. A la inversa, puede establecer reglas que coincidan con todo el tráfico excepto una entidad especificada.

Limitación del tráfico

Opcionalmente, puede agregar los siguientes tipos de límite a una política:

- Ancho de banda de agregado
- Ancho de banda por solicitud
- Solicitudes simultáneas
- Tasa de solicitud

Los valores límite se aplican por cada equilibrador de carga. Si el tráfico se distribuye de forma simultánea entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de velocidad que especifique.

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, la StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado.

Para límites de ancho de banda agregados o por solicitud, las solicitudes se transmiten de entrada o salida a la velocidad establecida. StorageGRID sólo puede aplicar una velocidad, por lo que la política más específica, por tipo de matrcher, es la aplicada. El ancho de banda consumido por la solicitud no cuenta en comparación con otras políticas que coincidan menos específicas que contengan políticas de límite de ancho de banda agregado. Para todos los demás tipos de límites, las solicitudes de clientes se retrasan 250 milisegundos y reciben una respuesta de reducción lenta de 503 para las solicitudes que exceden cualquier límite de directiva coincidente.

En Grid Manager, puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Utilice las políticas de clasificación del tráfico con los SLA

Puede utilizar políticas de clasificación del tráfico junto con los límites de capacidad y protección de datos para aplicar acuerdos de nivel de servicio (SLA) que ofrezcan detalles sobre la capacidad, la protección de datos y el rendimiento.

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	El máximo rendimiento permitido	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
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

Cree directivas de clasificación de tráfico

Puede crear políticas de clasificación del tráfico si desea supervisar y, de manera opcional, limitar el tráfico de red por bloque, periodo de reunión, CIDR, extremo de equilibrador de carga o inquilino. 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Ha creado cualquier punto final de equilibrador de carga que desee que coincida.
- Ha creado los inquilinos que desea que coincidan.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Introduzca un nombre y una descripción (opcional) para la política y seleccione **Continuar**.

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

4. Seleccione **Añadir regla** y especifique los siguientes detalles para crear una o más reglas de coincidencia para la política. Cualquier política que cree debe tener al menos una regla de coincidencia. Seleccione **continuar**.

Campo	Descripción
Tipo	Seleccione los tipos de tráfico a los que se aplica la regla de coincidencia. Los tipos de tráfico son bucket, bucket regex, CIDR, load balancer endpoint y tenant.
Valor de coincidencia	Introduzca el valor que coincida con el tipo seleccionado. • Bucket: Introduzca uno o más nombres de bucket. • Bucket Regex: Introduzca una o más expresiones regulares utilizadas para hacer coincidir un juego de nombres de cubos. La expresión regular no está anclada. Utilice el anclaje ^ para que coincida al principio del nombre del cubo y utilice el anclaje $ para que coincida al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de sintaxis PCRE (expresión regular compatible con Perl). • CIDR: Introduzca una o más subredes IPv4, en notación CIDR, que coincida con la subred deseada. • Punto final de equilibrio de carga: Seleccione un nombre de punto final. Estos son los puntos finales del equilibrador de carga definidos en "Configurar puntos finales del equilibrador de carga". • Tenant: La coincidencia de inquilinos utiliza el ID de clave de acceso. Si la solicitud no contiene un identificador de clave de acceso (por ejemplo, acceso anónimo), la propiedad del bloque al que se accede se utiliza para determinar el inquilino.
Coincidencia inversa	Si desea hacer coincidir todo el tráfico de red *excepto* tráfico consistente con el valor Tipo y Coincidencia que acaba de definir, seleccione la casilla de verificación **Coincidencia inversa**. De lo contrario, deje la casilla de verificación desactivada. Por ejemplo, si desea que esta política se aplique a todos los puntos finales excepto a uno de los de equilibrio de carga, especifique el punto final de equilibrio de carga que se va a excluir y seleccione **Coincidencia inversa**. 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.

5. Opcionalmente, seleccione **Agregar un límite** y seleccione los siguientes detalles para agregar uno o más límites para controlar el tráfico de red que coincide con una regla.

> StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias del tráfico.

Campo	Descripción
Tipo	El tipo de límite que desea aplicar al tráfico de red coincidente con la regla. Por ejemplo, puede limitar el ancho de banda o la tasa de solicitud. **Nota**: Puede crear políticas para limitar el ancho de banda agregado o limitar el ancho de banda por solicitud. Sin embargo, la StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Cuando se utiliza el ancho de banda agregado, el ancho de banda por solicitud no está disponible. Por el contrario, cuando se utiliza el ancho de banda por solicitud, el ancho de banda agregado no estará disponible. 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 implanta las «mejores» coincidencias para los 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
Se aplica a.	Si este límite se aplica a las solicitudes de lectura del cliente (GET o HEAD) o las solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, en función de la unidad que seleccione. Por ejemplo, introduzca 10 y seleccione MiB/s para evitar que el tráfico de red que coincide con esta regla supere los 10 MiB/s. **Nota**: Dependiendo de la configuración de unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar la configuración de unidades, seleccione la lista desplegable de usuario en la parte superior derecha del Administrador de cuadrícula y, a continuación, seleccione **Preferencias de usuario**.
Unidad	La unidad que describe el valor introducido.

Por ejemplo, si desea crear un límite de ancho de banda de 40 GB/s para un nivel de SLA, cree dos límites de ancho de banda agregados: GET/HEAD at 40 GB/s y PUT/POST/DELETE at 40 GB/s.

6. Seleccione **continuar**.

7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

   El tráfico de clientes S3 y Swift ahora se maneja de acuerdo con la política de clasificación del tráfico.

Después de terminar

"Ver las métricas de tráfico de red" para verificar que las políticas están aplicando los límites de tráfico que espera.

Edite la política 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.

Antes de empezar

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Políticas de clasificación de tráfico y las políticas existentes se muestran en una tabla.

2. Edite la política mediante el menú Acciones o la página de detalles. Consulte "crear políticas de clasificación de tráfico" para qué entrar.

   Menú Actions

   a. Seleccione la casilla de verificación de la política.
   b. Selecciona **Acciones** > **Editar**.

   Detalles

   a. Seleccione el nombre de la política.
   b. Seleccione el botón **Editar** junto al nombre de la política.

3. Para el paso Introducir nombre de política, edite opcionalmente el nombre o la descripción de la política y seleccione **Continuar**.
4. Para el paso Agregar reglas de coincidencia, opcionalmente agregue una regla o edite el **Tipo** y **Valor de coincidencia** de la regla existente, y seleccione **Continuar**.
5. Para el paso Establecer límites, opcionalmente agregue, edite o elimine un límite, y seleccione **Continuar**.
6. Revise la política actualizada y seleccione **Guardar y continuar**.

   Los cambios realizados en la directiva se guardan y el tráfico de red se gestiona de acuerdo con las directivas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Eliminar una directiva de clasificación de tráfico

Puede eliminar una política de clasificación de tráfico si ya no la necesita. Asegúrese de eliminar la política correcta porque no se puede recuperar una política al eliminarla.

Antes de empezar

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Políticas de clasificación de tráfico con las políticas existentes enumeradas en una tabla.

2. Elimine la política mediante el menú Acciones o la página de detalles.

   Menú Actions

   a. Seleccione la casilla de verificación de la política.

   b. Seleccione **acciones** > **Quitar**.

   Página de detalles de política

   a. Seleccione el nombre de la política.

   b. Seleccione el botón **Eliminar** junto al nombre de la política.

3. Seleccione **Sí** para confirmar que desea eliminar la política.

   La directiva se elimina.

Ver las métricas de tráfico de red

Puede supervisar el tráfico de red mediante los gráficos que están disponibles en la página de políticas de clasificación del tráfico.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso de acceso root o el permiso de cuentas de tenant.

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puede ver métricas para el servicio de equilibrio de carga para determinar si la política está limitando correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si necesita ajustar la política.

Incluso si no se establecen límites para una política de clasificación del tráfico, se recopilan las métricas y los gráficos proporcionan información útil para comprender las tendencias del tráfico.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

Aparece la página Políticas de clasificación de tráfico y las políticas existentes se muestran en la tabla.

2. Seleccione el nombre de la política de clasificación de tráfico para la que desea ver las métricas.
3. Seleccione la pestaña **Métricas**.

   Aparecen los gráficos de política de clasificación de tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Los siguientes gráficos se incluyen en la página.

   - Tasa de solicitud: Este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los equilibradores de carga. Los datos recibidos incluyen cabeceras de solicitud para todas las solicitudes y tamaño de datos de cuerpo para las respuestas que tienen datos de cuerpo. Enviado incluye cabeceras de respuesta para todas las solicitudes y tamaño de datos de cuerpo de respuesta para las solicitudes que incluyen datos de cuerpo en la respuesta.

     > Cuando se completan las solicitudes, este gráfico sólo muestra el uso del ancho de banda. Para solicitudes de objetos lentas o grandes, el ancho de banda instantáneo real puede diferir de los valores indicados en este gráfico.

   - Tasa de respuesta de error: Este gráfico proporciona una tasa aproximada a la que las solicitudes que coinciden con esta política devuelven errores (código de estado HTTP >= 400) a los clientes.
   - Duración media de la solicitud (sin error): Este gráfico proporciona una duración media de las solicitudes correctas que coinciden con esta política.
   - Uso de ancho de banda de política: Este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los equilibradores de carga. Los datos recibidos incluyen cabeceras de solicitud para todas las solicitudes y tamaño de datos de cuerpo para las respuestas que tienen datos de cuerpo. Enviado incluye cabeceras de respuesta para todas las solicitudes y tamaño de datos de cuerpo de respuesta para las solicitudes que incluyen datos de cuerpo en la respuesta.
4. Coloque el cursor sobre un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.
5. Seleccione **Grafana dashboard** justo debajo del título de Métricas para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Métricas**, puedes ver dos gráficos más:
   - Ratio de solicitud de escritura por tamaño de objeto: Ratio de solicitudes DE PUT/POST/DELETE que coincidan con esta política. El posicionamiento en una celda individual muestra las tasas por segundo. Las tasas que se muestran en la vista flotante se truncan en números enteros y pueden informar de 0 cuando hay solicitudes que no sean cero en el bloque.
   - Tasa de solicitud de lectura por tamaño de objeto: La tasa de SOLICITUDES DE OBTENCIÓN/CABECERA que coinciden con esta política. El posicionamiento en una celda individual muestra las tasas por segundo. Las tasas que se muestran en la vista flotante se truncan en números enteros y pueden informar de 0 cuando hay solicitudes que no sean cero en el bloque.
6. También puede acceder a los gráficos desde el menú **SUPPORT**.
   a. Seleccione **SUPPORT** > **Tools** > **Metrics**.
   b. Selecciona **Política de clasificación de tráfico** en la sección **Grafana**.
   c. Seleccione la política en el menú en la parte superior izquierda de la página.
   d. Coloque el cursor sobre un gráfico para ver una ventana emergente que muestra la fecha y hora de la muestra, los tamaños de los objetos que se agregan al recuento y el número de solicitudes por segundo durante ese período de tiempo.

Las directivas de clasificación del tráfico se identifican por su ID. Los ID de política se muestran en la página de políticas de clasificación de tráfico.

7. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

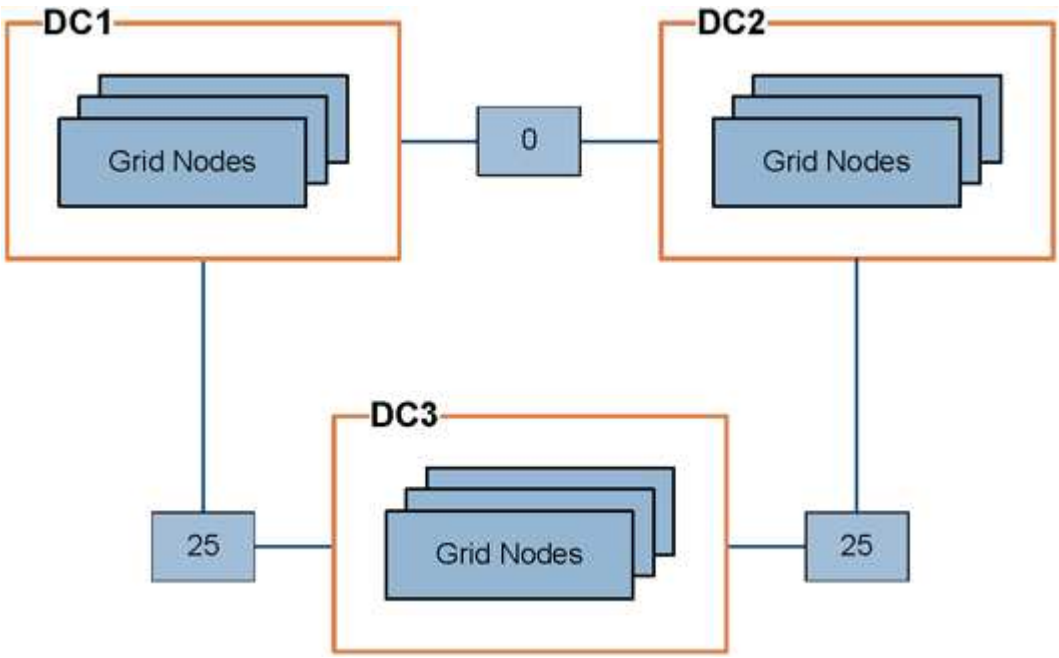
Gestionar costes de enlaces

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.

¿Qué son los costes de enlace?

- 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 de equilibrio de carga en los nodos de administración y de gateway para dirigir las conexiones de cliente. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

El diagrama muestra una cuadrícula de tres sitios con costes de enlace configurados entre sitios:



- El servicio Load Balancer en los nodos de administración y de puerta de enlace distribuye equitativamente las conexiones de los clientes a todos los nodos de almacenamiento en el 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 de DC2 recupera un objeto almacenado tanto en DC1 como en DC3, el objeto se recupera de DC1, porque el coste del enlace de DC1 a DC2 es 0, que es inferior al coste del enlace de DC3 a DC2 (25).

Los costes de enlace son números relativos arbitrarios sin unidad de medida específica. Por ejemplo, un costo de enlace de 50 se utiliza de forma menos preferente que un costo de enlace de 25. En la tabla se muestran los costes de los enlaces más utilizados.

Enlace	Coste del enlace	Notas
Entre sitios físicos del centro de datos	25 (predeterminado)	Centros de datos conectados por un enlace WAN.
Entre las ubicaciones lógicas del centro de datos en la misma ubicación física	0	Centros de datos lógicos en el mismo edificio físico o campus conectados por una LAN.

Actualizar costes de enlace

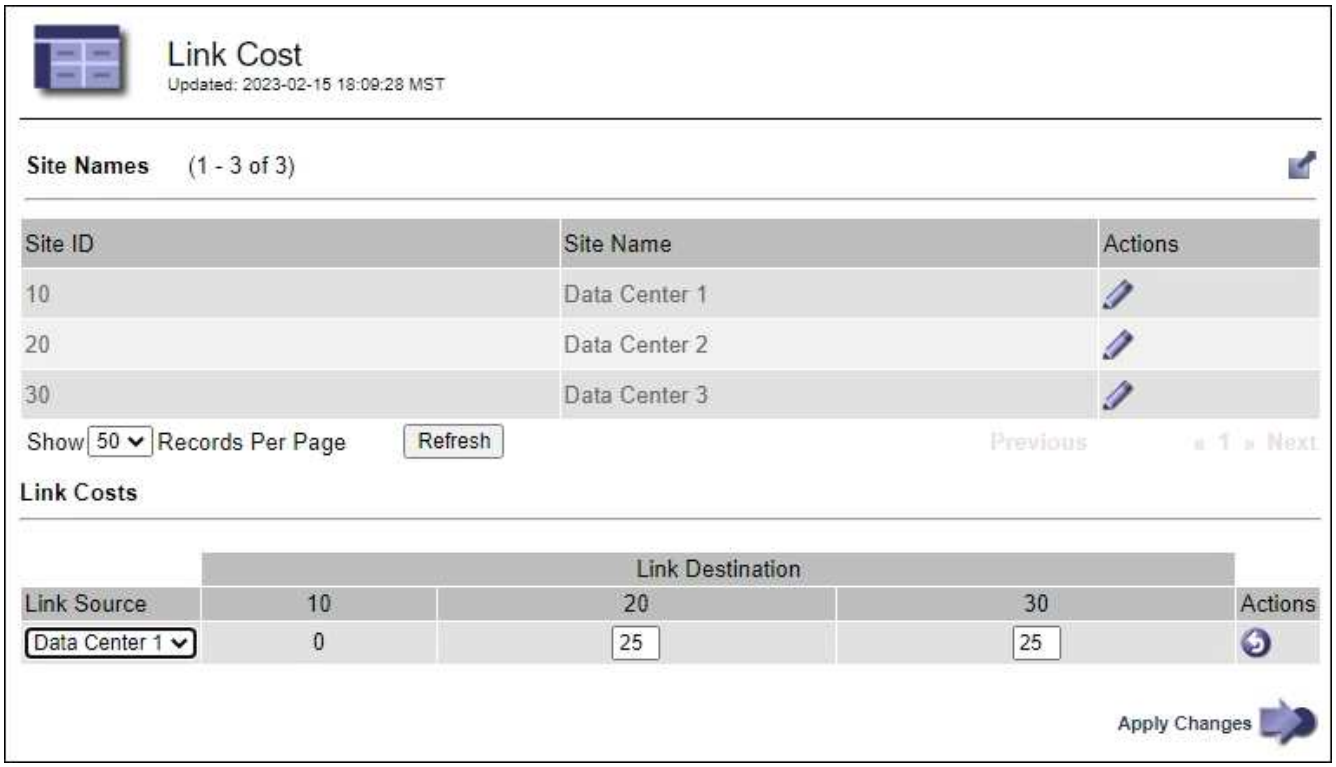
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de configuración de la página de topología de cuadrícula".

Pasos

1. Selecciona **SOPORTE** > **OTRO** > **Costo 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 puede cambiar el coste del enlace si el origen es el mismo que el destino.

   Para cancelar los cambios, seleccione **Revert**.

3. Seleccione **aplicar cambios**.

Utilice AutoSupport

Utilice AutoSupport: Descripción general

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.

Debe configurar StorageGRID AutoSupport solo en el nodo de administración principal. Sin embargo, debe configurar AutoSupport de hardware en cada aparato.

Información incluida en los mensajes de AutoSupport

Los mensajes de AutoSupport incluyen información como la siguiente:

- Versión del software StorageGRID
- Versión del sistema operativo

- Información de atributos a nivel de sistema y ubicación
- Alertas y alarmas recientes (sistema heredado)
- Estado actual de todas las tareas de cuadrícula, incluidos los datos históricos
- Uso de la base de datos del nodo de administrador
- Número de objetos perdidos o faltantes
- Ajustes de configuración de cuadrícula
- Entidades NMS
- Política de ILM activa
- Archivo de especificación de grid aprovisionado
- Métricas de diagnóstico

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante. Si AutoSupport no está activado, aparece un mensaje en el panel de control de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport.

Si cierra el mensaje, no volverá a aparecer hasta que se borre la caché del explorador, aunque AutoSupport permanezca deshabilitado.

¿Qué es el asesor digital?

El asesor digital está basado en la nube y 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 del asesor digital en el sitio de soporte de NetApp.

"Documentación del asesor digital"

Protocolos para enviar mensajes AutoSupport

Puede elegir uno de los tres protocolos para enviar mensajes de AutoSupport:

- HTTPS
- HTTP
- SMTP

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.

AutoSupport para dispositivos

AutoSupport para dispositivos informa de problemas de hardware de StorageGRID, mientras que StorageGRID AutoSupport informa de problemas de software de StorageGRID (excepto SGF6112, donde StorageGRID AutoSupport informa de problemas de hardware y software). Debe configurar AutoSupport en cada dispositivo, excepto para el SGF6112 que no requiera una configuración adicional. AutoSupport se ha implantado de forma diferente para los servicios y las aplicaciones de almacenamiento.

Debe habilitar AutoSupport en SANtricity para cada dispositivo de almacenamiento. Es posible configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de haber instalado un dispositivo:

- Para dispositivos SG6000 y SG5700, "Configure AutoSupport en SANtricity System Manager"

Los mensajes de AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si se configura la entrega de AutoSupport mediante proxy en "System Manager de SANtricity".

StorageGRID AutoSupport no informa de problemas de hardware, como fallos de DIMM o de tarjeta de interfaz del host (HIC). Sin embargo, algunos fallos de componentes pueden desencadenarse "alertas de hardware". En el caso de dispositivos StorageGRID con un controlador de administración de placa base (BMC), como SG100, SG1000, SG6060 o SGF6024, puede configurar capturas de correo electrónico y SNMP para informar de fallos de hardware:

- "Configure notificaciones por correo electrónico para las alertas"
- "Configure los ajustes de SNMP" Para la controladora SG6000-CN o los dispositivos de servicios SG100 y SG1000

Información relacionada

"Soporte de NetApp"

Configure AutoSupport

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz u otra configuración de cuadrícula.

- Si va a utilizar HTTPS para enviar mensajes de AutoSupport, ha proporcionado acceso a Internet saliente al nodo de administración principal, ya sea directamente o "utilizando un servidor proxy" (no se requieren conexiones entrantes).
- Si se selecciona HTTP en la página StorageGRID AutoSupport, se ha configurado un servidor proxy para reenviar mensajes de AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazarán los mensajes enviados mediante HTTP.

  "Obtenga más información sobre la configuración de los ajustes de proxy de administración".

- Si utilizará SMTP como protocolo para mensajes de AutoSupport, configuró un servidor de correo SMTP. La misma configuración del servidor de correo se utiliza para las notificaciones de correo electrónico de alarma (sistema heredado).

Especifique el protocolo para los mensajes de AutoSupport

Puede utilizar cualquiera de los siguientes protocolos para enviar mensajes de AutoSupport:

- **HTTPS**: Es la configuración predeterminada y recomendada para nuevas instalaciones. Este protocolo utiliza el puerto 443. Si desea Habilite la función AutoSupport On Demand, Debe utilizar HTTPS.
- **HTTP**: Si selecciona HTTP, debe configurar un servidor proxy para reenviar mensajes AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazan los mensajes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP**: Utilice esta opción si desea que se envíen mensajes de AutoSupport por correo electrónico. Si utiliza SMTP como protocolo para mensajes AutoSupport, debe configurar un servidor de correo SMTP en la página Configuración de correo electrónico heredado (**SUPPORT** > **Alarmas (heredado)** > **Configuración de correo electrónico heredado**).

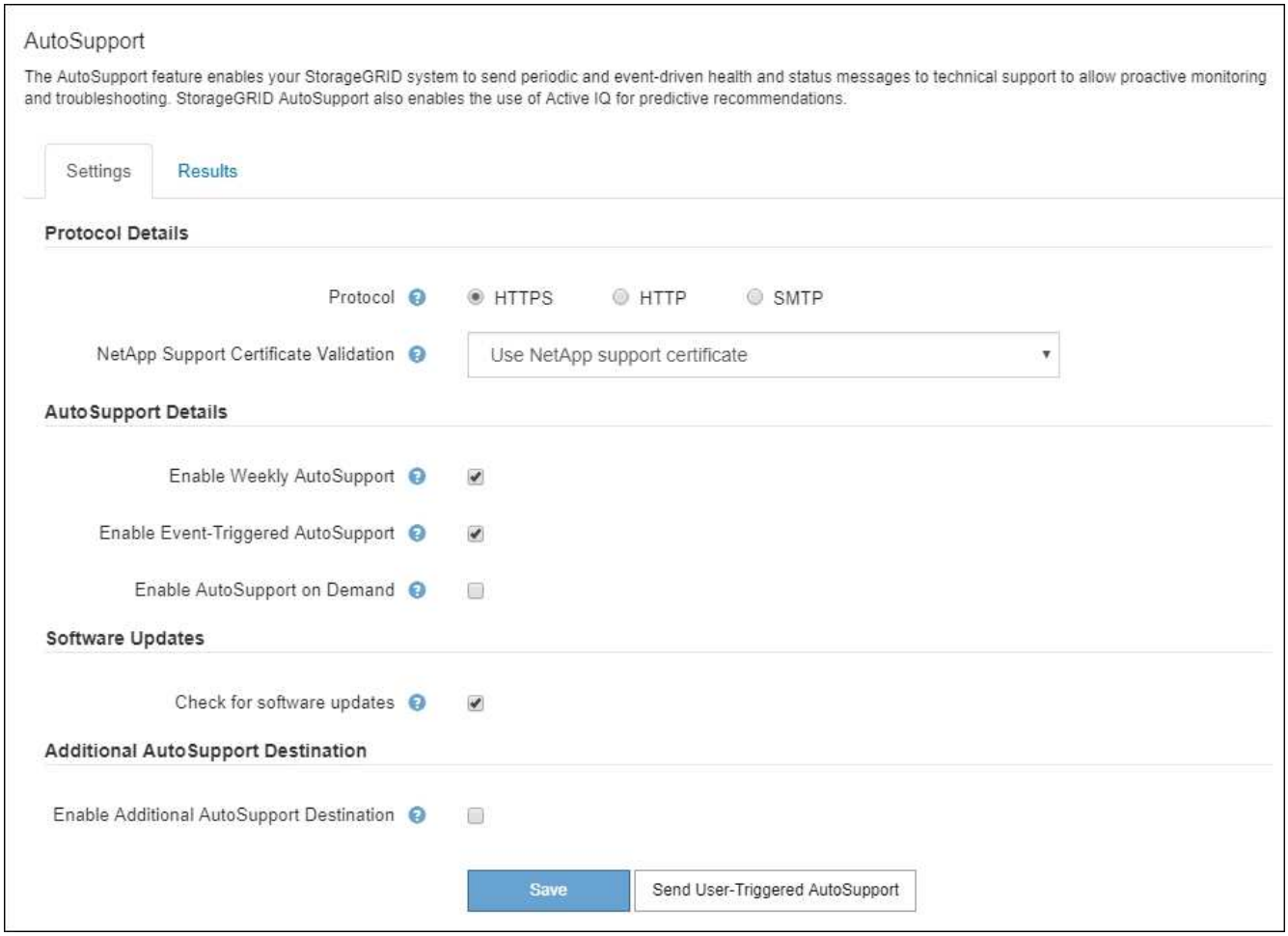
> ⓘ SMTP era el único protocolo disponible para mensajes de AutoSupport antes de la versión de StorageGRID 11.2. Si instaló inicialmente una versión anterior de StorageGRID, es posible que SMTP sea el protocolo seleccionado.

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.

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



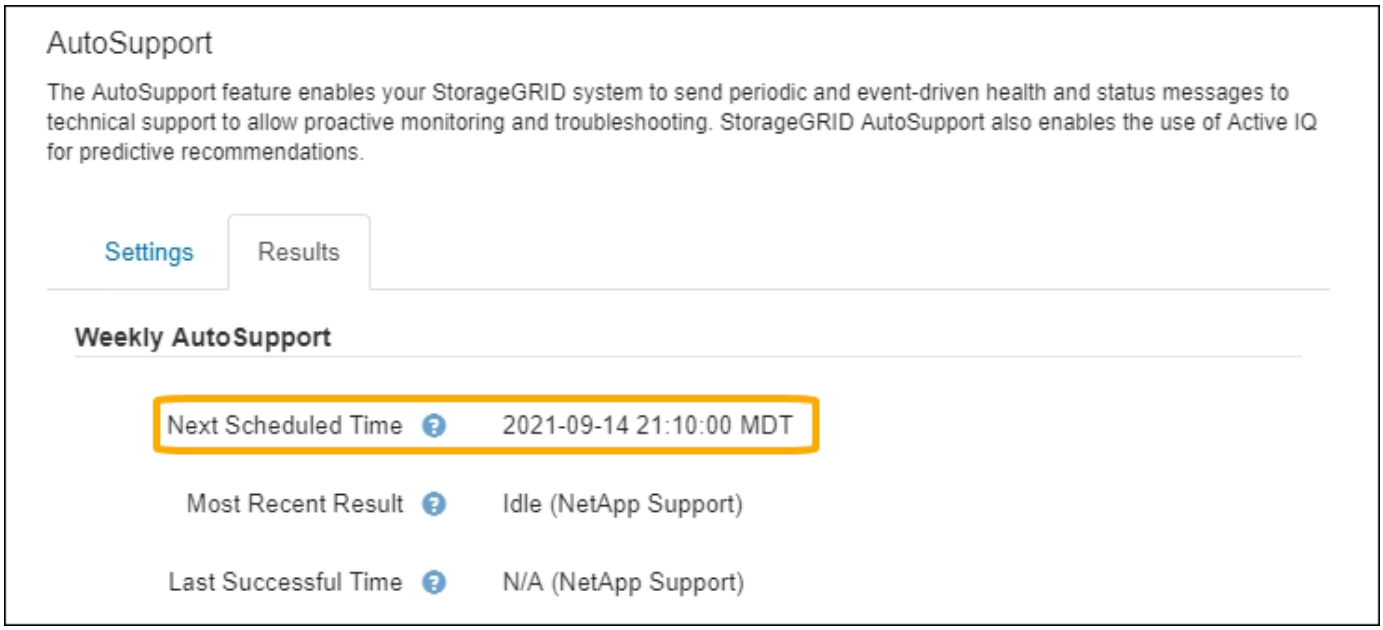
2. Seleccione el protocolo que desea utilizar para enviar mensajes de AutoSupport.
3. Si seleccionó **HTTPS**, seleccione si desea utilizar un certificado TLS para proteger la conexión con el servidor de soporte de NetApp.
   - **Utilizar el certificado de soporte de NetApp** (predeterminado): La validación del certificado garantiza la seguridad de la transmisión de mensajes AutoSupport. El certificado de soporte de NetApp ya está instalado con el software StorageGRID.
   - **No verificar certificado**: Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.
4. Seleccione **Guardar**.

   Todos los mensajes semanales, activados por el usuario y activados por un evento se envían mediante el protocolo seleccionado.

Desactivar los mensajes semanales de AutoSupport

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

Para determinar cuándo se enviará el mensaje semanal de AutoSupport, vaya a la ficha **AutoSupport** > **resultados**. En la sección **AutoSupport** semanal, consulte el valor de **próxima hora programada**.



Puede deshabilitar el envío automático de mensajes semanales de AutoSupport en cualquier momento.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Desactive la casilla de verificación **Activar AutoSupport semanal**.
3. Seleccione **Guardar**.

Deshabilite los mensajes de AutoSupport activados por un evento

De forma predeterminada, el sistema StorageGRID se configura para enviar un mensaje de AutoSupport al soporte de NetApp cuando se produce una alerta importante u otro evento significativo del sistema.

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Desactive la casilla de verificación **Activar AutoSupport desencadenado por eventos**.
3. Seleccione **Guardar**.

Habilite AutoSupport bajo demanda

AutoSupport On Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente.

De manera predeterminada, AutoSupport On Demand está deshabilitado. Al habilitar esta función, el soporte técnico puede solicitar que el sistema StorageGRID envíe mensajes de AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de sondeo para AutoSupport en consultas bajo demanda.

El soporte técnico no puede habilitar ni deshabilitar AutoSupport On Demand.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.

2. Seleccione **HTTPS** para el protocolo.
3. Seleccione la casilla de verificación **Activar AutoSupport semanal**.
4. Seleccione la casilla de verificación **Activar AutoSupport On Demand**.
5. Seleccione **Guardar**.

   AutoSupport On Demand está habilitado y el soporte técnico puede enviar solicitudes AutoSupport On Demand a StorageGRID.

Desactive las comprobaciones de actualizaciones de software

De forma predeterminada, StorageGRID se pone en contacto con NetApp para determinar si hay actualizaciones de software disponibles para su sistema. Si hay disponible una revisión o versión nueva de StorageGRID, se muestra la nueva versión en la página actualización de StorageGRID.

Según sea necesario, puede desactivar opcionalmente la comprobación de actualizaciones de software. Por ejemplo, si el sistema no tiene acceso WAN, debe desactivar la comprobación para evitar errores de descarga.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Desactive la casilla de verificación **Comprobar si hay actualizaciones de software**.
3. Seleccione **Guardar**.

Añada un destino de AutoSupport adicional

Cuando habilita AutoSupport, se envían mensajes de estado y estado al soporte de NetApp. Puede especificar un destino adicional para todos los mensajes de AutoSupport.

Para comprobar o cambiar el protocolo utilizado para enviar mensajes AutoSupport, consulte las instrucciones a. Especifique el protocolo para los mensajes de AutoSupport.

No puede usar el protocolo SMTP para enviar mensajes de AutoSupport a un destino adicional.

Pasos

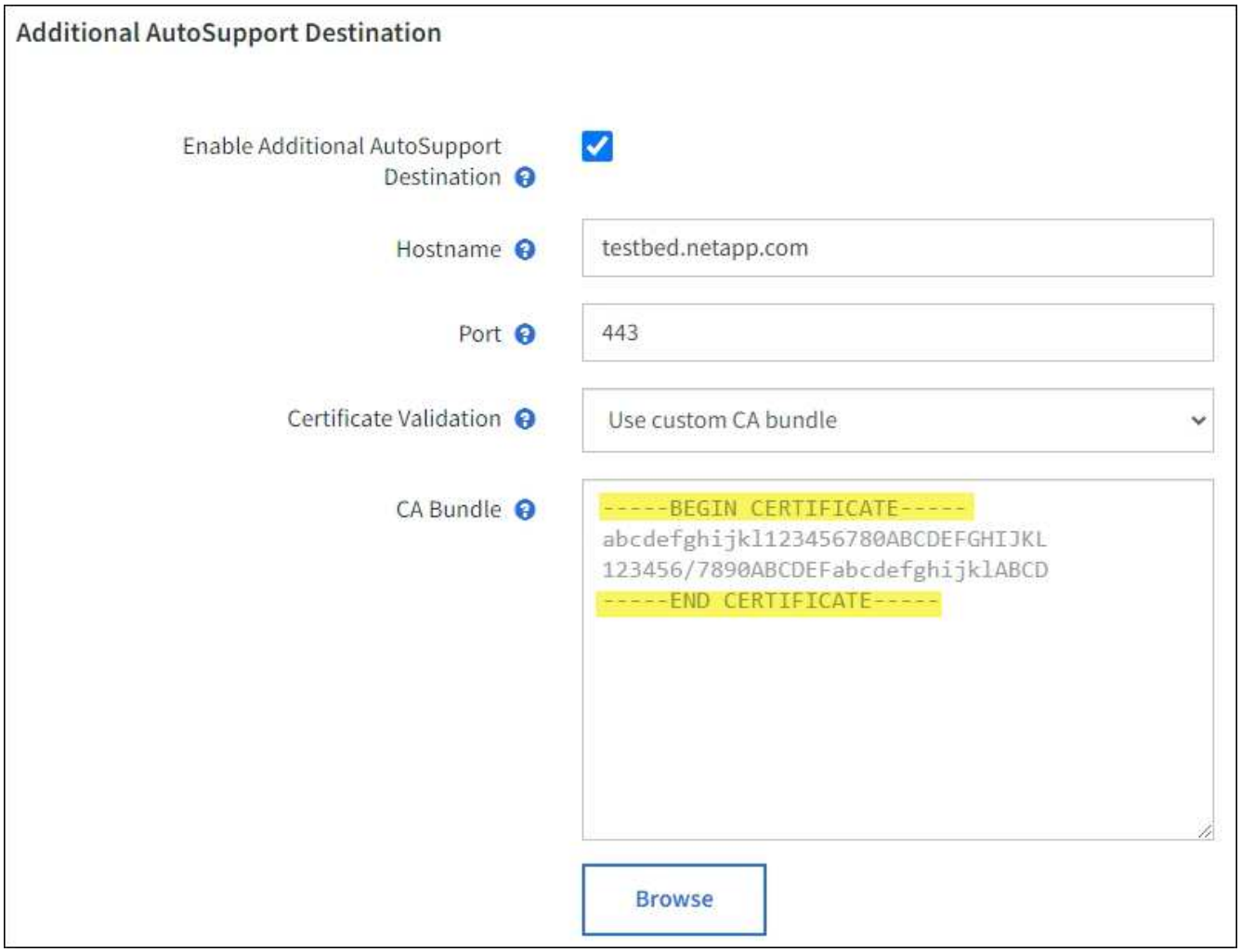
1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Selecciona **Activar destino AutoSupport adicional**.
3. Especifique lo siguiente:

Campo	Descripción
Nombre del hostl	Nombre de host o dirección IP del servidor de un servidor de destino AutoSupport adicional. **Nota**: Puedes ingresar solo un destino adicional.
Puerto	Puerto utilizado para conectarse a un servidor de destino AutoSupport adicional. El valor predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

Campo	Descripción
Validación de certificación	Si se utiliza un certificado TLS para proteger la conexión al destino adicional. • Seleccione **No verificar certificado** para enviar sus mensajes AutoSupport sin validación de 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. • Seleccione **Usar paquete de CA personalizado** para utilizar la validación de certificados.

4. Si seleccionó **Usar paquete de CA personalizado**, realice una de las siguientes acciones:
   - Seleccione **examinar**, desplácese hasta el archivo que contiene los certificados y, a continuación, seleccione **Abrir** para cargar el archivo.
   - Utilice una herramienta de edición para copiar y pegar todo el contenido de cada uno de los archivos de certificado CA codificados con PEM en el campo **CA Bundle**, concatenado en orden de cadena de certificados.

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



5. Seleccione **Guardar**.

   Todos los futuros mensajes de AutoSupport semanales, activados por un evento y activados por el usuario se enviarán al destino adicional.

Active manualmente un mensaje de AutoSupport

Con el fin de ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID, puede activar manualmente el envío de un mensaje de AutoSupport.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Debe tener el acceso root u otro permiso de configuración de grid.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. En la pestaña **Configuración**, selecciona **Enviar AutoSupport activado por el usuario**.

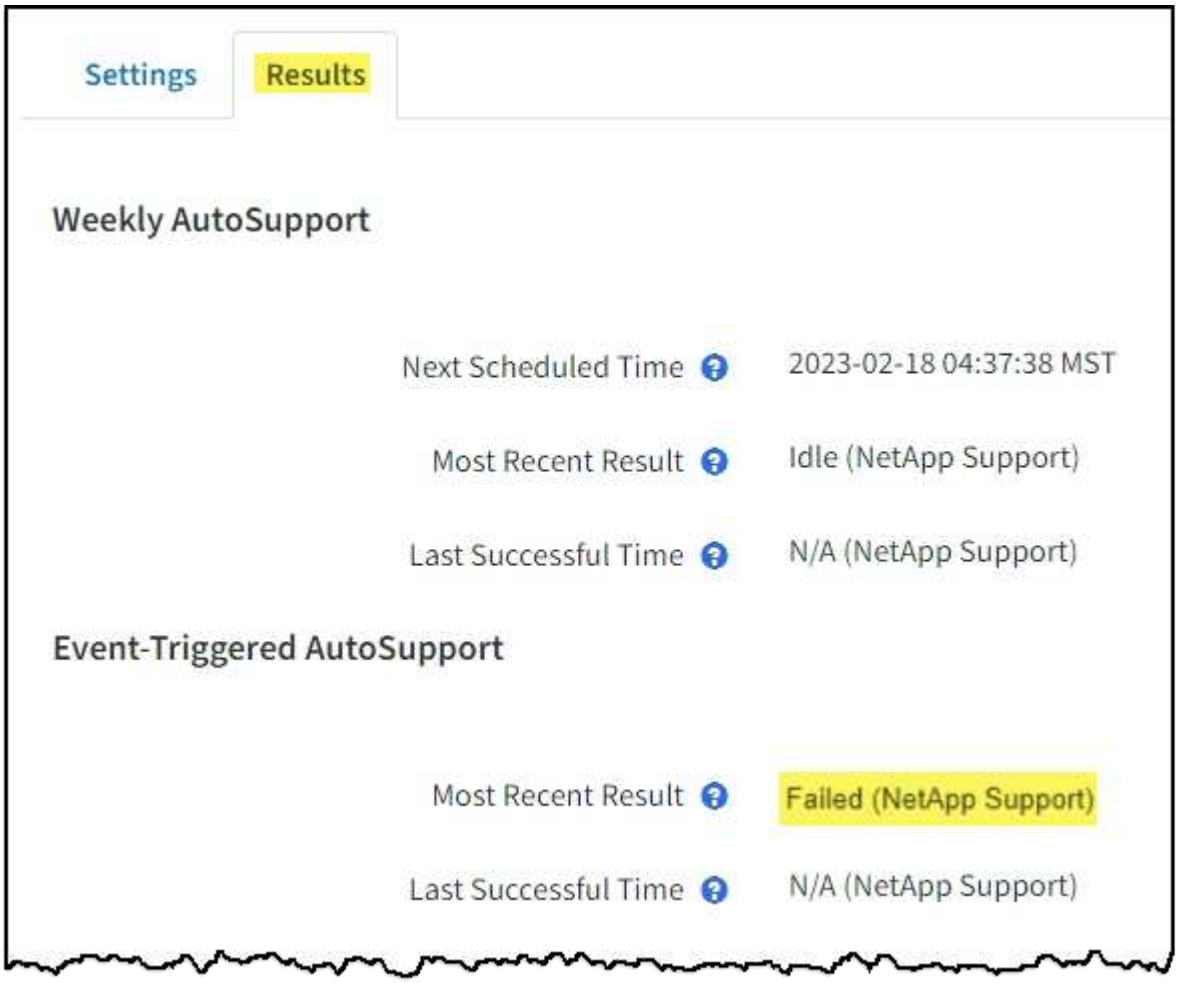
   StorageGRID intenta enviar un mensaje de AutoSupport al soporte técnico. Si el intento se realiza correctamente, se actualizan los valores **resultado más reciente** y **tiempo más reciente** de la ficha **resultados**. Si hay algún problema, el valor del **resultado más reciente** se actualiza a "error" y StorageGRID no intenta volver a enviar el mensaje AutoSupport.

Después de enviar un mensaje AutoSupport activado por el usuario, actualice la página AutoSupport en el explorador después de 1 minuto para acceder a los resultados más recientes.

Solucionar los problemas de los mensajes de AutoSupport

Si se produce un error al intentar enviar un mensaje de AutoSupport, el sistema StorageGRID realiza distintas acciones según el tipo de mensaje de AutoSupport. Puede comprobar el estado de los mensajes de AutoSupport seleccionando **ASISTENCIA** > **Herramientas** > **AutoSupport** > **resultados**.

Cuando el mensaje AutoSupport no se envía, aparece "'failed'" en la ficha **resultados** de la página **AutoSupport**.



Si configuró un servidor proxy para reenviar mensajes de AutoSupport a NetApp, debería hacerlo "compruebe que los valores de configuración del servidor proxy son correctos".

Fallo de mensaje semanal de AutoSupport

Si un mensaje semanal de AutoSupport no se envía, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo de resultado más reciente a Reintentando.

2. Intenta reenviar el mensaje AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de errores de envío, actualiza el atributo de resultado más reciente a error.
4. Intenta enviar de nuevo un mensaje de AutoSupport a la siguiente hora programada.
5. Mantiene la programación normal de AutoSupport si el mensaje falla porque el servicio NMS no está disponible y si se envía un mensaje antes de pasar siete días.
6. Cuando el servicio NMS está disponible de nuevo, envía un mensaje AutoSupport inmediatamente si no se ha enviado un mensaje durante siete días o más.

Error de mensaje AutoSupport activado por el usuario o activado por eventos

Si un mensaje AutoSupport activado por el usuario o activado por un evento no se puede enviar, el sistema StorageGRID lleva a cabo las siguientes acciones:

1. Muestra un mensaje de error si se conoce el error. Por ejemplo, si un usuario selecciona el protocolo SMTP sin proporcionar la configuración de correo electrónico correcta, se muestra el siguiente error: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. No intenta volver a enviar el mensaje.
3. Registra el error en `nms.log`.

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico está en ejecución (**SUPPORT** > **Alarmas (heredado)** > **> Configuración de correo electrónico heredado**). El siguiente mensaje de error puede aparecer en la página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Aprenda cómo "configure los ajustes del servidor de correo electrónico".

Corrija un error en un mensaje de AutoSupport

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico se está ejecutando. El siguiente mensaje de error puede aparecer en la página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envíe mensajes de AutoSupport de E-Series a través de StorageGRID

Puede enviar mensajes de AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administrador de StorageGRID en lugar de hacerlo con el puerto de gestión del dispositivo de almacenamiento.

Consulte "AutoSupport de hardware E-Series" Para obtener más información sobre el uso de AutoSupport con dispositivos E-Series.

Antes de empezar

- Se ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene los permisos de administrador de dispositivo de almacenamiento o acceso raíz.
- Ha configurado SANtricity AutoSupport:

- Para dispositivos SG6000 y SG5700, "Configure AutoSupport en SANtricity System Manager"

> 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.

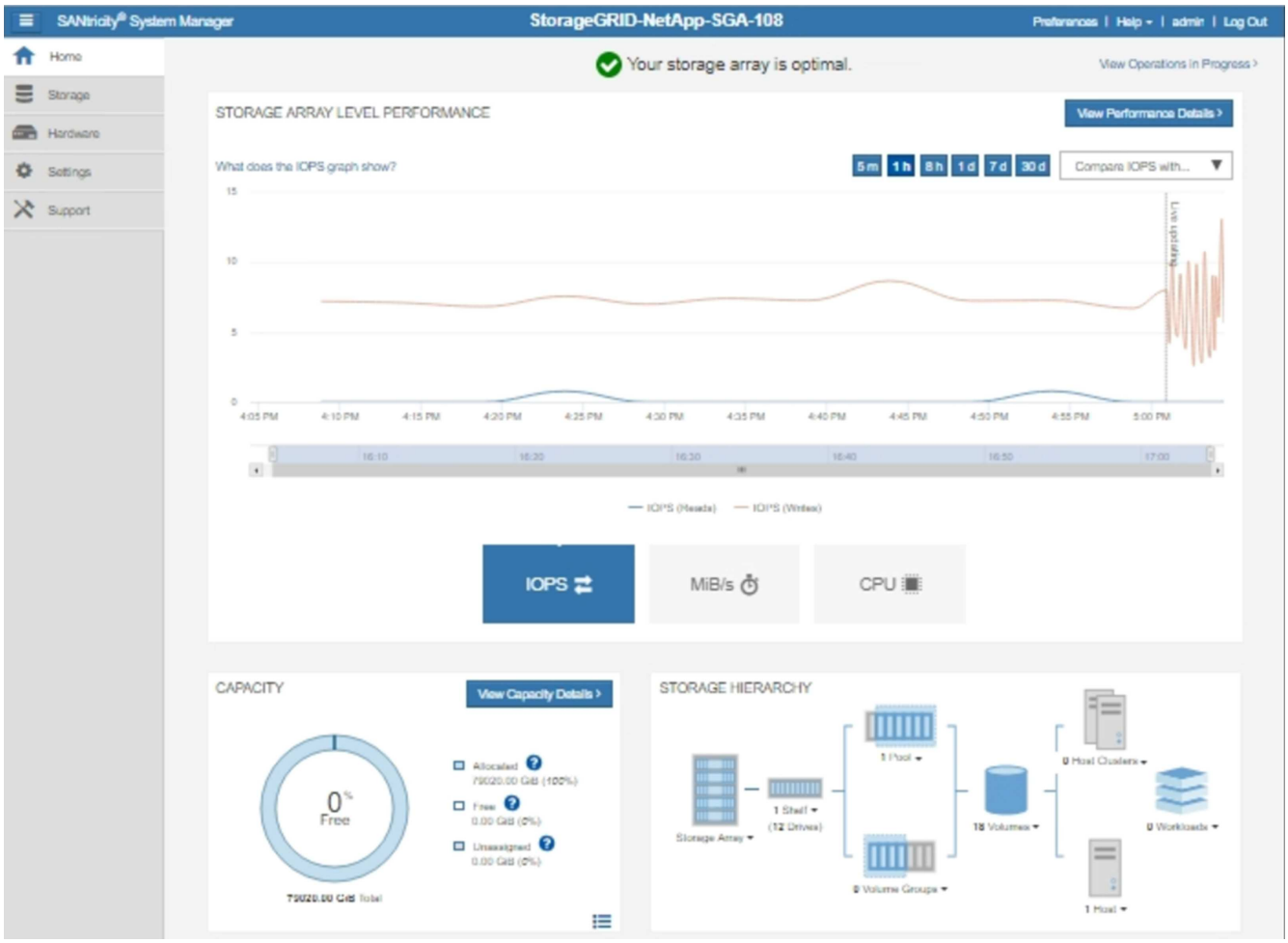
Es posible configurar una dirección de servidor proxy especial en SANtricity System Manager para transmitir mensajes de AutoSupport a través de un nodo de administración de StorageGRID sin el uso del puerto de gestión del dispositivo. Los mensajes de AutoSupport transmitidos de esta manera los envía el "Nodo de administración de remitente preferido", y usan cualquiera "Configuración de proxy de administración" Que se han configurado en Grid Manager.

> Este procedimiento solo se utiliza para configurar un servidor proxy StorageGRID para los mensajes de AutoSupport E-Series. Si quiere más información sobre la configuración de la serie AutoSupport de E-Series, consulte "Documentación de SANtricity y E-Series de NetApp".

Pasos

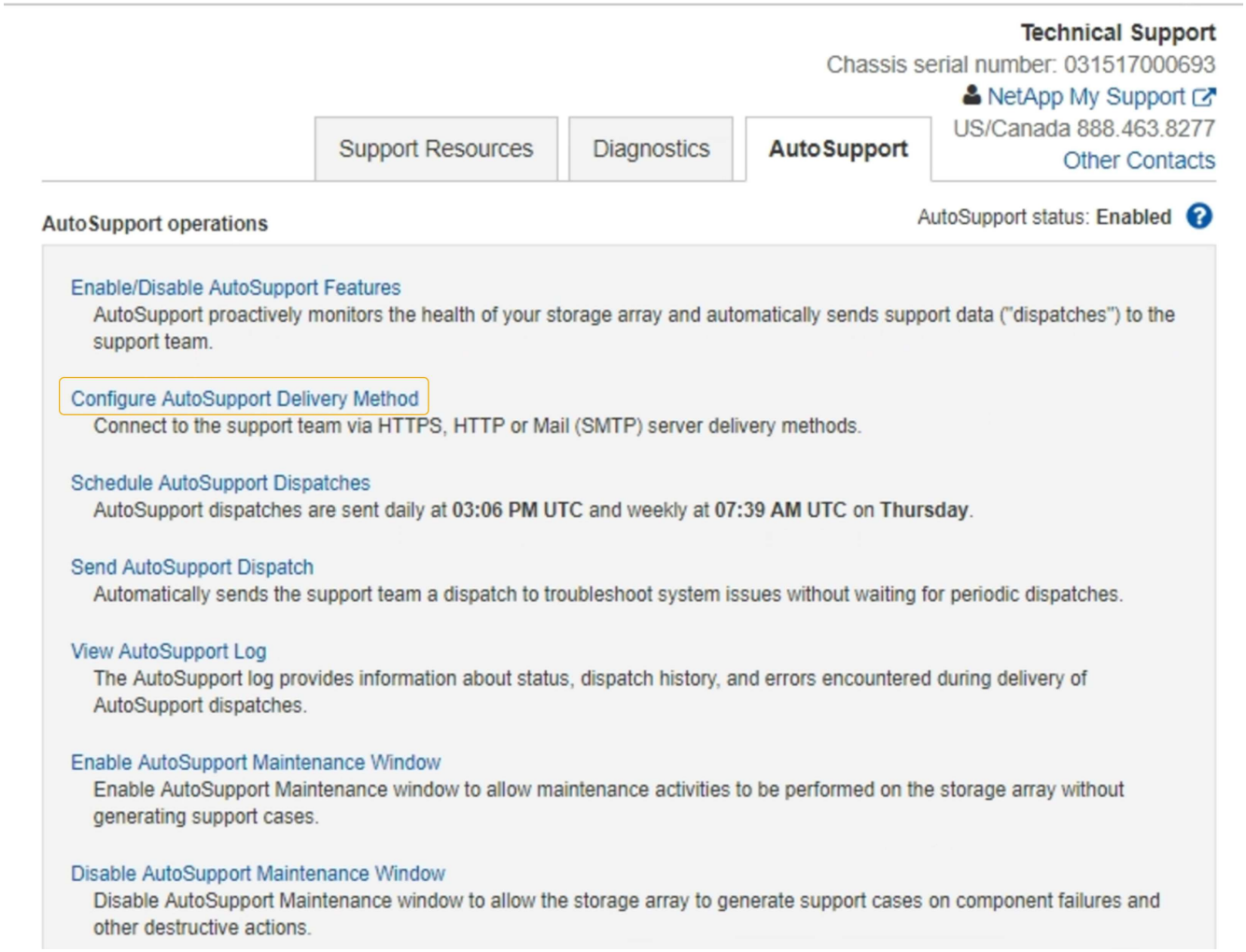
1. En Grid Manager, seleccione **NODES**.
2. En la lista de nodos que aparece a la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione **Administrador del sistema SANtricity**.

   Se mostrará la página de inicio de SANtricity System Manager.



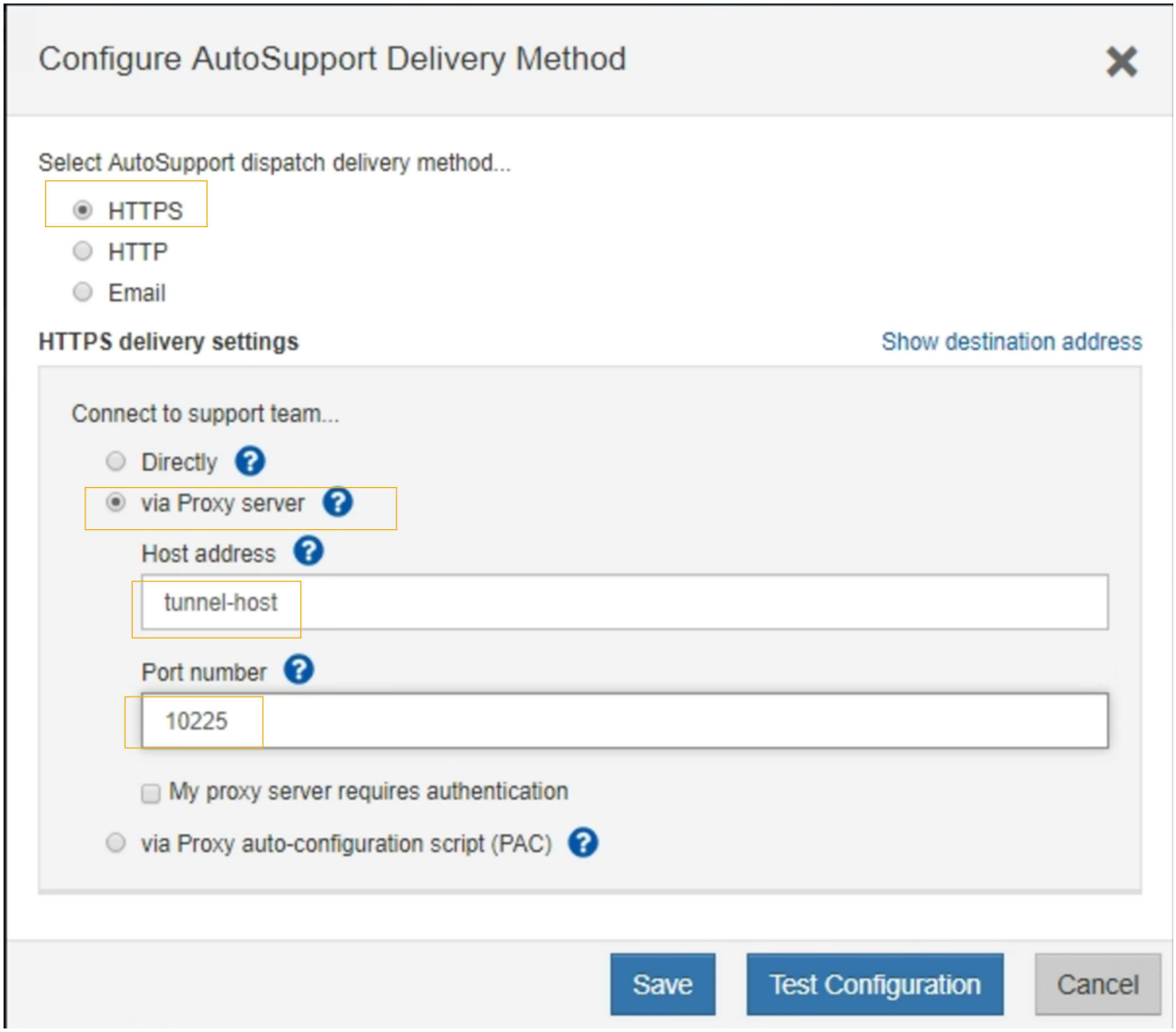
4. Seleccione **SUPPORT** > **Support Center** > **AutoSupport**.

   Se muestra la página de operaciones AutoSupport.



5. Seleccione **Configurar método de entrega de AutoSupport**.

   Se muestra la página Configurar método de entrega de AutoSupport.



6. Seleccione **HTTPS** para el método de entrega.

   El certificado que habilita 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 de StorageGRID y la red, asegúrese del "Nodo de administración de remitente preferido" Puede conectarse al sitio de soporte de NetApp y volver a intentar la prueba.

11. Seleccione **Guardar**.

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

Gestione nodos de almacenamiento

Gestionar nodos de almacenamiento: Información general

Los nodos de almacenamiento proporcionan servicios y capacidad de almacenamiento en disco. La gestión de nodos de almacenamiento conlleva lo siguiente:

- Gestión de las opciones de almacenamiento
- Comprender qué son las marcas de agua del volumen de almacenamiento y cómo se pueden utilizar anulaciones de Marca de agua para controlar cuando los nodos de almacenamiento pasan a ser de sólo lectura
- Supervisar y gestionar el espacio usado para los metadatos de objetos
- Configuración de la configuración global de los objetos almacenados
- Aplicar las opciones de configuración del nodo de almacenamiento
- Gestión de nodos de almacenamiento completos

¿Qué es un nodo de almacenamiento?

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Cada sistema StorageGRID debe tener al menos tres nodos de almacenamiento. Si tiene varios sitios, cada sitio dentro del sistema StorageGRID también debe tener tres nodos de almacenamiento.

Un nodo de almacenamiento incluye los servicios y procesos necesarios para almacenar, mover, verificar y recuperar metadatos y datos de objetos en el disco. Puede ver información detallada sobre los nodos de almacenamiento en la página **NODES**.

¿Qué es el servicio ADC?

El servicio de controlador de dominio administrativo (ADC) autentica los nodos de grid y sus conexiones entre sí. El servicio ADC está alojado en cada uno de los tres primeros nodos de almacenamiento de un sitio.

El servicio ADC mantiene la información de topología, incluida la ubicación y disponibilidad de los servicios. Cuando un nodo de cuadrícula requiere información de otro nodo de cuadrícula o una acción que debe realizar otro nodo de cuadrícula, se pone en contacto con un servicio de ADC para encontrar el mejor nodo de cuadrícula para procesar su solicitud. Además, el servicio ADC conserva una copia de los paquetes de configuración de la implementación StorageGRID, lo que permite que cualquier nodo de la cuadrícula recupere la información de configuración actual.puede ver la información de ADC de un nodo de almacenamiento en la página Topología de la cuadrícula (**SUPPORT** > **topología de la cuadrícula**).

Para facilitar las operaciones distribuidas e iaterradas, cada servicio ADC sincroniza certificados, paquetes de configuración e información sobre servicios y topología con los otros servicios ADC del sistema StorageGRID.

En general, todos los nodos de grid mantienen una conexión al menos a un servicio de ADC. De este modo se garantiza que los nodos grid accedan siempre a la información más reciente. Cuando los nodos de grid se conectan, almacenan en caché los certificados de otros nodos de grid, lo que permite a los sistemas seguir funcionando con nodos de grid conocidos incluso cuando un servicio de ADC no está disponible. Los nuevos nodos de grid solo pueden establecer conexiones mediante un servicio ADC.

La conexión de cada nodo de cuadrícula permite al servicio ADC recopilar información de topología. Esta información sobre los nodos de grid incluye la carga de CPU, el espacio en disco disponible (si tiene almacenamiento), los servicios admitidos y el ID de sitio del nodo de grid. Otros servicios solicitan al servicio ADC información de topología a través de consultas de topología. El servicio ADC responde a cada consulta con la información más reciente recibida del sistema StorageGRID.

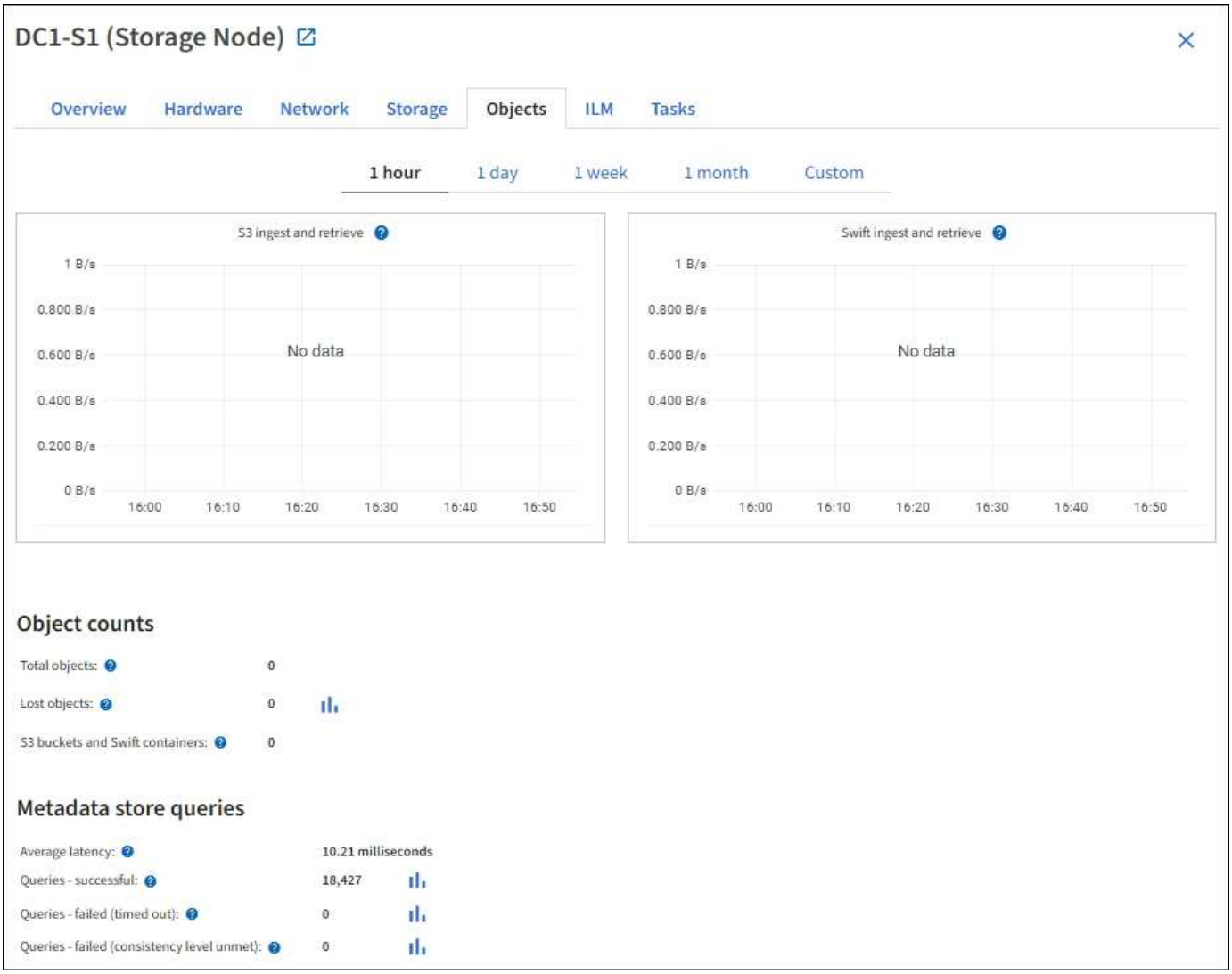
¿Qué es el servicio DDS?

Alojado por un nodo de almacenamiento, el servicio almacén de datos distribuidos (DDS) interactúa con la base de datos de Cassandra para realizar tareas en segundo plano en los metadatos de objeto almacenados en el sistema StorageGRID.

El número de objetos

El servicio DDS realiza un seguimiento del número total de objetos ingeridos en el sistema StorageGRID, así como del número total de objetos ingeridos a través de cada una de las interfaces compatibles del sistema (S3 o Swift).

Puede ver el número total de objetos en la página Nodes > la pestaña Objects de cualquier nodo de almacenamiento.



Consultas

Puede identificar el tiempo medio que tarda en ejecutar una consulta en el almacén de metadatos a través del servicio DDS específico, el número total de consultas correctas y el número total de consultas que han fallado debido a un problema de tiempo de espera.

Se recomienda revisar la información de consulta para supervisar el estado del almacén de metadatos, Cassandra, lo que afecta al rendimiento de procesamiento y recuperación del sistema. Por ejemplo, si la latencia de una consulta media es lenta y el número de consultas con errores debido a tiempos de espera es elevado, es posible que el almacén de metadatos encuentre una carga mayor o realice otra operación.

También puede ver el número total de consultas que han fallado debido a los fallos de consistencia. Los fallos de nivel de coherencia se deben a un número insuficiente de almacenes de metadatos disponibles en el momento en que se realiza una consulta a través del servicio DDS específico.

Puede utilizar la página Diagnóstico para obtener información adicional sobre el estado actual de la cuadrícula. Consulte "Ejecutar diagnóstico".

Garantías y controles de coherencia

StorageGRID garantiza la coherencia de lectura tras escritura para los objetos recién creados. Cualquier OPERACIÓN DE OBTENER después de una operación DE PUT completada correctamente podrá leer los

datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones siguen siendo coherentes en la actualidad.

¿Qué es el servicio LDR?

Alojado por cada nodo de almacenamiento, el servicio de router de distribución local (LDR) gestiona el transporte de contenido para el sistema StorageGRID. El transporte de contenido abarca numerosas tareas, como el almacenamiento de datos, el enrutamiento y la gestión de solicitudes. El servicio LDR hace la mayor parte del trabajo duro del sistema StorageGRID al manejar las cargas de transferencia de datos y las 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 Diagnóstico para obtener información adicional sobre el estado actual de la cuadrícula. Consulte "Ejecutar diagnóstico".

Actividad de ILM

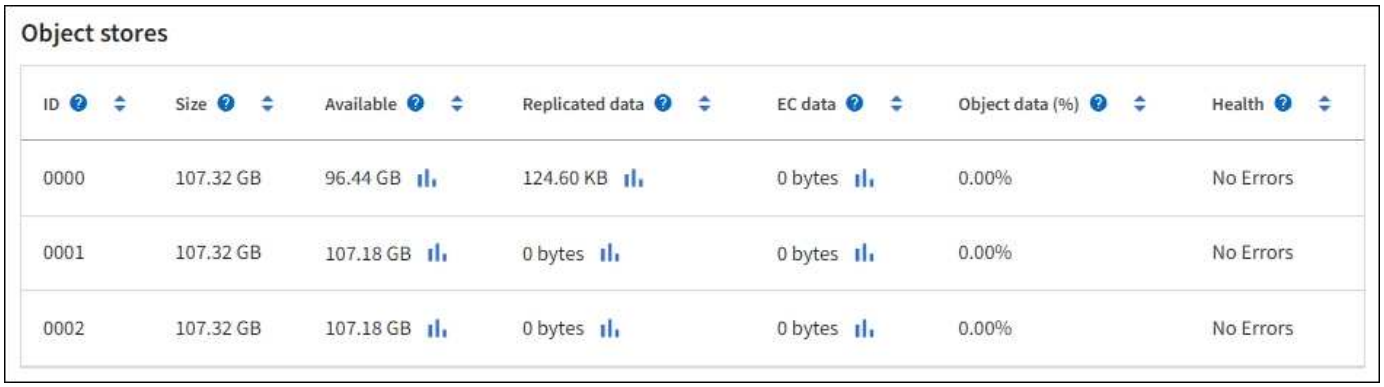
Las métricas de gestión de ciclo de vida de la información (ILM) permiten supervisar la velocidad a la que se evalúan los objetos para la implementación de ILM. Puede ver estas métricas en el panel de control o en **NODES** > ***Storage Node*** > **ILM**.

Almacenes de objetos

El almacenamiento de datos subyacente de un servicio LDR se divide en un número fijo de almacenes de objetos (también conocidos como volúmenes de almacenamiento). Cada almacén de objetos es un punto de

montaje independiente.

Puede ver los almacenes de objetos de un nodo de almacenamiento en la página nodos > pestaña Storage.



Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Los almacenes de objetos de un nodo de almacenamiento se identifican mediante un número hexadecimal entre 0000 y 002F, que se conoce como el ID del volumen. El espacio se reserva en el primer almacén de objetos (volumen 0) para los metadatos de objetos en una base de datos de Cassandra; todo el espacio restante en ese volumen se usa para los datos de objetos. El resto de almacenes de objetos se utilizan exclusivamente para datos de objetos, lo que incluye copias replicadas y fragmentos codificados para borrado.

Para garantizar hasta el uso de espacio para las copias replicadas, los datos de objetos para un objeto determinado se almacenan en un almacén de objetos en función del espacio de almacenamiento disponible. Cuando uno o varios almacenes de objetos se llenan de capacidad, los almacenes de objetos restantes siguen almacenando objetos hasta que no hay más espacio en el nodo de almacenamiento.

Protección de metadatos

Los metadatos de objetos son información relacionada con un objeto o una descripción de él; por ejemplo, el tiempo de modificación del objeto o la ubicación de almacenamiento. StorageGRID almacena metadatos de objetos en una base de datos de Cassandra, que se conecta con el servicio LDR.

Para garantizar la redundancia y, por lo tanto, la protección contra la pérdida, se mantienen tres copias de metadatos de objetos en cada sitio. Esta replicación no puede configurarse y se realiza de forma automática.

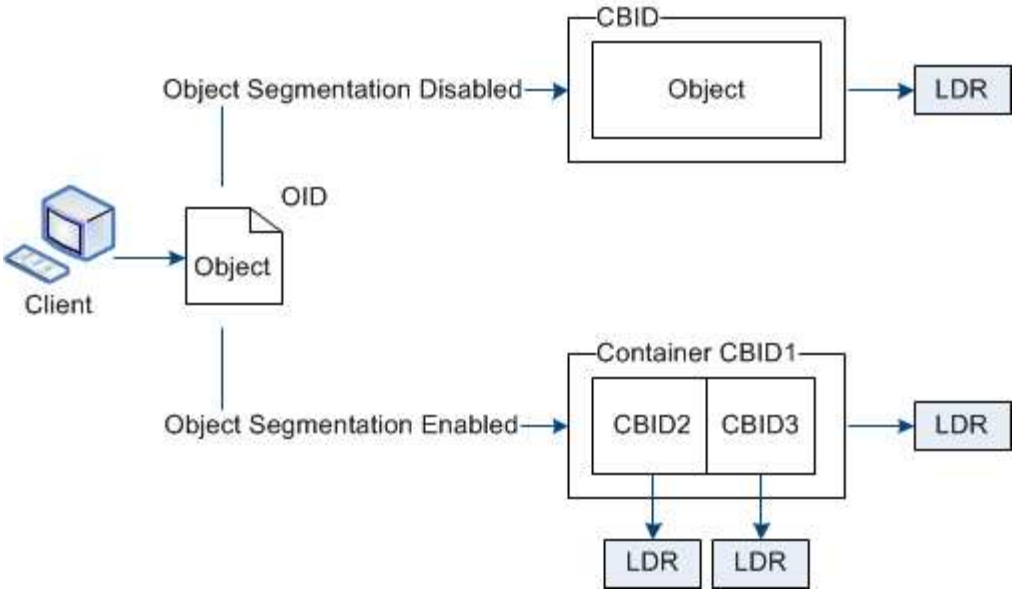
"Gestione el almacenamiento de metadatos de objetos"

Utilice las opciones de almacenamiento

¿Qué es la segmentación de objetos?

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos más pequeños de tamaño fijo para optimizar el uso de recursos y almacenamiento para objetos grandes. La carga de varias partes de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando un objeto se procesa en el sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que enumera la información de encabezado de todos los segmentos como contenido.



Al recuperar un contenedor de segmentos, el servicio LDR reúne el objeto original de sus segmentos y devuelve el objeto al cliente.

El contenedor y los segmentos no se almacenan necesariamente en el mismo nodo de almacenamiento. El contenedor y los segmentos pueden almacenarse en cualquier nodo de almacenamiento dentro del pool de almacenamiento especificado en la regla de ILM.

El sistema StorageGRID trata cada segmento de forma independiente y contribuye al recuento de atributos como objetos gestionados y objetos almacenados. Por ejemplo, si un objeto almacenado en el sistema StorageGRID se divide en dos segmentos, el valor de objetos gestionados aumenta en tres una vez completada la ingesta, de la siguiente manera:

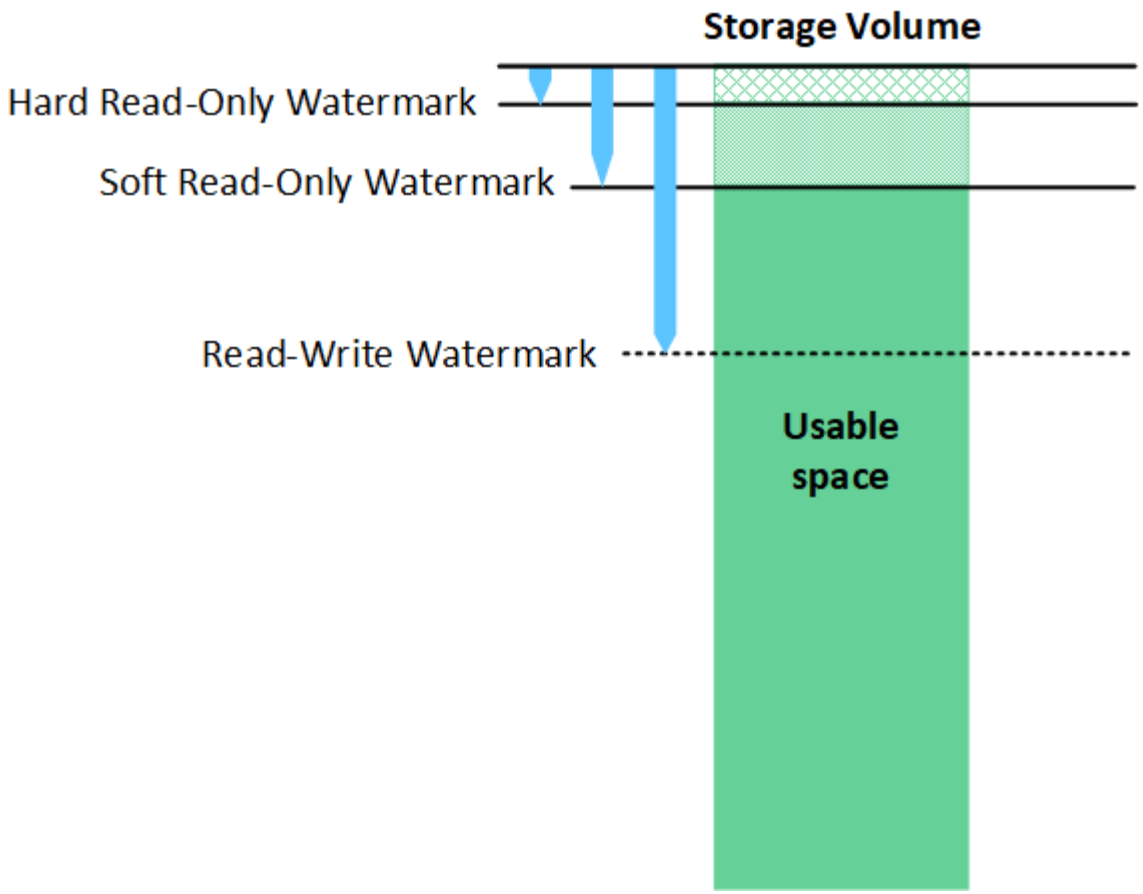
```
segment container + segment 1 + segment 2 = three stored objects
```

Puede mejorar el rendimiento al manejar objetos grandes asegurándose de que:

- Cada puerta de enlace y cada nodo de almacenamiento tiene suficiente ancho de banda de red para el rendimiento requerido. Por ejemplo, configure redes de cliente y de cuadrícula independientes en interfaces Ethernet de 10 Gbps.
- Se ponen en marcha suficientes nodos de pasarela y almacenamiento para el rendimiento requerido.
- Cada nodo de almacenamiento tiene suficiente rendimiento de I/O de disco para el rendimiento requerido.

¿Qué son las marcas de agua del volumen de almacenamiento?

StorageGRID usa tres marcas de agua de volúmenes de almacenamiento para garantizar que los nodos de almacenamiento pasan de forma segura a un estado de solo lectura antes de que se ejecuten con un espacio mínimo y para permitir que los nodos de almacenamiento que se hayan migrado al estado de solo lectura se vuelvan a escribir.



Las marcas de agua del volumen de almacenamiento solo se aplican al espacio utilizado para los datos de objetos replicados y codificados por borrado. Para obtener más información acerca del espacio reservado para los metadatos de objetos en el volumen 0, vaya a."Gestione el almacenamiento de metadatos de objetos".

¿Qué es la Marca de agua blanda de sólo lectura?

Marca de agua de sólo lectura suave del volumen de almacenamiento es la primera Marca de agua que indica que el espacio utilizable de un nodo de almacenamiento para los datos del objeto se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que la Marca de agua de solo lectura suave de ese volumen, el nodo de almacenamiento pasará al *modo de solo lectura*. El modo de solo lectura significa que el nodo de almacenamiento anuncia servicios de solo lectura al resto del sistema StorageGRID, pero completa todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una Marca de agua blanda de solo lectura de 10 GB. En cuanto cada volumen tiene menos de 10 GB de espacio libre, el nodo de almacenamiento pasa al modo de solo lectura suave.

¿Qué es la Marca de agua dura de sólo lectura?

- Marca de agua de sólo lectura dura de volumen de almacenamiento* es la siguiente Marca de agua para indicar que el espacio utilizable de un nodo para los datos de objeto se está llenando.

Si el espacio libre en un volumen es menor que la Marca de agua de sólo lectura de ese volumen, las escrituras en el volumen fallarán. Sin embargo, las escrituras en otros volúmenes pueden continuar hasta que el espacio libre en esos volúmenes sea menor que sus marcas de agua de sólo lectura.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una Marca de agua de solo lectura rígida de 5 GB. En cuanto cada volumen tenga menos de 5 GB de espacio libre, el nodo de almacenamiento ya no aceptará ninguna solicitud de escritura.

La Marca de agua dura de sólo lectura es siempre inferior a la Marca de agua blanda de sólo lectura.

¿Qué es la Marca de agua de lectura y escritura?

Marca de agua de lectura y escritura de volumen de almacenamiento sólo se aplica a los nodos de almacenamiento que hayan pasado al modo de sólo lectura. Determina cuándo el nodo puede volver a ser de lectura y escritura. Cuando el espacio libre de un volumen de almacenamiento en un nodo de almacenamiento es mayor que la Marca de agua de lectura y escritura de ese volumen, el nodo cambia automáticamente al estado de lectura y escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Supongamos también que cada volumen tiene una Marca de agua de lectura y escritura de 30 GB. En cuanto el espacio libre de cualquier volumen aumente a 30 GB, el nodo volverá a ser de lectura y escritura.

La Marca de agua de lectura y escritura es siempre mayor que la Marca de agua de sólo lectura suave y la Marca de agua de sólo lectura dura.

Ver marcas de agua de volumen de almacenamiento

Puede ver los ajustes de Marca de agua actuales y los valores optimizados para el sistema. Si no se utilizan marcas de agua optimizadas, puede determinar si puede o debe ajustar la configuración.

Antes de empezar

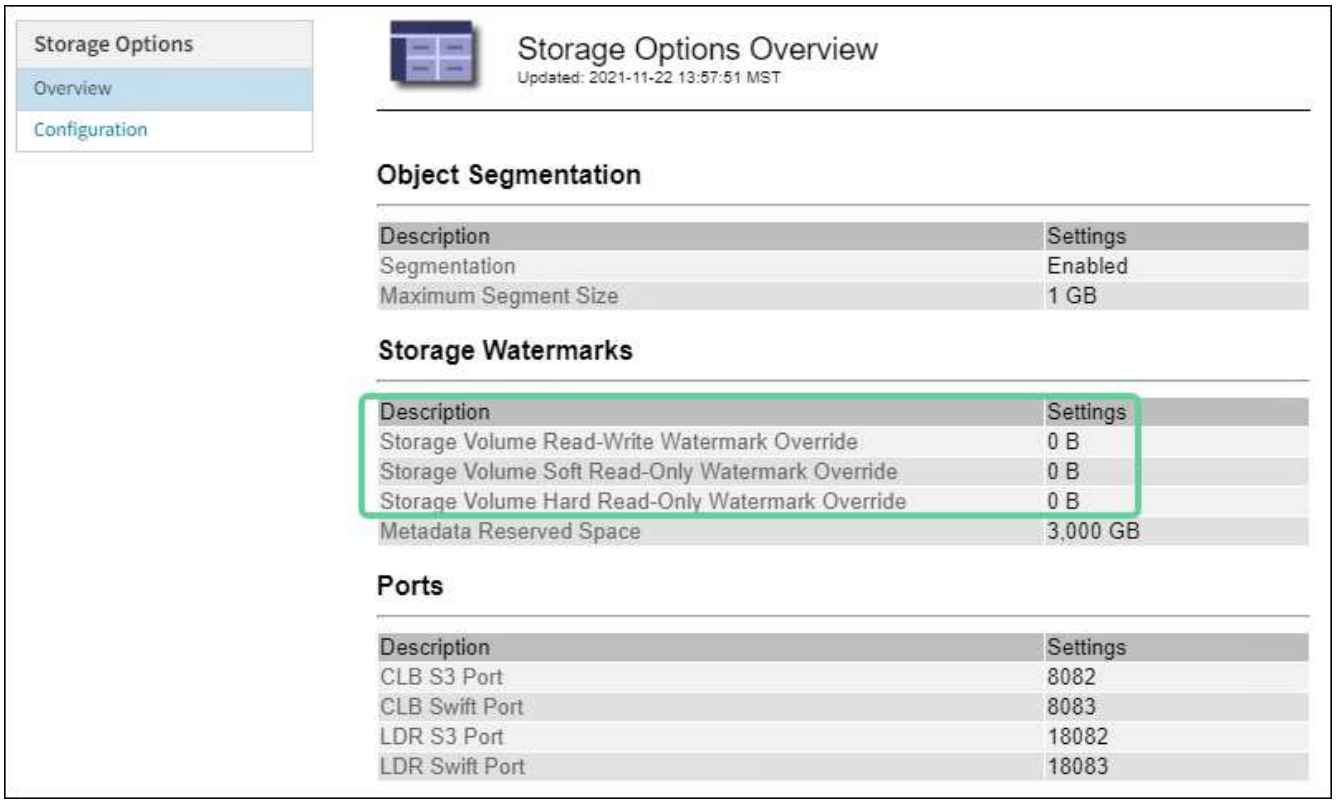
- Ha completado la actualización a StorageGRID 11,6 o superior.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.

Ver la configuración actual de la Marca de agua

Puede ver la configuración actual de la Marca de agua de almacenamiento en el Administrador de grid.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. En la sección Marcas de agua de almacenamiento, observe los ajustes para las tres anulaciones de la Marca de agua de volumen de almacenamiento.



- Si las anulaciones de la Marca de agua son **0**, las tres marcas de agua están optimizadas para cada volumen de almacenamiento en cada nodo de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

  Esta es la configuración predeterminada y recomendada. No debe actualizar estos valores. Según sea necesario, puede opcionalmente Vea las marcas de agua de almacenamiento optimizadas.

- Si las anulaciones de la Marca de agua son valores distintos de 0, se utilizan marcas de agua personalizadas (no optimizadas). No se recomienda utilizar la configuración de Marca de agua personalizada. Utilice las instrucciones para "Solución de problemas de alertas de anulación de Marca de agua de sólo lectura baja" para determinar si puede o debe ajustar la configuración.

Vea las marcas de agua de almacenamiento optimizadas

StorageGRID utiliza dos métricas Prometheus para mostrar los valores optimizados que ha calculado para la Marca de agua * de sólo lectura suave de volumen de almacenamiento*. Puede ver los valores mínimos y máximos optimizados para cada nodo de almacenamiento en la cuadrícula.

1. Seleccione **SUPPORT** > **Tools** > **Metrics**.
2. En la sección Prometheus, seleccione el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor optimizado mínimo de la Marca de agua de solo lectura suave para todos los volúmenes de almacenamiento de cada nodo de almacenamiento. Si este valor es mayor que el valor personalizado para **Marca de agua blanda de sólo lectura de volumen de almacenamiento**, se activa la alerta **anulación de Marca de agua de sólo lectura baja** para el nodo de almacenamiento.

4. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor optimizado máximo de la Marca de agua de solo lectura suave para todos los volúmenes de almacenamiento de cada nodo de almacenamiento.

Gestione el almacenamiento de metadatos de objetos

La capacidad de metadatos de objetos de un sistema StorageGRID controla la cantidad máxima de objetos que se pueden almacenar en ese sistema. Para garantizar que el sistema StorageGRID tenga espacio suficiente para almacenar objetos nuevos, debe comprender dónde y cómo StorageGRID almacena los metadatos de objetos.

¿Qué son los metadatos de objetos?

Los metadatos de objetos son cualquier información que describa un objeto. StorageGRID utiliza metadatos de objetos para realizar un seguimiento de las ubicaciones de todos los objetos en el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

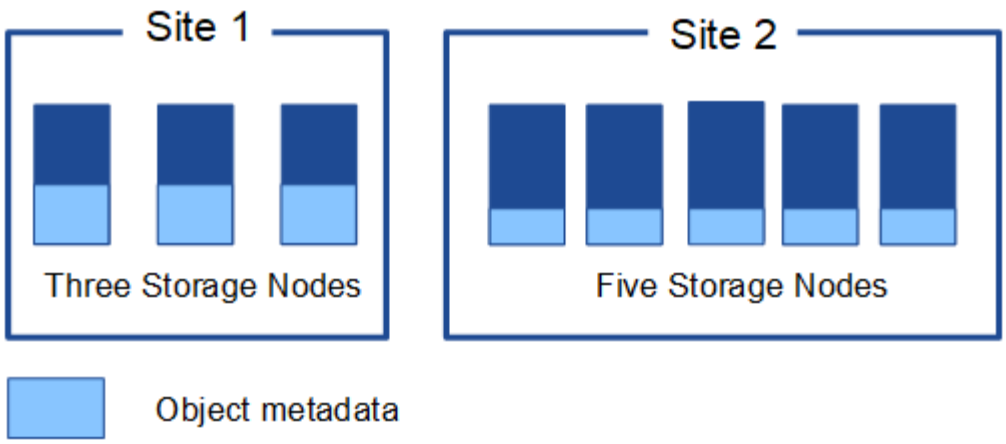
Para un objeto en StorageGRID, los metadatos de objeto incluyen los siguientes tipos de información:

- Metadatos del sistema, incluidos un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bloque de S3 o el contenedor Swift, el nombre o el ID de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y hora en que se modificó por última vez el objeto.
- Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
- Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
- Para objetos segmentados y objetos multipartes, identificadores de segmentos y tamaños de datos.

¿Cómo se almacenan los metadatos de objetos?

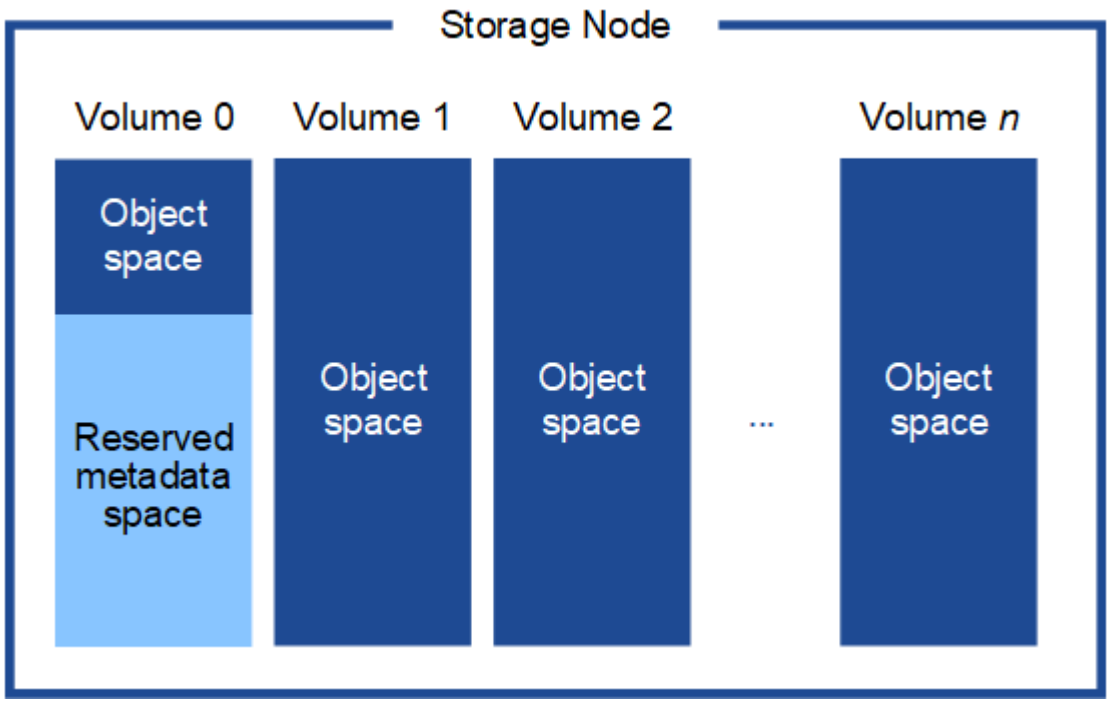
StorageGRID mantiene los metadatos de objetos en una base de datos de Cassandra, que se almacena independientemente de los datos de objetos. Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio.

Esta figura representa los nodos de almacenamiento de dos sitios. Cada sitio tiene la misma cantidad de metadatos de objeto y los metadatos de cada sitio se subdividen entre todos 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 reservado para los metadatos de objeto en un nodo de almacenamiento en particular 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. Como se muestra en la tabla, el valor predeterminado de esta configuración se basa en:

- La versión de software que estaba utilizando cuando instaló inicialmente StorageGRID.
- La cantidad de RAM en cada nodo de almacenamiento.

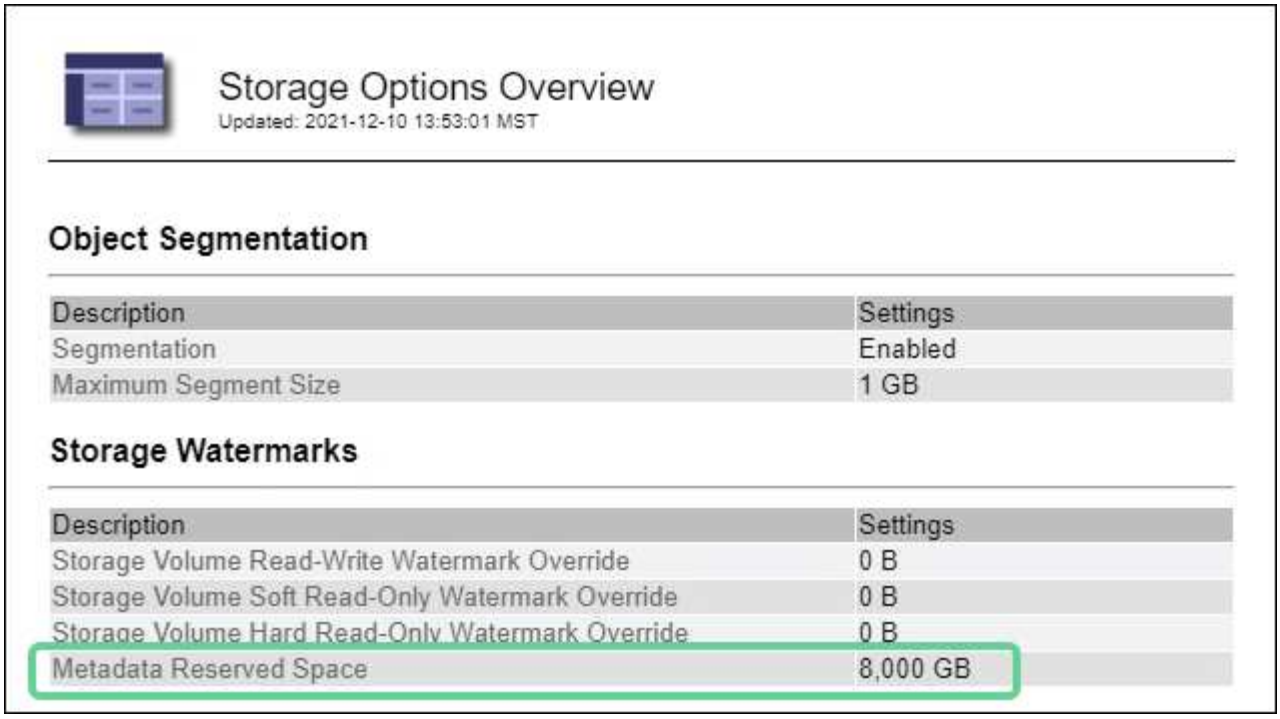
Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Valor de Espacio Reservado de Metadatos por Defecto
11,5 a 11,7	128 GB o más en cada nodo de almacenamiento del grid	8 TB (8,000 GB)
	Debe haber menos de 128 GB en cualquier nodo de almacenamiento del grid	3 TB (3,000 GB)
11.1 a 11.4	128 GB o más en cada nodo de almacenamiento en un sitio	4 TB (4,000 GB)
	Menos de 128 GB en cualquier nodo de almacenamiento de cada sitio	3 TB (3,000 GB)
11.0 o anterior	Cualquier cantidad	2 TB (2,000 GB)

Configuración de Ver Espacio Reservado de Metadatos

Siga estos pasos para ver la configuración de Espacio reservado de metadatos para el sistema StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. En la tabla Marcas de agua de almacenamiento, busque **espacio reservado de metadatos**.



En la captura de pantalla, el valor **espacio reservado de metadatos** es 8,000 GB (8 TB). Este es el valor predeterminado para una nueva instalación de StorageGRID 11,6 o superior 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

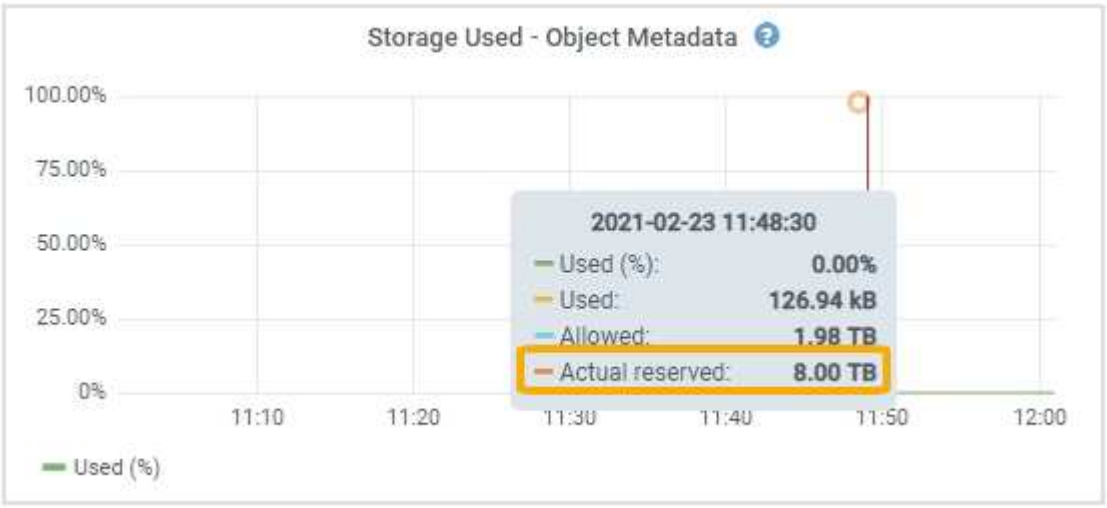
Ver el espacio reservado real para metadatos

Siga estos pasos para ver el espacio reservado real para metadatos en un nodo de almacenamiento en particular.

Pasos

1. En Grid Manager, seleccione **NODES** > ***Storage Node***.
2. Seleccione la ficha **almacenamiento**.

3. Coloque el cursor sobre el gráfico Almacenamiento usado - Metadatos de objetos y localice el valor **Real reserved**.



En la captura de pantalla, el valor **Real reservado** es 8 TB. Esta captura de pantalla es para un nodo de almacenamiento grande en una nueva instalación de StorageGRID 11.6. Debido a que la configuración de espacio reservado de metadatos para todo el sistema es menor que el volumen 0 para este nodo de almacenamiento, el espacio reservado real para este nodo es igual a la configuración de espacio reservado de metadatos.

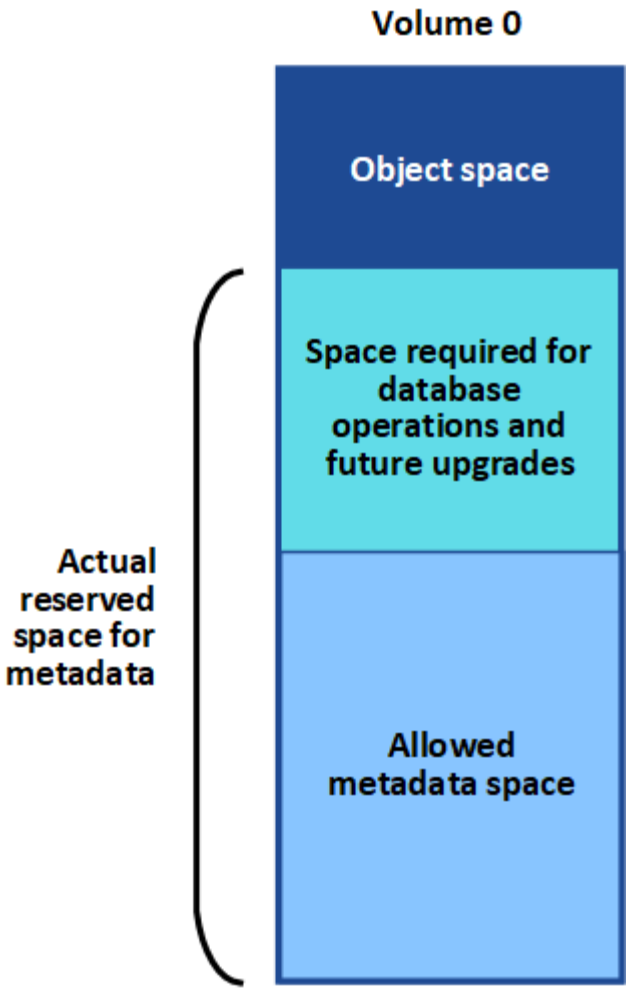
Ejemplo de espacio de metadatos reservado real

Supongamos que instala un nuevo sistema StorageGRID con la versión 11,7. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado de metadatos* para todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11,6 o superior si cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (El volumen completo se reserva porque el volumen 0 es menor que la configuración **espacio reservado de metadatos**).

Espacio de metadatos permitido

El espacio reservado real de cada nodo de almacenamiento para metadatos se subdivide en el espacio disponible para los metadatos del objeto (el *espacio de metadatos permitido*) y el espacio necesario para las operaciones esenciales de la base de datos (como compactación y reparación) y las futuras actualizaciones de hardware y software. El espacio de metadatos permitido rige la capacidad general del objeto.



En la tabla siguiente se muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes nodos de almacenamiento, en función de la cantidad de memoria del nodo y del espacio reservado real para los metadatos.

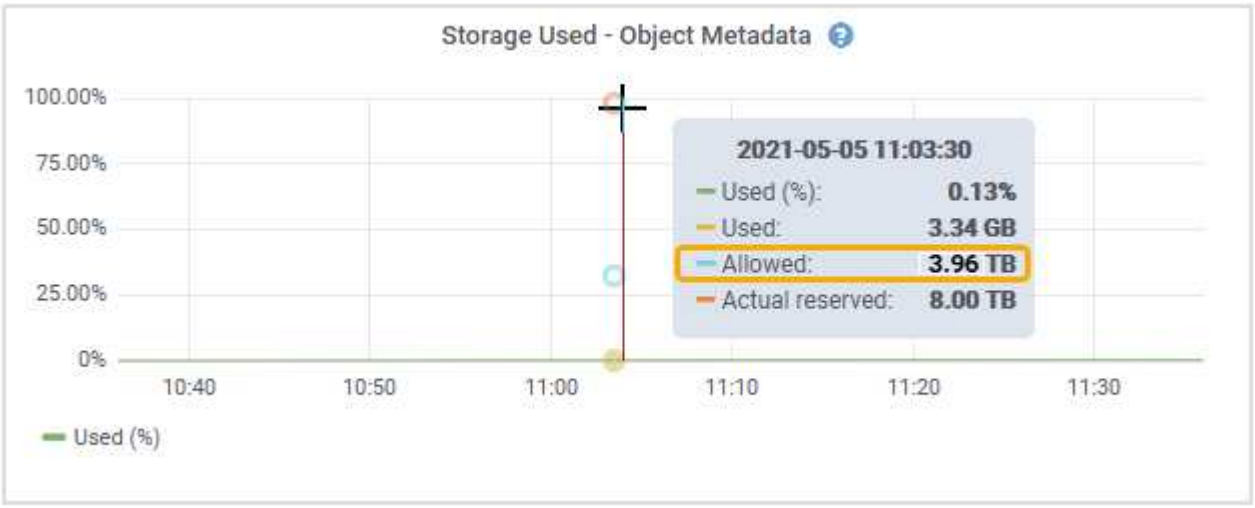
		Cantidad de memoria en el nodo de almacenamiento	
	≪ 128 GB	>= 128 GB	**Espacio reservado real para metadatos**
≪= 4 TB	60 % del espacio reservado real para metadatos, hasta un máximo de 1.32 TB	60 % del espacio reservado real para metadatos, hasta un máximo de 1.98 TB	> 4 TB

Ver el espacio de metadatos permitido

Siga estos pasos para ver el espacio de metadatos permitido para un nodo de almacenamiento.

Pasos

1. En Grid Manager, seleccione **NODES**.
2. Seleccione el nodo de almacenamiento.
3. Seleccione la ficha **almacenamiento**.
4. Coloque el cursor sobre el gráfico de metadatos de objetos Storage Used y localice el valor **Allowed**.



En la captura de pantalla, el valor **permitido** es 3.96 TB, que es el valor máximo para un nodo de almacenamiento cuyo espacio reservado real para metadatos es superior a 4 TB.

El valor **permitido** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Ejemplo de espacio de metadatos permitido

Supongamos que instala un sistema StorageGRID mediante la versión 11.6. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado de metadatos* para todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para StorageGRID 11,6 o superior cuando cada nodo de almacenamiento tiene más de 128 GB de RAM.)
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (El volumen completo se reserva porque el volumen 0 es menor que la configuración **espacio reservado de metadatos**).
- El espacio permitido para los metadatos en SN1 es de 3 TB, según el cálculo mostrado en la tabla para el espacio permitido para los metadatos: (Espacio reservado real para metadatos − 1 TB) × 60%, hasta un máximo de 3.96 TB.

Cómo afectan los nodos de almacenamiento de diferentes tamaños a la capacidad de objetos

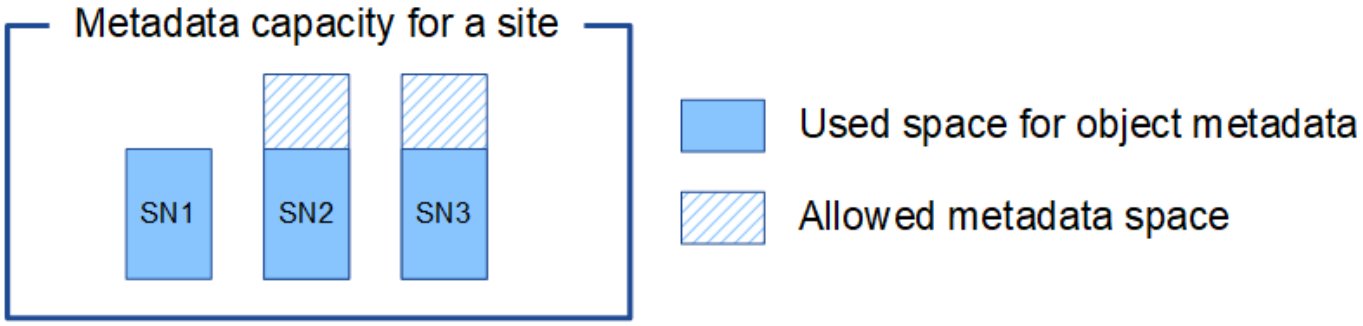
Como se ha descrito anteriormente, StorageGRID distribuye uniformemente los metadatos de objetos de los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

Observe el siguiente ejemplo:

- Hay una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de distintos tamaños.
- El ajuste **espacio reservado de metadatos** es de 4 TB.
- Los nodos de almacenamiento tienen los siguientes valores para el espacio de metadatos reservado real y el espacio de metadatos permitido.

Nodo de almacenamiento	Tamaño del volumen 0	Espacio real de metadatos reservado	Espacio de metadatos permitido
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Como los metadatos de objetos se distribuyen uniformemente por los nodos de almacenamiento de un sitio, cada nodo de este ejemplo solo puede contener 1.32 TB de metadatos. No se pueden utilizar los 0,66 TB adicionales de espacio permitido 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 obtener más información sobre cómo supervisar la capacidad de metadatos del objeto para cada nodo de almacenamiento, consulte las instrucciones para "Supervisión de StorageGRID".
- Para aumentar la capacidad de metadatos de objetos del sistema, "amplíe su grid" Añadiendo nuevos nodos de almacenamiento.

Aumentar la configuración del espacio reservado de metadatos

Es posible que pueda aumentar la configuración del sistema de espacio reservado de metadatos si sus nodos de almacenamiento cumplen requisitos específicos de RAM y espacio disponible.

Lo que necesitarás

- Has iniciado sesión en el Administrador de la red mediante un "navegador web compatible".

- Tienes el "Permiso de acceso raíz o la configuración de la página de topología de la red y otros permisos de configuración de la red".

Acerca de esta tarea

Es posible que pueda aumentar manualmente la configuración del Espacio reservado de metadatos de todo el sistema hasta 8 TB.

Solo puede aumentar el valor de la configuración de Espacio reservado de metadatos de todo el sistema si ambas afirmaciones son verdaderas:

- Los nodos de almacenamiento en cualquier sitio de su sistema tienen cada uno 128 GB o más de RAM.
- Cada uno de los nodos de almacenamiento de cualquier sitio de su sistema tiene suficiente espacio disponible en el volumen de almacenamiento 0.

Tenga en cuenta que si aumenta esta configuración, reducirá simultáneamente el espacio disponible para el almacenamiento de objetos en el volumen de almacenamiento 0 de todos los nodos de almacenamiento. Por este motivo, es posible que prefieras establecer el Espacio reservado de metadatos en un valor menor a 8 TB, en función de los requisitos de metadatos de tu objeto esperados.

> En general, es mejor utilizar un valor más alto en lugar de un valor más bajo. Si la configuración de Espacio reservado de metadatos es demasiado grande, puede reducirla más tarde. Por el contrario, si aumenta el valor más adelante, es posible que el sistema necesite mover datos del objeto para liberar espacio.

Para obtener una explicación detallada de cómo la configuración de Espacio reservado para metadatos afecta al espacio permitido para el almacenamiento de metadatos de objetos en un nodo de almacenamiento específico, consulte "Gestione el almacenamiento de metadatos de objetos".

Pasos

1. Determinar la configuración actual del espacio reservado de metadatos.
   a. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
   b. En la sección Marcas de agua de almacenamiento, tenga en cuenta el valor de **Espacio reservado para metadatos**.
2. Asegúrese de tener suficiente espacio disponible en el volumen de almacenamiento 0 de cada nodo de almacenamiento para aumentar este valor.
   a. Seleccione **NODES**.
   b. Seleccione el primer nodo de almacenamiento en la cuadrícula.
   c. Seleccione la pestaña Almacenamiento.
   d. En la sección Volúmenes, busque la entrada **/var/local/rangedb/0**.
   e. Confirme que el valor Disponible sea igual o mayor que la diferencia entre el nuevo valor que desea utilizar y el valor actual del Espacio reservado de metadatos.

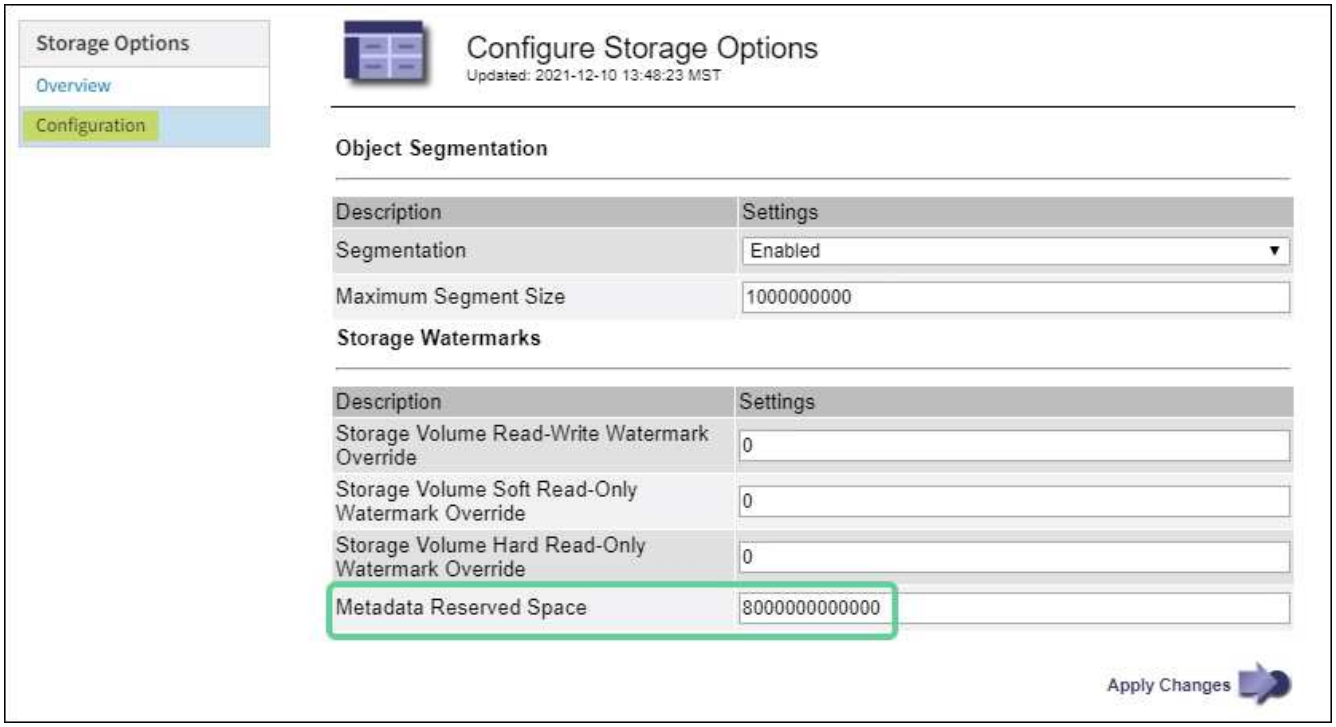
      Por ejemplo, si la configuración actual del Espacio reservado de metadatos es 4 TB y desea aumentarla a 6 TB, el valor Disponible debe ser 2 TB o más.

   f. Repita estos pasos para todos los nodos de almacenamiento.
      - Si uno o más nodos de almacenamiento no tienen suficiente espacio disponible, no se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.

- Si cada nodo de almacenamiento tiene suficiente espacio disponible en el volumen 0, vaya al siguiente paso.

3. Asegúrese de tener al menos 128 GB de RAM en cada nodo de almacenamiento.
   a. Seleccione **NODES**.
   b. Seleccione el primer nodo de almacenamiento en la cuadrícula.
   c. Seleccione la ficha **hardware**.
   d. Coloque el cursor sobre el gráfico de uso de memoria. Asegúrese de que la **Memoria total** sea de al menos 128 GB.
   e. Repita estos pasos para todos los nodos de almacenamiento.
      - Si uno o más nodos de almacenamiento no tienen suficiente memoria total disponible, no se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
      - Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, vaya al siguiente paso.
4. Actualice la configuración del espacio reservado de metadatos.
   a. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
   b. Seleccione la pestaña Configuración.
   c. En la sección Marcas de agua de almacenamiento, seleccione **Espacio reservado para metadatos**.
   d. Introduzca el nuevo valor.

      Por ejemplo, para ingresar 8 TB, que es el valor máximo admitido, ingrese **8000000000000** (8, seguido de 12 ceros)



   a. Seleccione **aplicar cambios**.

Comprimir objetos almacenados

Es posible habilitar la compresión de objetos para reducir el tamaño de los objetos

almacenados en StorageGRID, de modo que los objetos consuman menos almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

De forma predeterminada, la compresión de objetos está deshabilitada. Si habilita la compresión, StorageGRID intenta comprimir cada objeto al guardarlo, utilizando la 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 la compresión de objetos, tenga en cuenta lo siguiente:

- No debe seleccionar **Comprimir objetos almacenados** 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, al seleccionar esta opción no se reducirá aún más el tamaño de un objeto.
- No seleccione **Comprimir objetos almacenados** si utiliza NetApp FabricPool con StorageGRID.
- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente S3 y Swift deben evitar realizar operaciones GET Object que especifiquen un rango de bytes. 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. Selecciona **CONFIGURACIÓN** > **Sistema** > **Compresión de objetos**.
2. Seleccione la casilla de verificación **Comprimir objetos almacenados**.
3. Seleccione **Guardar**.

Opciones de configuración del nodo de almacenamiento

Cada nodo de almacenamiento utiliza varias 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.

Siga estos pasos para acceder a la configuración y los contadores de un nodo de almacenamiento.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node***.
3. Expanda el nodo de almacenamiento y seleccione el servicio o el componente.
4. Seleccione la ficha **Configuración**.

Las siguientes tablas resumen los ajustes de configuración de nodos de almacenamiento.

LDR

Nombre de atributo	Codificación	Descripción
Estado HTTP	HSTE	El estado actual de HTTP para S3, Swift y otro tráfico StorageGRID interno: • 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 comprobación de la existencia del objeto. El sistema StorageGRID restaura automáticamente los datos de objetos replicados que faltan.
Tasa de verificación	VPRI	Establecer la velocidad a la que se realiza la verificación en segundo plano. Consulte la información sobre la configuración de 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).
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.
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.

Nombre de atributo	Codificación	Descripción
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 comprobación de la existencia del objeto.

LDR > replicación

Nombre de atributo	Codificación	Descripción
Restablecer recuento de fallos de replicación entrante	RICR	Restablezca el contador de fallos de replicación de entrada. Esto se puede utilizar para borrar la alarma RIRF (replicación entrante — fallida).
Restablecer recuento de fallos de replicación de salida	RCR	Restablezca el contador para fallos de replicación saliente. Esto se puede utilizar para borrar la alarma RORF (réplicas de salida — fallida).
Desactivar la replicación entrante	DSIR	Seleccione esta opción para desactivar la replicación entrante como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal. Cuando la replicación entrante está desactivada, los objetos se pueden recuperar del nodo de almacenamiento para copiarlos 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 solo 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 desactivada, los objetos se pueden copiar en este nodo de almacenamiento, pero los objetos no se pueden recuperar del nodo de almacenamiento para copiarlos en otras ubicaciones del sistema StorageGRID. El servicio LDR es de sólo escritura.

Gestione nodos de almacenamiento completos

A medida que los nodos de almacenamiento alcancen la capacidad, debe ampliar el sistema StorageGRID añadiendo almacenamiento nuevo. Hay tres opciones disponibles: Añadir volúmenes de almacenamiento, añadir bandejas de ampliación de almacenamiento y añadir nodos de almacenamiento.

Añadir volúmenes de almacenamiento

Cada nodo de almacenamiento es compatible con un número máximo de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento contiene menos de la cantidad máxima de volúmenes de almacenamiento, es posible añadir volúmenes para aumentar su capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Añada bandejas de ampliación del almacenamiento

Algunos nodos de almacenamiento de dispositivos StorageGRID, como el SG6060, pueden admitir bandejas de almacenamiento adicionales. Si tiene dispositivos StorageGRID con funcionalidades de expansión que todavía no se han expandido hasta la máxima capacidad, se pueden añadir bandejas de almacenamiento para aumentar la capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Añada nodos de almacenamiento

Puede aumentar la capacidad de almacenamiento con la adición de nodos de almacenamiento. Al añadir almacenamiento, deben tenerse en cuenta las reglas de ILM activas y los requisitos de capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Gestione los nodos de administrador

¿Qué es un nodo de administración?

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.

¿Cuál es el remitente preferido

Si la implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para las notificaciones de alertas, los mensajes de AutoSupport, las capturas e informes SNMP y las notificaciones de alarmas heredadas.

En operaciones normales del sistema, solo el remitente preferido envía notificaciones. Sin embargo, el resto de los nodos de administración supervisan el remitente preferido. Si se detecta un problema, otros nodos de administración actúan como *remitentes en espera*.

Es posible que se envíen varias notificaciones en los siguientes casos:

- Si los nodos de administración pasan a ser “indistribuidos” entre sí, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones, y es posible que se reciban varias copias de las notificaciones.
- Si el remitente en espera detecta problemas con el remitente preferido y comienza a enviar notificaciones, es posible que el remitente preferido recupere su capacidad para 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 los mensajes de AutoSupport, todos los nodos de 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.

Servicios primarios para nodos de administración

En la siguiente tabla se muestran los servicios principales de los nodos de administrador; sin embargo, esta tabla no enumera todos los servicios de nodo.

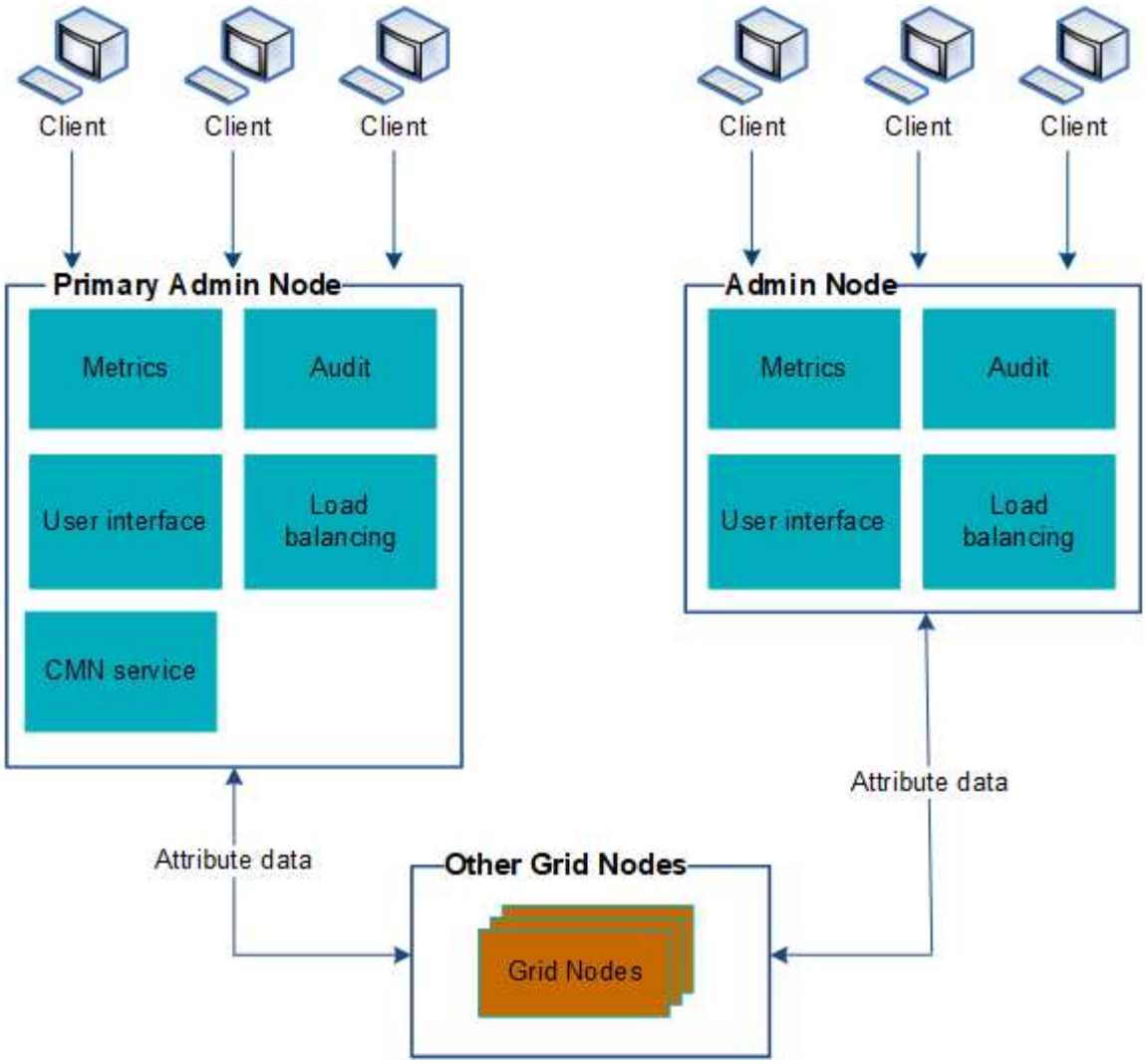
Servicio	Función de la tecla
Sistema de gestión de auditorías (AMS)	Realiza un seguimiento de la actividad y los eventos del sistema.
Nodo de gestión de configuraciones (CMN)	Gestiona la configuración en todo el sistema. Solo nodo de administrador principal.
Interfaz de programas de aplicaciones de gestión (API de gestión)	Procesa las solicitudes de la API de gestión de grid y la API de gestión de inquilinos.
Alta disponibilidad	Administra direcciones IP virtuales de alta disponibilidad para grupos de nodos de administración y nodos de puerta de enlace. **Nota:** este servicio también se encuentra en los nodos Gateway.

Servicio	Función de la tecla
Equilibrador de carga	Proporciona el equilibrio de carga del tráfico de S3 y Swift desde los clientes a los nodos de almacenamiento. **Nota:** este servicio también se encuentra en los nodos Gateway.
Sistema de gestión de redes (NMS)	Proporciona funcionalidad para Grid Manager.
Prometheus	Recopila y almacena métricas de series temporales de los servicios en todos los nodos.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

Use varios nodos de administrador

Un sistema StorageGRID puede incluir varios nodos de administrador para permitir supervisar y configurar continuamente el sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, las alertas y alarmas (sistema heredado) aún se activan y las notificaciones por correo electrónico y los mensajes de AutoSupport siguen enviados. Sin embargo, disponer de varios nodos de administrador no proporciona protección contra conmutación al nodo de respaldo, excepto notificaciones y mensajes de AutoSupport. En particular, las confirmaciones de alarma realizadas desde un nodo de administración no se copian en otros nodos de administración.



Si falla un nodo de administración, existen dos opciones para ver y configurar el sistema StorageGRID:

- Los clientes web pueden volver a conectarse a cualquier otro nodo de administrador disponible.
- Si un administrador del sistema ha configurado un grupo de nodos de administración de alta disponibilidad, los clientes web pueden seguir accediendo a Grid Manager o al Gestor de inquilinos mediante la dirección IP virtual del grupo de alta disponibilidad. Consulte "Gestión de grupos de alta disponibilidad".

> Al utilizar un grupo de alta disponibilidad, el acceso se interrumpe si el nodo de administración activo falla. Los usuarios deben volver a iniciar sesión después de que la dirección IP virtual del grupo ha conmute a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo se pueden realizar con el nodo de administrador principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar completamente.

Identifique el nodo de administración principal

El nodo de administración principal aloja el servicio CMN. Algunos procedimientos de mantenimiento solo se pueden realizar mediante el nodo de administrador principal.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > **Admin Node** y, a continuación, seleccione ➕ Para expandir el árbol de topología y mostrar los servicios alojados en este nodo de administración.

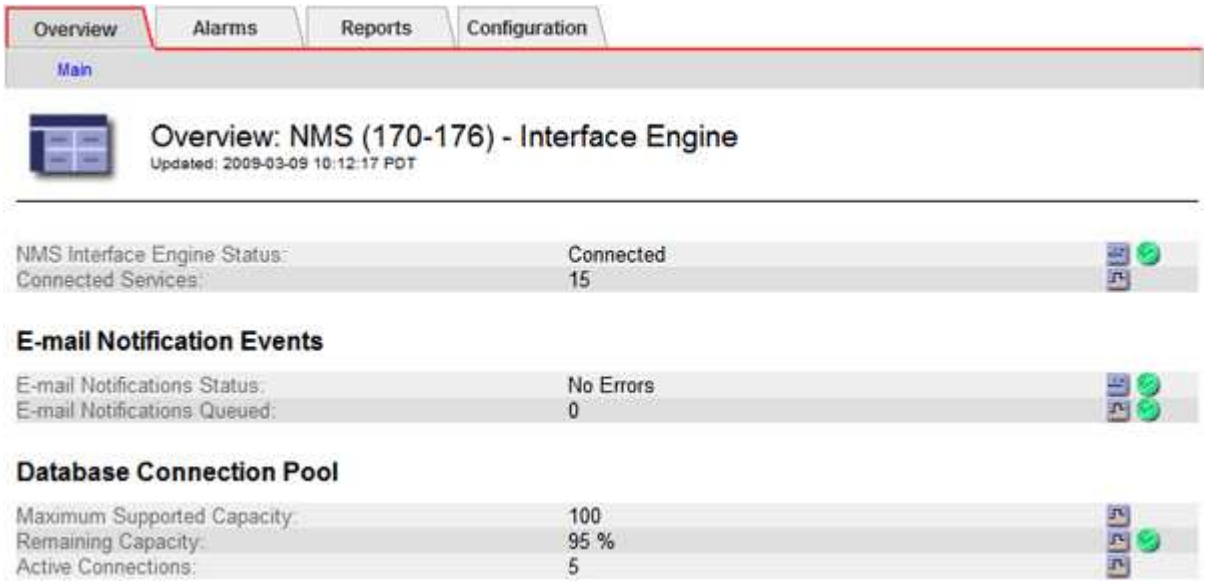
   El nodo de administración principal aloja el servicio CMN.

3. Si este nodo de administrador no aloja el servicio CMN, compruebe los demás nodos de administración.

Ver el estado de notificación y las colas

El servicio del sistema de administración de redes (NMS) en los nodos de administración envía notificaciones al servidor de correo. Puede ver el estado actual del servicio NMS y el tamaño de su cola de notificaciones en la página Motor de interfaz.

Para acceder a la página Motor de interfaz, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. Por último, seleccione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



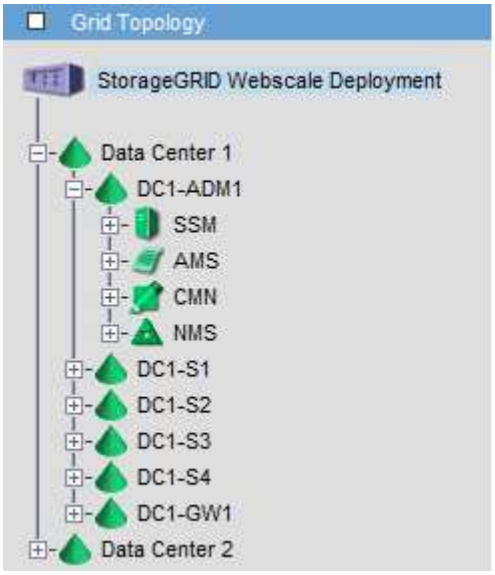
Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la notificación, un intento de mayor esfuerzo de reenviar la notificación al servidor de correo continúa durante un período de 60 segundos. Si la notificación no se envía al servidor de correo después de 60 segundos, la notificación se descarta de la cola de notificaciones y se realiza un intento de enviar la siguiente notificación de la cola.

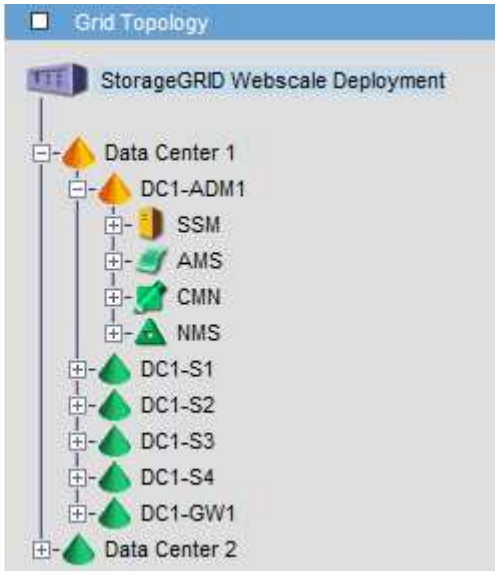
Puesto que las notificaciones se pueden borrar de la cola de notificaciones sin enviarse, es posible que se active una alarma sin que se envíe una notificación. Si se elimina una notificación de la cola sin que se envíe, se activa la alarma secundaria MINS (Estado de notificación de correo electrónico).

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. Puesto que las confirmaciones no se copian en otros nodos de administración, el árbol de topología de cuadrícula puede no tener el mismo aspecto para cada nodo de administración.

Esta diferencia puede ser útil al conectar clientes Web. Los clientes web pueden tener diferentes vistas del sistema StorageGRID de acuerdo con las necesidades del administrador.





Tenga en cuenta que las notificaciones se envían desde el nodo de administración donde se produce la confirmación.

Configure el acceso de los clientes de auditoría

Configure el acceso del cliente de auditoría para NFS

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. El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

Para acceder a los registros de auditoría, puede configurar el acceso de clientes a recursos compartidos de auditoría para NFS. O bien, puede hacerlo "usar un servidor de syslog externo".

El sistema StorageGRID utiliza un reconocimiento positivo para evitar la pérdida de mensajes de auditoría antes de que se escriban en el archivo de registro. Un mensaje permanece en cola en un servicio hasta que el servicio AMS o un servicio intermedio de retransmisión de auditoría ha reconocido el control de él. Para obtener más información, consulte "Revisar los registros de auditoría".

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña root/admin.
- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).

- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

Acerca de esta tarea

Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Confirme que todos los servicios tienen el estado en ejecución o verificado. Introduzca: `storagegrid-status`

   Si alguno de los servicios no aparece como en ejecución o verificado, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos. Pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración NFS. Introduzca: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Agregue el cliente de auditoría: `add-audit-share`
   a. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: `client_IP_address`
   b. Cuando se le solicite, pulse **Intro**.
6. Si se permite que más de un cliente de auditoría acceda al recurso compartido de auditoría, agregue la dirección IP del usuario adicional: `add-ip-to-share`
   a. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
   b. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*
   c. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de NFS.

d. Repita estos mismos pasos para cada cliente de auditoría adicional que tenga acceso al recurso compartido de auditoría.

7. De manera opcional, compruebe su configuración.
   a. Introduzca lo siguiente: `validate-config`

      Los servicios se comprueban y visualizan.

   b. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

   c. Cierre la utilidad de configuración NFS: `exit`
8. Determine si debe habilitar los recursos compartidos de auditoría en otros sitios.
   - Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.
   - Si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite estos recursos compartidos de auditoría según sea necesario:
     i. Inicie sesión de forma remota en el nodo de administración del sitio:
        A. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
        B. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
        C. Introduzca el siguiente comando para cambiar a la raíz: `su -`
        D. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
     ii. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.
     iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota. Introduzca: `exit`
9. Cierre la sesión del shell de comandos: `exit`

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido o elimine un cliente de auditoría existente eliminando su dirección IP.

Agregar un cliente de auditoría NFS a un recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido de auditoría.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña de la cuenta root/admin.
- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Introduzca: `add-ip-to-share`

   Se muestra una lista de los recursos compartidos de auditoría de NFS habilitados en el nodo de administración. El recurso compartido de auditoría aparece como: `/var/local/audit/export`

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*

   El cliente de auditoría se agrega al recurso compartido de auditoría.

6. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

7. Repita los pasos para cada cliente de auditoría que se debe agregar al recurso compartido de auditoría.
8. Si lo desea, compruebe la configuración: `validate-config`

   Los servicios se comprueban y visualizan.

   a. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

9. Cierre la utilidad de configuración NFS: `exit`
10. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

De lo contrario, si la implementación de StorageGRID incluye nodos de administración en otros sitios, opcionalmente podrá habilitar estos recursos compartidos de auditoría según sea necesario:

a. Inicie sesión de forma remota en el nodo de administración de un sitio:
   i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración.
c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`

11. Cierre la sesión del shell de comandos: `exit`

Comprobar la integración de auditoría de NFS

Después de configurar un recurso compartido de auditoría y agregar un cliente de auditoría NFS, puede montar el recurso compartido del cliente de auditoría y comprobar que los archivos estén disponibles en el recurso compartido de auditoría.

Pasos

1. Verifique la conectividad (o variante para el sistema cliente) usando la dirección IP del cliente del nodo de administración que aloja el servicio AMS. Introduzca: `ping IP_address`

   Verifique que el servidor responde, indicando conectividad.

2. Monte el recurso compartido de sólo lectura de auditoría usando un comando apropiado para el sistema operativo cliente. Un comando de Linux de ejemplo es (introduzca en una línea):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Utilice la dirección IP del nodo de administración que aloja el servicio AMS y el nombre de recurso compartido predefinido para el sistema de auditoría. El punto de montaje puede ser cualquier nombre seleccionado por el cliente (por ejemplo, *`myAudit`* en el comando anterior).

3. Verifique que los archivos estén disponibles en el recurso compartido de auditoría. Introduzca: `ls myAudit /*`

   donde *`myAudit`* es el punto de montaje del recurso compartido de auditoría. Debe haber al menos un archivo de registro en la lista.

Eliminar un cliente de auditoría NFS del recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Puede eliminar un cliente de auditoría existente eliminando su dirección IP.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña de la cuenta root/admin.
- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).

Acerca de esta tarea

No puede eliminar la última dirección IP permitida para acceder al recurso compartido de auditoría.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Elimine la dirección IP del recurso compartido de auditoría: `remove-ip-from-share`

   Se muestra una lista numerada de recursos compartidos de auditoría configurados en el servidor. El recurso compartido de auditoría aparece como: `/var/local/audit/export`

4. Introduzca el número correspondiente al recurso compartido de auditoría: *`audit_share_number`*

   Se muestra una lista numerada de direcciones IP permitidas para acceder al recurso compartido de auditoría.

5. Introduzca el número correspondiente a la dirección IP que desea eliminar.

   El recurso compartido de auditoría se actualiza y ya no se permite el acceso desde ningún cliente de auditoría con esta dirección IP.

6. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

7. Cierre la utilidad de configuración NFS: `exit`
8. Si la implementación de StorageGRID es una puesta en marcha de varios sitios de centro de datos con

nodos de administración adicionales en otros sitios, deshabilite estos recursos compartidos de auditoría según sea necesario:

a. Inicie sesión de forma remota en el nodo de administración de cada sitio:
   i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.
c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`

9. Cierre la sesión del shell de comandos: `exit`

Cambiar la dirección IP de un cliente de auditoría de NFS

Complete estos pasos si necesita cambiar la dirección IP de un cliente de auditoría de NFS.

Pasos

1. Agregue una nueva dirección IP a un recurso compartido de auditoría NFS existente.
2. Elimine la dirección IP original.

Información relacionada

- "Agregar un cliente de auditoría NFS a un recurso compartido de auditoría"
- "Eliminar un cliente de auditoría NFS del recurso compartido de auditoría"

Gestione los nodos de archivado

¿Qué es un nodo de archivado?

Opcionalmente, cada sitio del centro de datos StorageGRID se puede poner en marcha con un nodo de archivado, que permite conectarse a un sistema de almacenamiento de archivado externo específico, como Tivoli Storage Manager (TSM).

La compatibilidad con los nodos de archivo (tanto para archivar en la nube mediante la API S3 como para archivar en cinta mediante el middleware TSM) está obsoleta y se eliminará en una versión futura. Mover objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo ha sido reemplazado por ILM Cloud Storage Pools, que ofrecen más funcionalidad.

Consulte:

- "Migrar objetos a un pool de almacenamiento en la nube"
- "Utilice Cloud Storage Pools"

Además, debe quitar Nodos de archivo de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o anterior. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

El nodo de archivado proporciona una interfaz a través de la cual se puede dirigir un sistema de almacenamiento de archivado externo para el almacenamiento a largo plazo de datos de objetos. El nodo de archivado también supervisa esta conexión y la transferencia de datos de objeto entre el sistema StorageGRID y el sistema de almacenamiento de archivado externo objetivo.

Después de configurar las conexiones con el destino externo, puede configurar el nodo de archivado para optimizar el rendimiento de TSM, desconectar un nodo de archivado cuando un servidor TSM se acerca a la capacidad o no está disponible y configurar la configuración de replicación y recuperación. También puede establecer alarmas personalizadas para el nodo de archivado.

Los datos de objetos que no se pueden eliminar, pero no se accede con frecuencia, pueden moverse en cualquier momento de los discos giratorios de un nodo de almacenamiento a un almacenamiento de archivado externo, como el cloud o la cinta. Este archivado de los datos de objetos se realiza mediante la configuración del nodo de archivado del sitio del centro de datos y, a continuación, con la configuración de las reglas de ILM donde este nodo de archivado se selecciona como el "destino" para obtener instrucciones de colocación de contenido. El nodo de archivado no gestiona los propios datos de objetos archivados, lo consigue el dispositivo de archivado externo.

Los metadatos de objetos no se archivan, pero siguen en los nodos de almacenamiento.

Qué es el servicio ARC

El servicio de archivado (ARC) en nodos de archivado ofrece la interfaz de gestión que se puede utilizar para configurar conexiones a almacenamiento de archivado externo, como la cinta, a través de middleware TSM.

Se trata del servicio de ARC que interactúa con un sistema de almacenamiento de archivado externo, por lo que envía datos de objetos para almacenamiento near-line y realiza recuperaciones cuando una aplicación cliente solicita un objeto archivado. Cuando una aplicación cliente solicita un objeto archivado, un nodo de almacenamiento solicita los datos del objeto del servicio ARC. El servicio ARC realiza una solicitud al sistema de almacenamiento de archivos externo, que recupera los datos de objeto solicitados y los envía al servicio ARC. El servicio ARC verifica los datos del objeto y los reenvía al nodo de almacenamiento, que a su vez devuelve el objeto a la aplicación cliente solicitante.

Las solicitudes de datos de objetos archivados a cinta mediante TSM Middleware se gestionan por la eficiencia de las recuperaciones. Las solicitudes se pueden solicitar para que los objetos almacenados en orden secuencial en la cinta se soliciten en el mismo orden secuencial. A continuación, las solicitudes se colocan en la cola de espera para su envío al dispositivo de almacenamiento. En función del dispositivo de

archivado, se pueden procesar simultáneamente varias solicitudes de objetos en diferentes volúmenes.

Archivado en el cloud mediante la API de S3

Puede configurar un nodo de archivado para conectarse directamente a Amazon Web Services (AWS) o a cualquier otro sistema que pueda conectarse al sistema StorageGRID a través de la API de S3.

> La compatibilidad con los nodos de archivo (tanto para archivar en la nube mediante la API S3 como para archivar en cinta mediante el middleware TSM) está obsoleta y se eliminará en una versión futura. Mover objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo ha sido reemplazado por ILM Cloud Storage Pools, que ofrecen más funcionalidad.
>
> Consulte "Utilice Cloud Storage Pools".

Configure los ajustes de conexión para la API de S3

Si se conecta a un nodo de archivado con la interfaz de S3, debe configurar los ajustes de conexión para la API de S3. Hasta que se hayan configurado estos ajustes, el servicio ARC permanecerá en un estado de alarma principal, ya que no puede comunicarse con el sistema de almacenamiento de archivos externo.

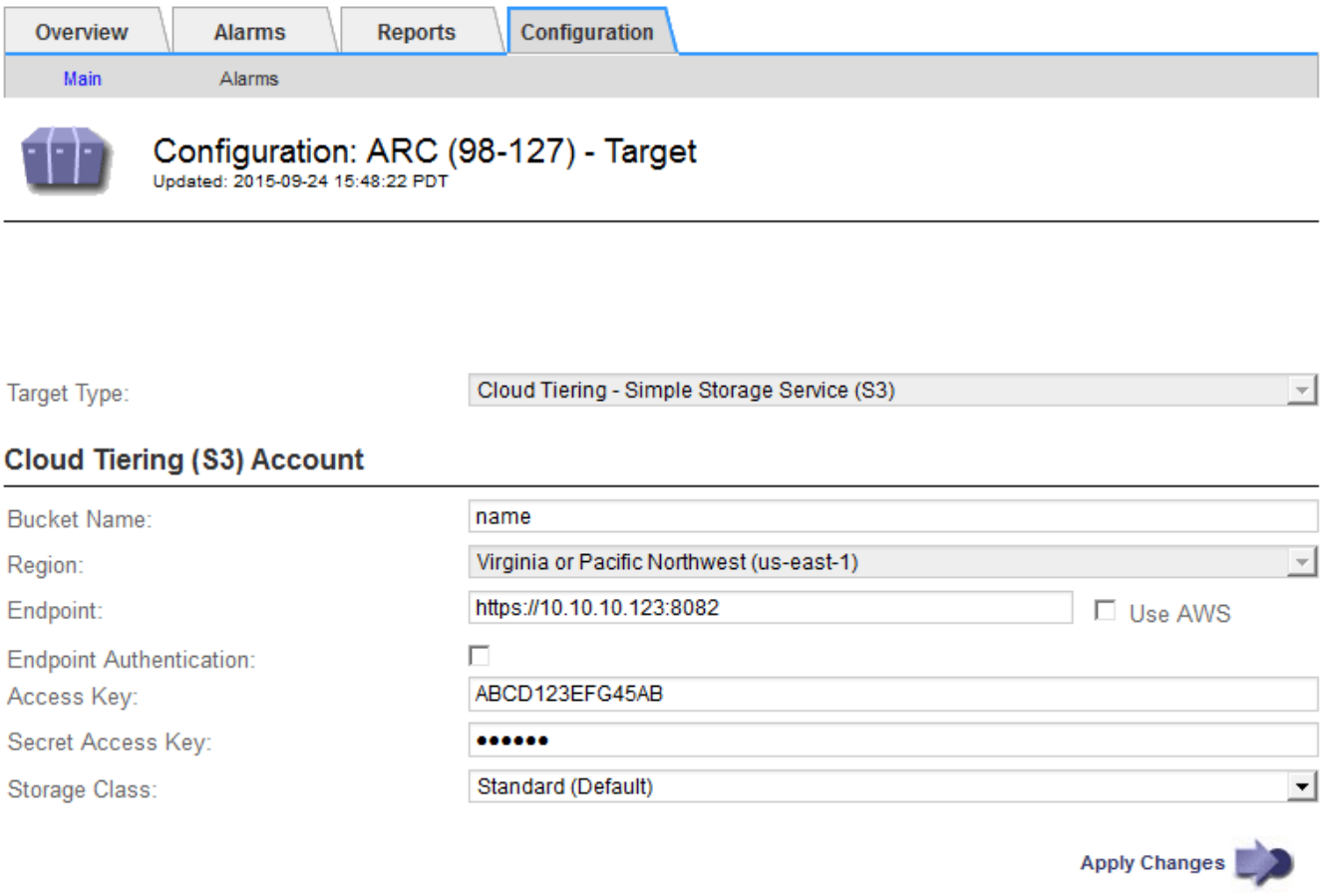
> La compatibilidad con los nodos de archivo (tanto para archivar en la nube mediante la API S3 como para archivar en cinta mediante el middleware TSM) está obsoleta y se eliminará en una versión futura. Mover objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo ha sido reemplazado por ILM Cloud Storage Pools, que ofrecen más funcionalidad.
>
> Consulte "Utilice Cloud Storage Pools".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Ha creado un bucket en el sistema de almacenamiento de archivado de destino:
  - El bloque está dedicado a un único nodo de archivado. No puede ser utilizado por otros nodos de archivo u otras aplicaciones.
  - El cucharón tiene la región adecuada seleccionada para su ubicación.
  - El bloque debe configurarse con el control de versiones suspendido.
- La segmentación de objetos está activada y el tamaño máximo de segmento es menor o igual a 4.5 GIB (4,831,838,208 bytes). Las solicitudes de API S3 que superen este valor fallarán si se usa S3 como sistema de almacenamiento de archivado externo.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **objetivo**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione **Cloud Tiering - simple Storage Service (S3)** en la lista desplegable Target Type.

> Los ajustes de configuración no estarán disponibles hasta que seleccione un tipo de destino.

5. Configure la cuenta de organización en niveles de cloud (S3) a través de la cual el nodo de archivado se conectará al sistema de almacenamiento de archivado externo compatible con S3 de destino.

   La mayoría de los campos en esta página son claros y explicativos. A continuación, se describen los campos que podrían presentar dificultades.

   - **Región**: Sólo está disponible si se selecciona **usar AWS**. La región que seleccione debe coincidir con la región del bloque.
   - **Endpoint** y **Use AWS**: Para Amazon Web Services (AWS), seleccione **usar AWS**. **Endpoint** se rellena automáticamente con una dirección URL de extremo basada en los atributos Nombre de bloque y Región. Por ejemplo:

     `https://bucket.region.amazonaws.com`

     En el caso de un destino que no sea AWS, introduzca la URL del sistema que aloja el bloque, incluido el número de puerto. Por ejemplo:

`https://system.com:1080`

   - **Autenticación de punto final**: Activada de forma predeterminada. Si la red al sistema de almacenamiento de archivado externo es de confianza, puede desactivar la casilla de verificación para desactivar el certificado SSL de punto final y la verificación de nombre de host 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 la casilla de verificación seleccionada.

- **Clase de almacenamiento**: Seleccione **Estándar (predeterminado)** para almacenamiento normal. Seleccione **redundancia reducida** sólo para objetos que se puedan volver a crear fácilmente. **Redundancia reducida** proporciona almacenamiento de menor costo con menos confiabilidad. Si el sistema de almacenamiento de archivado objetivo es otra instancia del sistema StorageGRID, **clase de almacenamiento** controla cuántas copias provisionales del objeto se realizan durante el procesamiento en el sistema de destino, si se utiliza el COMMIT doble cuando se ingieren objetos allí.

6. Seleccione **aplicar cambios**.

   Los ajustes de configuración especificados se validan y se aplican al sistema StorageGRID. Una vez configurado, el destino no se puede cambiar.

Modifique la configuración de conexión para la API de S3

Una vez que se configura el nodo de archivado para conectarse a un sistema de almacenamiento de archivado externo a través de la API S3, puede modificar algunos ajustes si cambia la conexión.

Antes de empezar

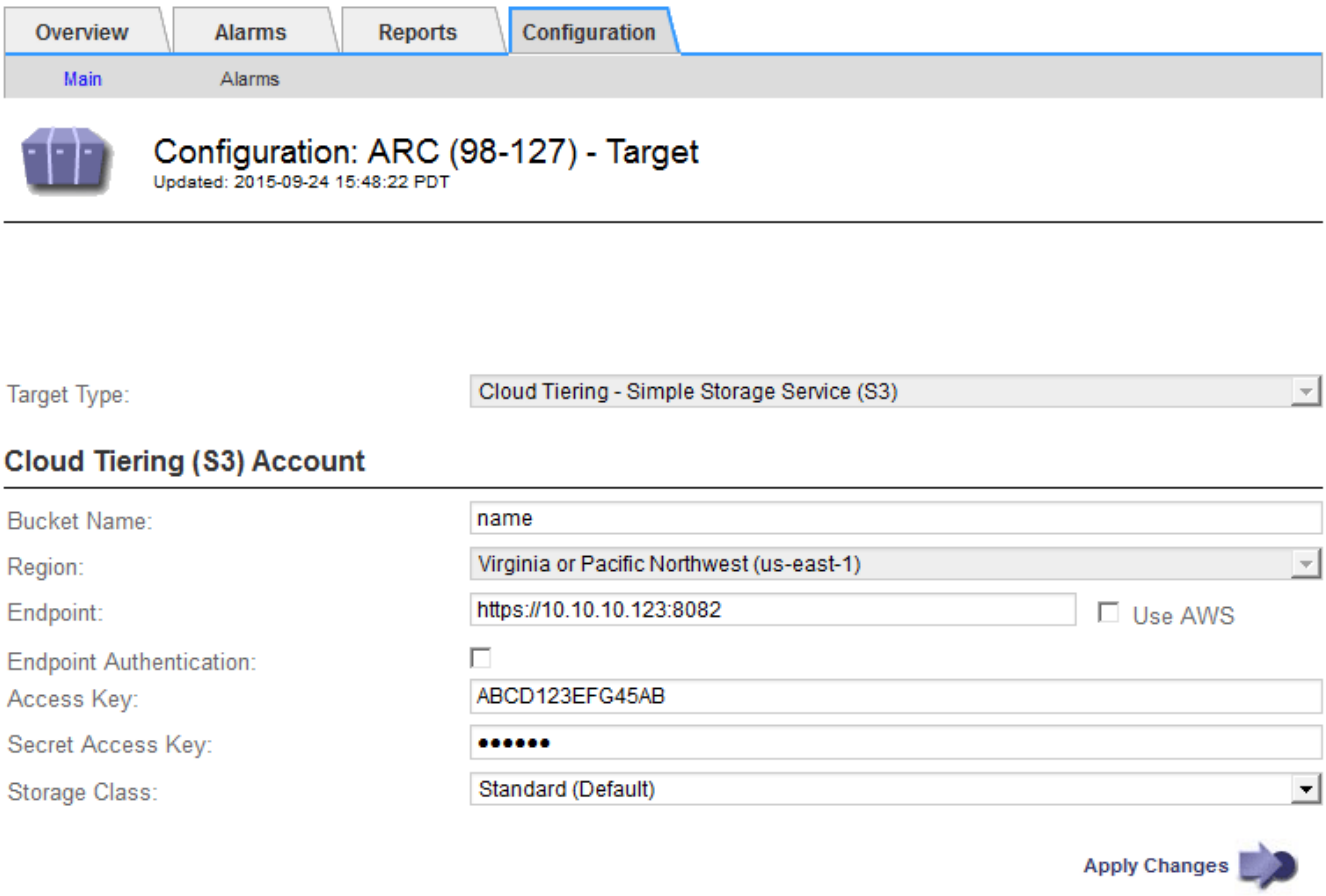
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

Si cambia la cuenta de Cloud Tiering (S3), debe asegurarse de que las credenciales de acceso del usuario tengan acceso de lectura/escritura al bloque, incluidos todos los objetos que el nodo de archivado había ingerido previamente en el bloque.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique la información de la cuenta, según sea necesario.

   Si cambia la clase de almacenamiento, se almacenan datos de objeto nuevos con la nueva clase de almacenamiento. El objeto existente continúa almacenado en la clase de almacenamiento definida cuando se procesa.

   Nombre de bloque, región y punto final, utilice valores de AWS y no se puede cambiar.

5. Seleccione **aplicar cambios**.

Modifique el estado del servicio de organización en niveles del cloud

Puede controlar la capacidad de lectura y escritura del nodo de archivado en el sistema de almacenamiento de archivado externo objetivo que se conecta a través de la API de S3 cambiando el estado del servicio de organización en niveles de cloud.

Antes de empezar

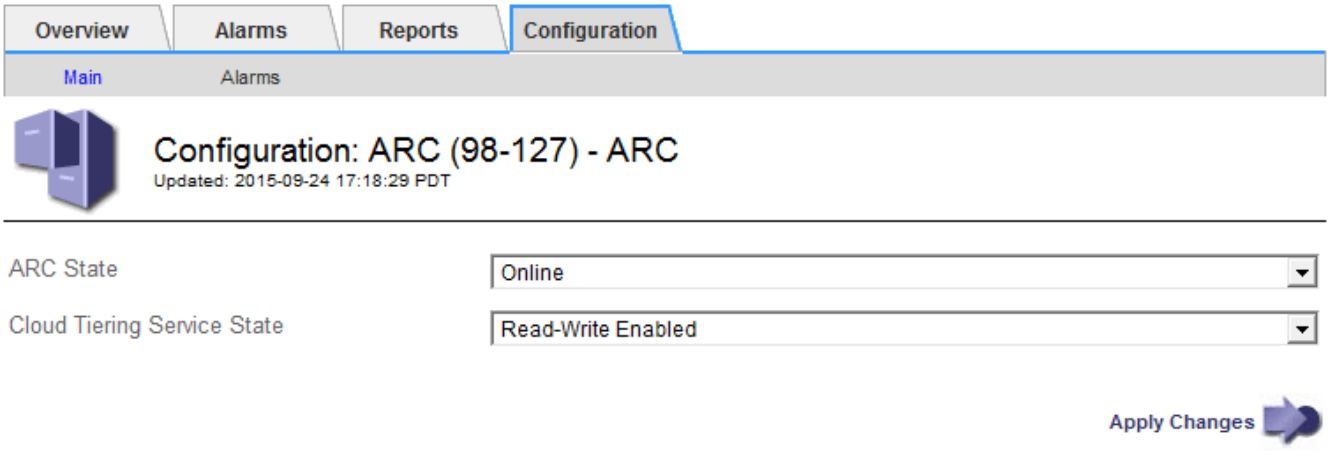
- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Debe tener permisos de acceso específicos.
- Debe configurarse el nodo de archivado.

Acerca de esta tarea

Puede desconectar el nodo de archivado de forma efectiva cambiando el estado del servicio de organización en niveles en la nube a **Read-Write Disabled**.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione un **Estado del servicio de organización en niveles de la nube**.
5. Seleccione **aplicar cambios**.

Restablezca el número de errores de almacén para la conexión API de S3

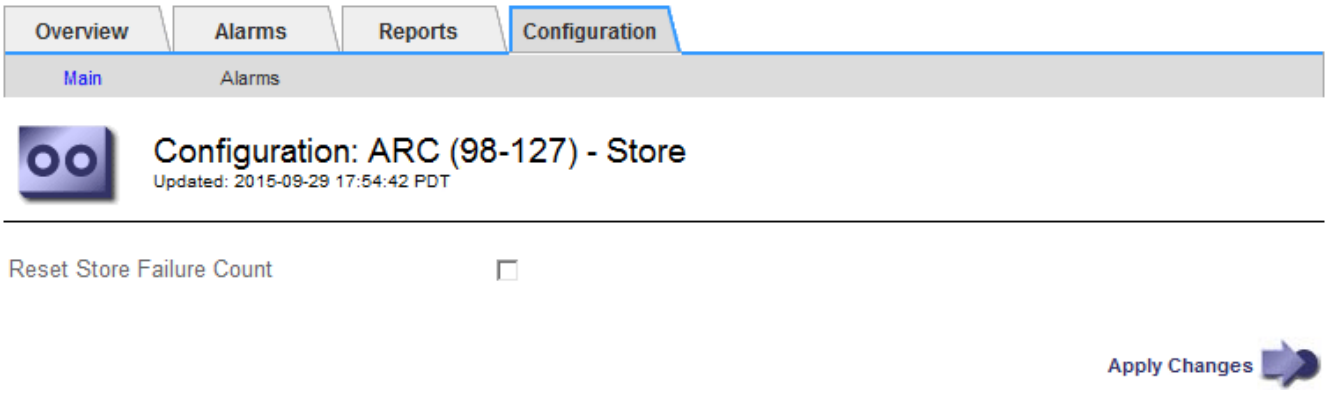
Si el nodo de archivado se conecta a un sistema de almacenamiento de archivado a través de la API de S3, puede restablecer el recuento de fallos de almacenamiento, que se puede utilizar para borrar la alarma de ARVF (fallos de almacenamiento).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione **Restablecer recuento de fallos de tienda**.

5. Seleccione **aplicar cambios**.

   El atributo fallos de almacén se restablece a cero.

Migrar objetos desde organización en niveles en el cloud: S3 a un pool de almacenamiento en el cloud

Si actualmente está utilizando la función **Cloud Tiering - Simple Storage Service (S3)** para organizar en niveles los datos de objetos en un bucket S3, debe 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Ya ha almacenado objetos en el bloque de S3 configurado para la organización en niveles del cloud.

> Antes de migrar datos de objetos, póngase en contacto con su representante de cuenta de NetApp para comprender y gestionar cualquier coste asociado.

Acerca de esta tarea

Desde el punto de vista de la gestión del ciclo de vida de la información, un pool de almacenamiento en cloud es similar al de un pool de almacenamiento. Sin embargo, si bien los pools de almacenamiento constan de nodos de almacenamiento o nodos de archivado dentro del sistema StorageGRID, un pool de almacenamiento en cloud consta de un bloque S3 externo.

Antes de migrar objetos desde Cloud Tiering: S3 a un pool de almacenamiento en cloud, primero debe crear un bucket de S3 y, a continuación, crear el Cloud Storage Pool en StorageGRID. A continuación, se puede crear una nueva política de ILM y reemplazar la regla de ILM utilizada para almacenar objetos en el bloque de niveles de cloud con una regla de ILM clonada que almacena los mismos objetos en el Cloud Storage Pool.

> Cuando los objetos se almacenan en un pool de almacenamiento en cloud, las copias de esos 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.

> La compatibilidad con los nodos de archivo (tanto para archivar en la nube mediante la API S3 como para archivar en cinta mediante el middleware TSM) está obsoleta y se eliminará en una versión futura. Mover objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo ha sido reemplazado por ILM Cloud Storage Pools, que ofrecen más funcionalidad.
>
> Consulte "Utilice Cloud Storage Pools".

Clases de gestión de TSM

Las clases de gestión definidas por el middleware TSM describen cómo funcionan las operaciones de copia de seguridad y archivado de TSM's y se pueden utilizar para especificar reglas para el contenido que aplica el servidor TSM. Estas reglas funcionan de manera independiente con la política de ILM del sistema StorageGRID, y deben ser coherentes con la necesidad del sistema StorageGRID de que los objetos se almacenen de forma permanente y que siempre estén disponibles para su recuperación en el nodo de archivado. Una vez que el nodo de archivado envía los datos de objeto a un servidor TSM, se aplican las reglas de ciclo de vida y retención de TSM mientras los datos del objeto se almacenan en cinta gestionada por el servidor TSM.

El servidor TSM utiliza la clase de gestión TSM para aplicar reglas para la ubicación de los datos o la retención después de que el nodo de archivado envía los objetos al servidor TSM. Por ejemplo, los objetos identificados como backups de base de datos (contenido temporal que puede sobrescribirse con datos más nuevos) se pueden tratar de forma diferente a los datos de la aplicación (contenido fijo que debe conservarse indefinidamente).

Configurar conexiones al middleware TSM

Para que el nodo de archivado pueda comunicarse con el middleware Tivoli Storage Manager (TSM), debe configurar varios valores.

Antes de empezar

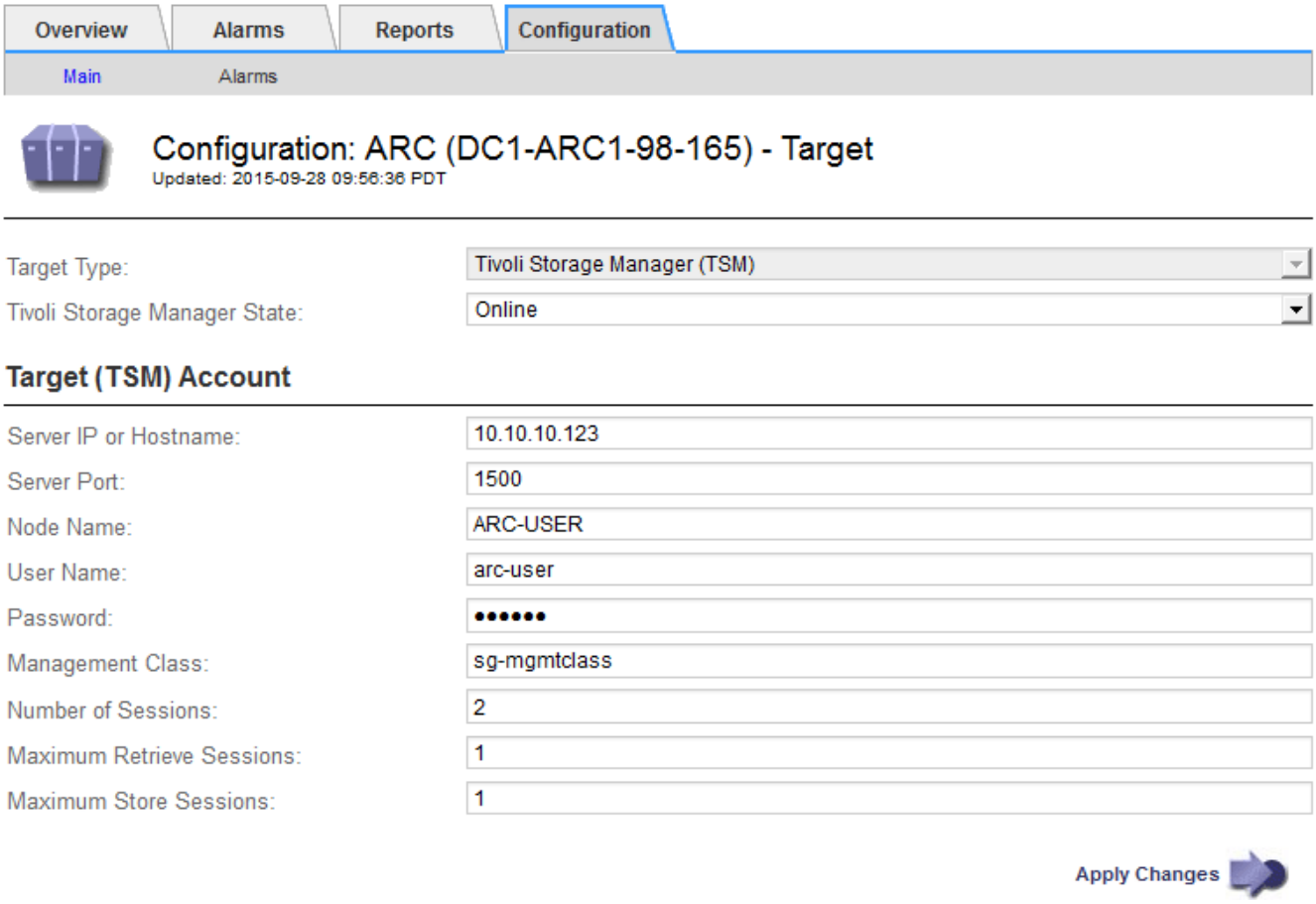
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

Hasta que se hayan configurado estos ajustes, el servicio ARC permanecerá en un estado de alarma principal, ya que no puede comunicarse con Tivoli Storage Manager.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.



4. En la lista desplegable **Tipo de destino**, seleccione **Tivoli Storage Manager (TSM)**.
5. En **Tivoli Storage Manager State**, seleccione **Offline** para evitar las recuperaciones desde el servidor de middleware TSM.

   De forma predeterminada, el estado de Tivoli Storage Manager se establece en línea, lo que significa que el nodo de archivado puede recuperar datos de objeto del servidor de middleware TSM.

6. Complete la siguiente información:

   - **IP del servidor o nombre de host**: Especifique la dirección IP o el nombre de dominio completo del servidor de middleware TSM utilizado por el servicio ARC. La dirección IP predeterminada es 127.0.0.1.

- **Puerto del servidor**: Especifique el número de puerto en el servidor de middleware TSM al que se conectará el servicio ARC. El valor predeterminado es 1500.
- **Nombre de nodo**: Especifique el nombre del nodo de archivado. Debe introducir el nombre (Arc-user) que ha registrado en el servidor de middleware TSM.
- **Nombre de usuario**: Especifique el nombre de usuario que el servicio ARC utiliza para iniciar sesión en el servidor TSM. Introduzca el nombre de usuario predeterminado (Arc-user) o el usuario administrativo que ha especificado para el nodo de archivado.
- **Contraseña**: Especifique la contraseña utilizada por el servicio ARC para iniciar sesión en el servidor TSM.
- **Clase de administración**: Especifique la clase de administración predeterminada que se va a utilizar si no se especifica una clase de administración cuando el objeto se está guardando en el sistema StorageGRID, o la clase de administración especificada no está definida en el servidor de middleware TSM.
- **Número de sesiones**: Especifique el número de unidades de cinta en el servidor de middleware TSM dedicadas al nodo de archivado. El nodo de archivado crea simultáneamente un máximo de una sesión por punto de montaje más un pequeño número de sesiones adicionales (menos de cinco).

  Debe cambiar este valor para que sea igual al valor establecido para MAXNUMMP (número máximo de puntos de montaje) cuando se registró o actualizó el nodo de archivado. (En el comando register, el valor predeterminado de MAXNUMMP utilizado es 1, si no se establece ningún valor.)

También debe cambiar el valor de MAXSESSIONS para el servidor TSM a un número que sea al menos tan grande como el número de sesiones establecido para el servicio ARC. El valor predeterminado de MAXSESSIONS en el servidor TSM es 25.

- **Sesiones de recuperación máximas**: Especifique el número máximo de sesiones que el servicio ARC puede abrir al servidor de middleware TSM para las operaciones de recuperación. En la mayoría de los casos, el valor apropiado es el número de sesiones menos el número máximo de sesiones de almacén. Si necesita compartir una unidad de cinta para su almacenamiento y recuperación, especifique un valor igual al número de sesiones.
- **Sesiones de almacenamiento máximas**: Especifique el número máximo de sesiones simultáneas que el servicio ARC puede abrir al servidor de middleware TSM para operaciones de archivado.

  Este valor se debería establecer en uno excepto cuando el sistema de almacenamiento de archivado destino está lleno y solo se pueden llevar a cabo recuperaciones. Establezca este valor en cero para utilizar todas las sesiones para las recuperaciones.

7. Seleccione **aplicar cambios**.

Optimice un nodo de archivado para sesiones de middleware de TSM

Puede optimizar el rendimiento de un nodo de archivado que se conecta a Tivoli Server Manager (TSM) configurando las sesiones del nodo de archivado.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

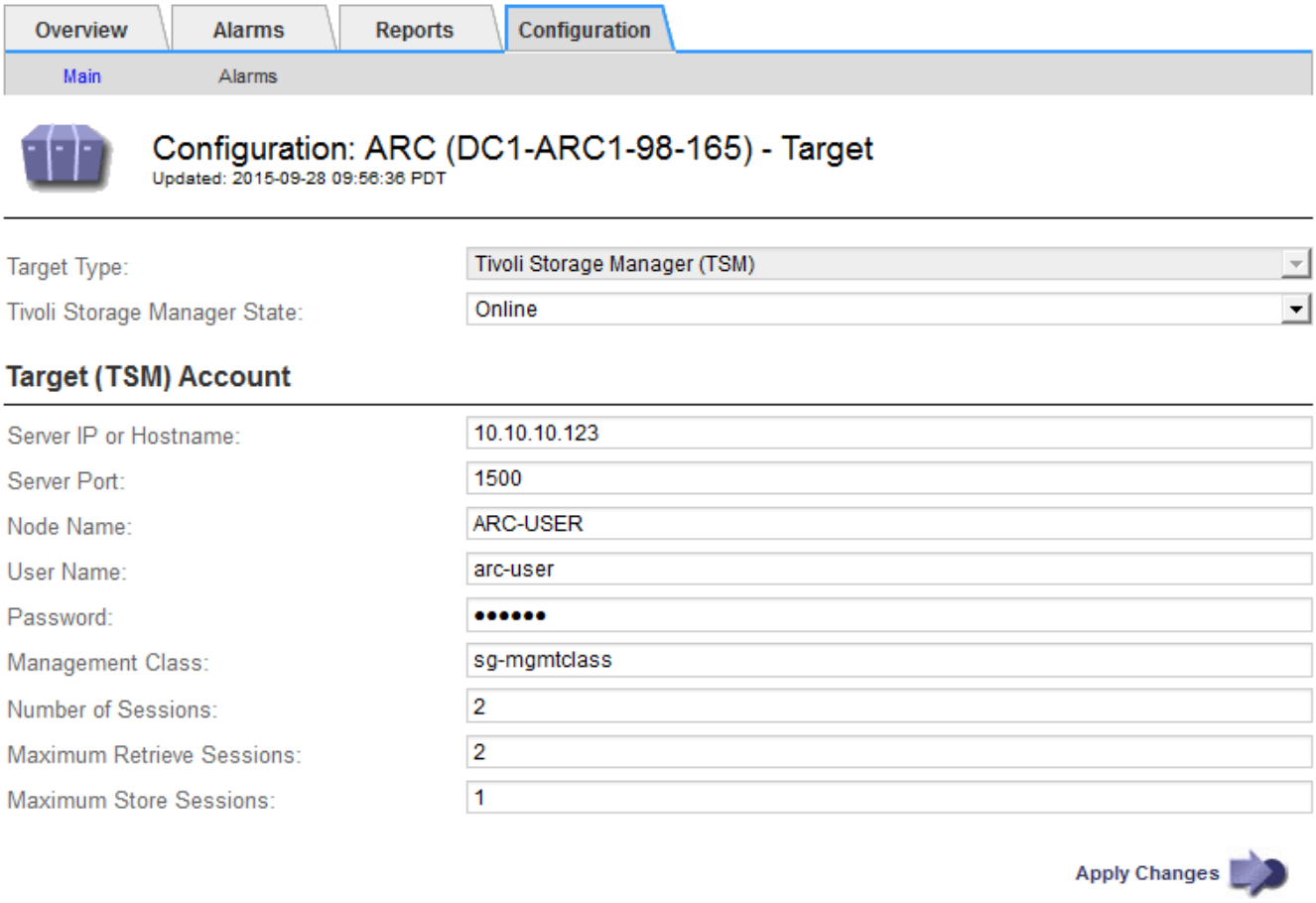
Acerca de esta tarea

Normalmente, el número de sesiones simultáneas que el nodo de archivado ha abierto al servidor de middleware TSM se establece en el número de unidades de cinta que el servidor TSM ha dedicado al nodo de

archivado. Se asigna una unidad de cinta para el almacenamiento mientras el resto se asigna para la recuperación. Sin embargo, en situaciones en las que un nodo de almacenamiento se está reconstruyendo desde copias de nodo de archivado o el nodo de archivado está funcionando en modo de sólo lectura, puede optimizar el rendimiento del servidor TSM estableciendo el número máximo de sesiones de recuperación para que sea el mismo que el número de sesiones simultáneas. El resultado es que todas las unidades pueden utilizarse al mismo tiempo para la recuperación; como máximo, una de estas unidades también puede utilizarse para el almacenamiento, si corresponde.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.
4. Cambiar **máximo de sesiones de recuperación** para que sea igual que **número de sesiones**.



5. Seleccione **aplicar cambios**.

Configure el estado del archivo y los contadores para TSM

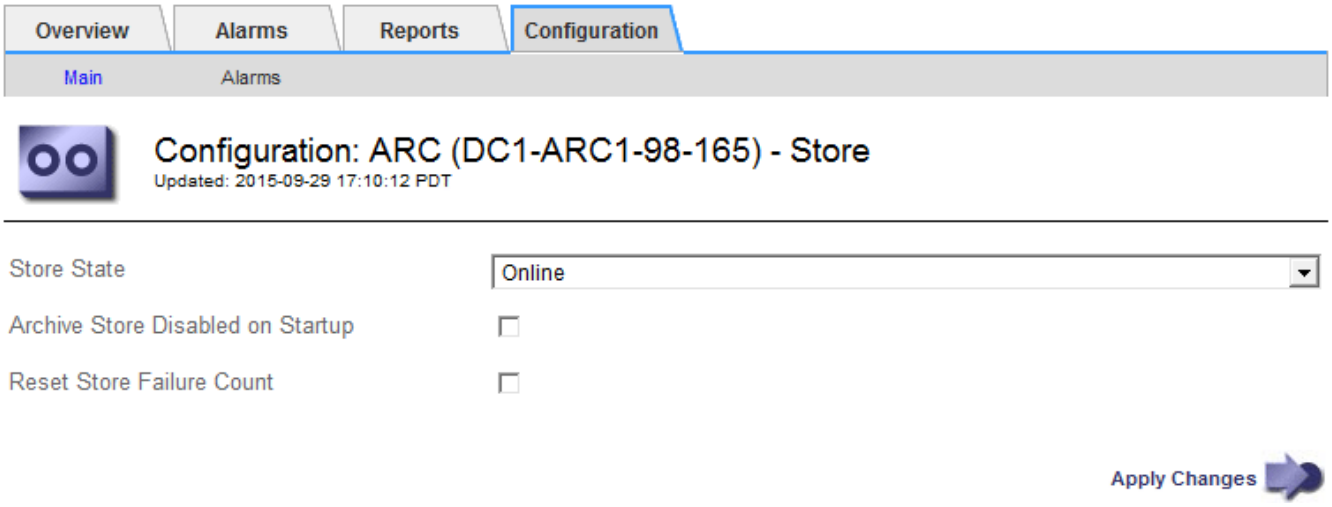
Si el nodo de archivado se conecta a un servidor de middleware TSM, puede configurar el estado del almacén de archivos de un nodo de archivado en línea o sin conexión. También puede desactivar el almacén de archivos cuando se inicie el nodo de archivado por primera vez o restablecer el recuento de fallos que se va a realizar el seguimiento de la alarma asociada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique los siguientes ajustes, según sea necesario:
   - Estado del almacén: Establezca el estado del componente en:
     - Online: El nodo de archivado está disponible para procesar datos de objetos para el almacenamiento del sistema de almacenamiento de archivado.
     - Offline: El nodo de archivado no está disponible para procesar datos de objetos para el almacenamiento del sistema de almacenamiento de archivado.
   - Almacén de archivos desactivado al inicio: Cuando se selecciona, el componente almacén de archivos permanece en el estado de sólo lectura cuando se reinicia. Se usa para deshabilitar de forma persistente el almacenamiento en el sistema de almacenamiento de archivado dirigido. Útil cuando el sistema de almacenamiento de archivado dirigido no puede aceptar contenido.
   - Restablecer recuento de fallos de almacén: Restablezca el contador para fallos de almacén. Se puede utilizar para borrar la alarma ARVF (fallo de almacén).
5. Seleccione **aplicar cambios**.

Información relacionada

"Gestione un nodo de archivado cuando el servidor TSM alcance la capacidad"

Gestione un nodo de archivado cuando el servidor TSM alcance la capacidad

El servidor TSM no tiene forma de notificar al nodo de archivado cuando la base de datos TSM o el almacenamiento multimedia de archivado gestionado por el servidor TSM está cerca de su capacidad. Esta situación se puede evitar gracias a la supervisión proactiva del servidor TSM.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

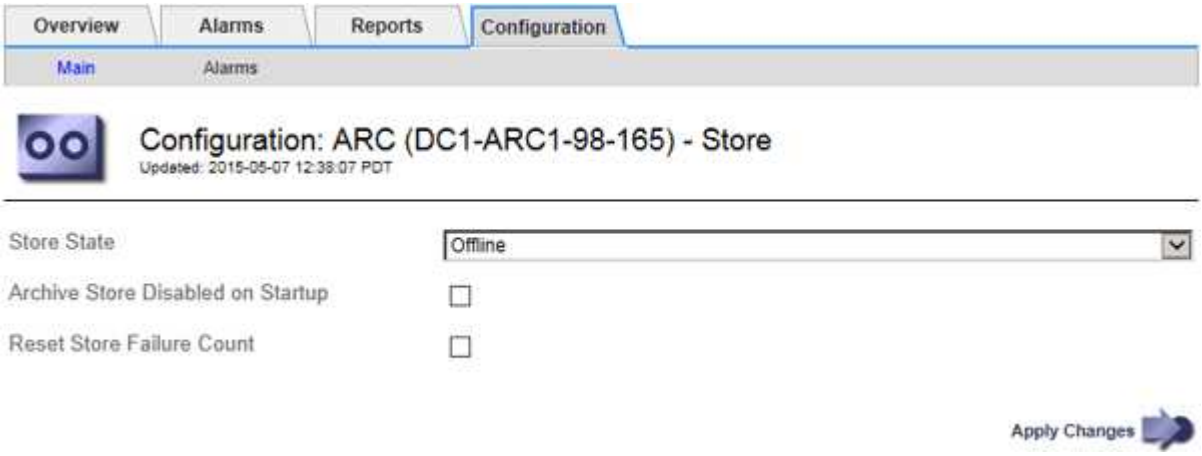
El nodo de archivado continúa aceptando datos de objetos para su transferencia al servidor TSM una vez que el servidor TSM deja de aceptar contenido nuevo. Este contenido no se puede escribir en medios gestionados por el servidor TSM. Si esto ocurre, se activa una alarma.

Impedir que el servicio ARC envíe contenido al servidor TSM

Para evitar que el servicio ARC envíe más contenido al servidor TSM, puede desconectar el nodo de archivado si desconecta el componente **ARC** > **Store**. Este procedimiento también puede ser útil para evitar alarmas cuando el servidor TSM no está disponible para tareas de mantenimiento.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.



4. Cambiar **Estado de tienda** a `Offline`.
5. Seleccione **almacén de archivos desactivado al inicio**.
6. Seleccione **aplicar cambios**.

Configure el nodo de archivado como de solo lectura si el middleware TSM alcanza la capacidad

Si el servidor de middleware TSM objetivo alcanza la capacidad, el nodo de archivado se puede optimizar para realizar únicamente recuperaciones.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.
4. Cambie el número máximo de sesiones de recuperación para que sea el mismo que el número de sesiones simultáneas enumeradas en el número de sesiones.
5. Cambie el número máximo de sesiones de almacenamiento a 0.

No es necesario cambiar el número máximo de sesiones de almacén a 0 si el nodo de archivado es de sólo lectura. No se crearán sesiones de almacenamiento.

6. Seleccione **aplicar cambios**.

Configure los ajustes de recuperación del nodo de archivado

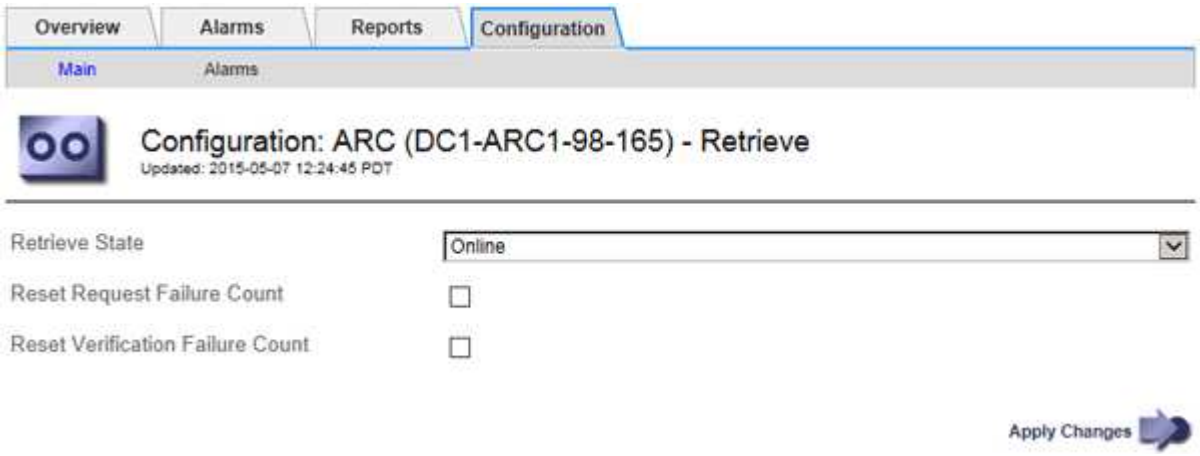
Puede configurar los ajustes de recuperación de un nodo de archivado para establecer el estado en línea o sin conexión, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **recuperar**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique los siguientes ajustes, según sea necesario:
   - **Estado de recuperación**: Establezca el estado del componente en:
     - En línea: El nodo de cuadrícula está disponible para recuperar datos de objeto del dispositivo multimedia de archivado.
     - Offline: El nodo de grid no está disponible para recuperar los datos del objeto.
   - Restablecer Recuento de Fallos de Solicitud: Seleccione la casilla de control para restablecer el contador 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 de fallos de verificación en los datos de objetos recuperados. Esto se puede utilizar para borrar la alarma ARRV (fallos de verificación).
5. Seleccione **aplicar cambios**.

Configure la replicación del nodo de archivado

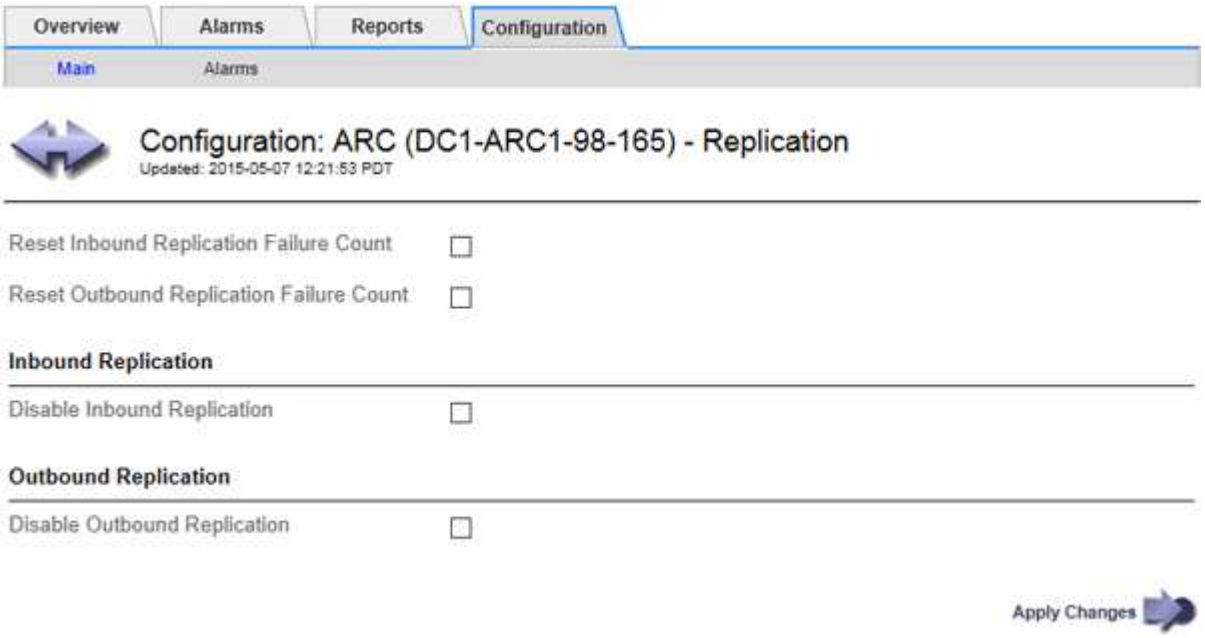
Puede configurar la configuración de replicación para un nodo de archivado y desactivar la replicación entrante y saliente, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Replication**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique los siguientes ajustes, según sea necesario:
   - **Restablecer recuento de fallos de replicación entrante**: Seleccione para restablecer el contador en caso de fallos de replicación entrante. Esto se puede utilizar para borrar la alarma RIRF (replicaciones entrantes — fallidas).
   - **Reset Outbound Replication Failure Count**: Seleccione para restablecer el contador de fallos de replicación saliente. Esto se puede utilizar para borrar la alarma RORF (réplicas de salida — fallida).
   - **Desactivar replicación entrante**: Seleccione esta opción para desactivar la replicación entrante como parte de un procedimiento de mantenimiento o prueba. Dejar borrado durante el funcionamiento normal.

     Cuando la replicación entrante está desactivada, los datos de objeto se pueden recuperar del servicio ARC para la replicación en 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-.

   - **Deshabilitar la replicación saliente**: Seleccione la casilla de verificación para desactivar la replicación saliente (incluidas las solicitudes de contenido para recuperaciones HTTP) como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal.

Cuando la replicación saliente está desactivada, los datos de objeto se pueden copiar en este servicio ARC para cumplir con las reglas de ILM, pero los datos de objeto no se pueden recuperar del servicio ARC para copiarlos en otras ubicaciones del sistema StorageGRID. El servicio ARC es de sólo escritura-.

5. Seleccione **aplicar cambios**.

Establezca alarmas personalizadas para el nodo de archivado

Debe establecer alarmas personalizadas para los atributos ARQL y ARRL que se utilizan para supervisar la velocidad y la eficacia de la recuperación de datos de objetos del sistema de almacenamiento de archivado por parte del nodo de archivado.

- ARQL: Longitud media de la cola. El tiempo medio, en microsegundos, que los datos de objetos se encuentran en cola para la recuperación del sistema de almacenamiento de archivado.
- ARRL: Promedio de latencia de solicitud. El tiempo medio, en microsegundos, que necesita el nodo de archivado para recuperar los datos de objetos del sistema de almacenamiento de archivado.

Los valores aceptables para estos atributos dependen de la configuración y el uso del sistema de almacenamiento de ficheros. (Vaya a **ARC** > **Retrieve** > **Overview** > **Main**.) Los valores establecidos para los tiempos de espera de las solicitudes y el número de sesiones disponibles para las solicitudes de recuperación tienen una influencia especial.

Una vez finalizada la integración, supervise las recuperaciones de datos de objetos del nodo de archivado para establecer valores para los tiempos de recuperación y las longitudes de cola normales. A continuación, cree alarmas personalizadas para ARQL y ARRL que se activarán si surge una condición de funcionamiento anormal. Consulte las instrucciones para "gestión de alarmas (sistema heredado)".

Integrar Tivoli Storage Manager

Configuración y funcionamiento del nodo de archivado

Su sistema StorageGRID gestiona el nodo de archivado como una ubicación en la que los objetos se almacenan de forma indefinida y siempre son accesibles.

Cuando se procesa un objeto, se crean copias en todas las ubicaciones necesarias, incluidos los nodos de archivado, según las reglas de gestión del ciclo de vida de la información (ILM) definidas para el sistema StorageGRID. El nodo de archivado actúa como cliente de un servidor TSM y las bibliotecas del cliente TSM se instalan en el nodo de archivado mediante el proceso de instalación del software StorageGRID. Los datos de objeto dirigidos al nodo de archivado para el almacenamiento se guardan directamente en el servidor TSM a medida que se reciben. El nodo de archivado no guarda los datos de objetos antes de guardarlos en el servidor TSM ni realiza la agregación de objetos. Sin embargo, el nodo de archivado puede enviar varias copias al servidor TSM en una única transacción cuando las tasas de datos lo garantizan.

Una vez que el nodo de archivado guarda los datos de objeto en el servidor TSM, el servidor TSM administra los datos de objeto con sus políticas de ciclo de vida/retención. Estas políticas de retención deben definirse para que sean compatibles con la operación del nodo de archivado. Es decir, los datos de objeto guardados por el nodo de archivado deben almacenarse indefinidamente y siempre deben ser accesibles desde el nodo de archivado, a menos que el nodo de archivado los elimine.

No hay conexión entre las reglas de ILM del sistema StorageGRID y las políticas de retención/ciclo de vida del servidor TSM. Cada uno de ellos funciona de forma independiente; sin embargo, a medida que se ingiere cada objeto en el sistema StorageGRID, puede asignarle una clase de gestión de TSM. Esta clase de gestión

se pasa al servidor TSM junto con los datos de objetos. La asignación de diferentes clases de gestión a diferentes tipos de objetos permite configurar el servidor TSM para colocar los datos de objetos en distintos pools de almacenamiento o aplicar distintas políticas de migración o retención según sea necesario. Por ejemplo, los objetos identificados como backups de base de datos (contenido temporal que puede sobrescribirse con datos más nuevos) pueden tratarse de forma diferente a los datos de la aplicación (contenido fijo que debe conservarse indefinidamente).

El nodo de archivado se puede integrar con un servidor TSM nuevo o existente; no requiere un servidor TSM dedicado. Los servidores TSM se pueden compartir con otros clientes, siempre que el tamaño del servidor TSM se ajusta de forma adecuada a la carga máxima esperada. TSM debe instalarse en un servidor o máquina virtual independiente del nodo de archivado.

Es posible configurar más de un nodo de archivado para escribir en el mismo servidor TSM; sin embargo, esta configuración sólo se recomienda si los nodos de archivado escriben diferentes conjuntos de datos en el servidor TSM. No se recomienda configurar más de un nodo de archivado para escribir en el mismo servidor TSM cuando cada nodo de archivado escribe copias de los mismos datos de objeto en el archivo. En este último caso, ambas copias están sujetas a un único punto de error (el servidor TSM) para las copias redundantes de datos de objetos.

Los nodos de archivado no utilizan el componente de gestión 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 involucrada en la escritura de objetos directamente en cinta u otros medios extraíbles. Por lo tanto, el servidor TSM debe configurarse con un pool de almacenamiento en disco para el almacenamiento inicial de datos guardados por el nodo de archivado siempre que se utilice un medio extraíble.
- Debe configurar las políticas de retención de TSM para utilizar la retención basada en eventos-. El nodo de archivado no admite las políticas de retención de TSM basadas en la creación. Utilice los siguientes valores recomendados de retmin=0 y retver=0 en la directiva de retención (que indica que la retención comienza cuando el nodo de archivado activa un evento de retención y se conserva durante 0 días después de ese). Sin embargo, estos valores para retmin y retver son opcionales.

El pool de discos debe estar configurado para migrar datos al pool de cintas (es decir, el pool de cintas debe ser NXTSTGPOOL del pool de discos). El pool de cintas no debe configurarse como un pool de copias del pool de discos con escritura simultánea en ambos pools (es decir, el pool de cintas no puede ser un COPYSTGPOOL para el pool de discos). Para crear copias sin conexión de las cintas que contienen datos del nodo de archivado, configure el servidor TSM con un segundo grupo de cintas que sea un grupo de copias del grupo de cintas utilizado para los datos del nodo de archivado.

Complete la configuración del nodo de archivado

El nodo de archivado no funciona después de completar el proceso de instalación. Antes de que el sistema StorageGRID pueda guardar objetos en el nodo de archivado de TSM, debe completar la instalación y configuración del servidor TSM y configurar el nodo de

archivado para que se comunique con el servidor TSM.

Consulte la siguiente documentación de IBM, según sea necesario, cuando prepare el servidor TSM para la integración con el nodo de archivado en un sistema StorageGRID:

- "Guía del usuario e instalación de los controladores de dispositivos de cinta de IBM"
- "Referencia de programación de controladores de dispositivo de cinta IBM"

Instale un nuevo servidor TSM

Puede integrar el nodo de archivado con un servidor TSM nuevo o existente. Si va a instalar un nuevo servidor TSM, siga las instrucciones de la documentación de TSM para completar la instalación.

Un nodo de archivado no se puede alojar conjuntamente con un servidor TSM.

Configure el servidor TSM

Esta sección incluye instrucciones de ejemplo para preparar un servidor TSM siguiendo las prácticas recomendadas de TSM.

Las siguientes instrucciones le guían en el proceso de:

- Definición de un pool de almacenamiento en disco y un pool de almacenamiento en cinta (si es necesario) en el servidor TSM
- Definición de una directiva de dominio que utiliza la clase de administración TSM para los datos guardados desde el nodo de archivado y registro de un nodo para utilizar esta directiva de dominio

Estas instrucciones se proporcionan solo para su guía; no están destinadas a reemplazar la documentación de TSM, ni para proporcionar instrucciones completas y adecuadas para todas las configuraciones. Un administrador de TSM debe proporcionar instrucciones específicas para la implementación que esté familiarizado con sus requisitos detallados y con el conjunto completo de documentación de TSM Server.

Definir los pools de almacenamiento en disco y cinta de TSM

El nodo de archivado escribe en un pool de almacenamiento en disco. Para archivar el contenido en cinta, debe configurar el grupo de almacenamiento en disco para mover el contenido a un grupo de almacenamiento en cinta.

Acerca de esta tarea

Para un servidor TSM, debe definir un pool de almacenamiento en cinta y un pool de almacenamiento en disco en Tivoli Storage Manager. Después de definir el pool de discos, cree un volumen de discos y asígnelo al pool de discos. -pool de cintas no es necesario si el servidor TSM utiliza únicamente el almacenamiento en disco.

Debe realizar varios pasos en el servidor TSM antes de poder crear un grupo de almacenamiento de cinta. (Cree una biblioteca de cintas y al menos una unidad en la biblioteca de cintas. Defina una ruta de acceso desde el servidor a la biblioteca y desde el servidor a las unidades y, a continuación, defina una clase de dispositivo para las unidades.) Los detalles de estos pasos pueden variar en función de la configuración de hardware y los requisitos de almacenamiento del sitio. Para obtener más información, consulte la documentación de TSM.

El siguiente conjunto de instrucciones ilustra el proceso. Debe tener en cuenta que los requisitos de su sitio pueden variar en función de los requisitos de la implementación. Para obtener detalles de configuración e instrucciones, consulte la documentación de TSM.

Debe iniciar sesión en el servidor con privilegios administrativos y utilizar la herramienta dsmadmc para ejecutar los siguientes comandos.

Pasos

1. Cree una biblioteca de cintas.

   ```
   define library tapelibrary libtype=scsi
   ```

   Donde *tapelibrary* es un nombre arbitrario elegido para la biblioteca de cintas y el valor de `libtype` pueden variar en función del tipo de biblioteca de cintas.

2. Defina una ruta de acceso desde el servidor a la biblioteca de cintas.

   ```
   define path servername tapelibrary srctype=server desttype=library device=lib-devicename
   ```

   - *servername* Es el nombre del servidor TSM
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido
   - *lib-devicename* es el nombre del dispositivo de la biblioteca de cintas

3. Defina una unidad para la biblioteca.

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* es el nombre que desea especificar para la unidad
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido

     Se recomienda configurar una unidad o unidades adicionales, según la configuración de hardware. (Por ejemplo, si el servidor TSM está conectado a un switch Fibre Channel que tiene dos entradas de una biblioteca de cintas, quizás desee definir una unidad para cada entrada).

4. Defina una ruta desde el servidor hasta la unidad definida.

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - *drive-dname* es el nombre del dispositivo de la unidad
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido

     Repita el procedimiento para cada unidad que haya definido para la biblioteca de cintas, utilizando una unidad aparte *drivename* y.. *drive-dname* para cada unidad.

5. Defina una clase de dispositivo para las unidades.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

- *DeviceClassName* es el nombre de la clase de dispositivo
- *lto* es el tipo de unidad conectada al servidor
- *tapelibrary* es el nombre de la biblioteca de cintas que ha definido
- *tapetype* es el tipo de cinta; por ejemplo, triunter3

6. Agregue volúmenes de cinta al inventario de la biblioteca.

   `checkin libvolume tapelibrary`

   tapelibrary es el nombre de la biblioteca de cintas que ha definido.

7. Cree la agrupación de almacenamiento de cinta principal.

   `define stgpool SGWSTapePool DeviceClassName description=description collocate=filespace maxscratch=XX`

   - *SGWSTapePool* Es el nombre del pool de almacenamiento de cinta del nodo de archivado. Puede seleccionar cualquier nombre para la agrupación de almacenamiento de cinta (siempre que el nombre utilice las convenciones de sintaxis esperadas por el servidor TSM).
   - *DeviceClassName* es el nombre de la clase de dispositivo para la biblioteca de cintas.
   - *description* Es una descripción del grupo de almacenamiento que se puede mostrar en el servidor TSM mediante `query stgpool` comando. Por ejemplo: «'bloque de almacenamiento en cinta para el nodo de archivado».
   - *collocate=filespace* Especifica que el servidor TSM debe escribir objetos del mismo espacio en una única cinta.
   - XX es uno de los siguientes:
     - El número de cintas vacías de la biblioteca de cintas (en el caso de que el nodo de archivado sea la única aplicación que utiliza la biblioteca).
     - El número de cintas asignadas para su uso por el sistema StorageGRID (en aquellos casos en los que se comparte la biblioteca de cintas).

8. En un servidor TSM, cree un pool de almacenamiento en disco. En la consola administrativa del servidor TSM, introduzca

   `define stgpool SGWSDiskPool disk description=description maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high lowmig=percent_low`

   - *SGWSDiskPool* Es el nombre del pool de discos del nodo de archivado. Es posible seleccionar cualquier nombre para el pool de almacenamiento de discos (siempre que el nombre utilice las convenciones de sintaxis que espera el TSM).
   - *description* Es una descripción del grupo de almacenamiento que se puede mostrar en el servidor TSM mediante `query stgpool` comando. Por ejemplo, «depósito de almacenamiento de disco para el nodo de archivado».
   - *maximum_file_size* fuerza a que los objetos de mayor tamaño se escriban directamente en la cinta, en lugar de en la caché del pool de discos. Se recomienda establecer *maximum_file_size* A 10 GB.
   - *nextstgpool=SGWSTapePool* Hace referencia al pool de almacenamiento de disco al pool de

almacenamiento de cinta definido para el nodo de archivado.

- *percent_high* establece el valor en el que el pool de discos comienza a migrar su contenido al grupo de cintas. Se recomienda establecer *percent_high* 0 para que la migración de datos comience inmediatamente
- *percent_low* establece el valor en el que se detiene la migración al pool de cintas. Se recomienda establecer *percent_low* 0 para borrar el pool de discos.

9. En un servidor TSM, cree un volumen de disco (o volúmenes) y asígnelo al pool de discos.

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* es el nombre del pool de discos.
- *volume_name* es la ruta completa a la ubicación del volumen (por ejemplo, `/var/local/arc/stage6.dsm`) En el servidor TSM en el que escribe el contenido del pool de discos como preparación para la transferencia a cinta.
- *size* Es el tamaño, en MB, del volumen de disco.

  Por ejemplo, para crear un único volumen de disco de forma que el contenido de un pool de discos llene una única cinta, configure el valor del tamaño en 200000 cuando el volumen de cinta tenga una capacidad de 200 GB.

  Sin embargo, es posible que sea conveniente crear varios volúmenes de disco de un tamaño menor, ya que el servidor TSM puede escribir en cada volumen del pool de discos. Por ejemplo, si el tamaño de la cinta es 250 GB, cree 25 volúmenes de disco con un tamaño de 10 GB (10000) cada uno.

El servidor TSM preasigna espacio en el directorio para el volumen de disco. Esto puede tardar algún tiempo en completarse (más de tres horas para un volumen de disco de 200 GB).

Defina una directiva de dominio y registre un nodo

Debe definir una directiva de dominio que utilice la clase de administración TSM para los datos guardados desde el nodo de archivado y, a continuación, registrar un nodo para utilizar esta directiva de dominio.

> Los procesos de nodo de archivado pueden perder memoria si caduca la contraseña de cliente para el nodo de archivado en Tivoli Storage Manager (TSM). Asegúrese de que el servidor TSM esté configurado para que el nombre de usuario/contraseña del cliente para el nodo de archivado no caduque nunca.

Al registrar un nodo en el servidor TSM para el uso del nodo de archivado (o actualizar un nodo existente), debe especificar el número de puntos de montaje que el nodo puede utilizar para las operaciones de escritura especificando el parámetro MAXNUMMP en el comando REGISTER NODE. La cantidad de puntos de montaje suele ser equivalente al número de cabezales de unidad de cinta asignados al nodo de archivado. El número especificado para MAXNUMMP en el servidor TSM debe ser al menos tan grande como el valor establecido para **ARC** > **Target** > **Configuration** > **Main** > **Maximum Store Sessions** para el nodo de archivado, Que se define en un valor de 0 o 1, ya que las sesiones de almacén simultáneas no son compatibles con el nodo de archivado.

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 utiliza una clase de gestión 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 configurar `retinit` para `retinit=create`. Ajuste `retinit=create` Bloquea el nodo de archivado para que no elimine contenido, ya que los eventos de retención se utilizan para eliminar contenido del servidor TSM.

4. Asigne la clase de administración para que sea la predeterminada.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Establezca el nuevo conjunto de directivas como activo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignore la advertencia «'no backup copy group'» que aparece cuando se introduce el comando Activate.

6. Registre un nodo para utilizar el nuevo conjunto de directivas en el servidor TSM. En el servidor TSM, introduzca (en una línea):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user y Arc-password son el mismo nombre de nodo de cliente y contraseña que se define en Archive Node, y el valor de MAXNUMMP se establece en el número de unidades de cinta reservadas para las sesiones de almacén de nodo de archivado.

   > De forma predeterminada, al registrar un nodo se crea un ID de usuario administrativo con la autoridad del propietario del cliente, con la contraseña definida para el nodo.

Migrar datos a StorageGRID

Puede migrar grandes cantidades de datos al sistema StorageGRID a la vez que utiliza el sistema StorageGRID para realizar operaciones diarias.

Utilice esta guía cuando planifique una migración de grandes cantidades de datos al sistema StorageGRID. No es una guía general sobre la migración de datos y no incluye pasos detallados para realizar una migración. Siga las directrices y las instrucciones de esta sección para asegurarse de que la migración de datos al sistema StorageGRID se realice de forma eficiente sin interferir en las operaciones del día a día y de que el sistema StorageGRID gestione los datos migrados de forma adecuada.

Confirmar la capacidad del sistema StorageGRID

Antes de migrar grandes cantidades de datos al sistema StorageGRID, confirme que el sistema StorageGRID tiene la capacidad de disco necesaria para gestionar el volumen previsto.

Si el sistema StorageGRID incluye un nodo de archivado y se ha guardado una copia de los objetos migrados en un almacenamiento near-line (como la cinta), asegúrese de que el almacenamiento del nodo de archivado tenga suficiente capacidad para el volumen previsto de datos migrados.

Como parte de la evaluación de la capacidad, observe el perfil de datos de los objetos que tiene pensado migrar y calcule la cantidad de capacidad de disco necesaria. Para obtener información detallada sobre cómo supervisar la capacidad del disco del sistema StorageGRID, consulte "Gestione nodos de almacenamiento" y las instrucciones para "Supervisión de StorageGRID".

Determine la política de ILM para los datos migrados

La política de ILM del sistema StorageGRID determina cuántas copias se realizan, las ubicaciones a las que se almacenan las copias y durante el tiempo que se conservan estas copias. Una política de ILM consta de un conjunto de reglas de ILM que describen cómo filtrar objetos y gestionar datos de objetos a lo largo del tiempo.

En función del uso que se haga de los datos migrados y de los requisitos relativos a los datos migrados, es posible que desee definir reglas de ILM únicas para los datos migrados que difieren de las reglas de ILM que se usan para las operaciones cotidianas. Por ejemplo, si hay requisitos normativos diferentes para la gestión diaria de los datos que para los datos que se incluyen en la migración, es posible que desee usar un número distinto de copias de los datos migrados en un grado de almacenamiento diferente.

Puede configurar reglas que se apliquen exclusivamente a los datos migrados si es posible distinguir de forma única entre los datos migrados y los datos de objetos guardados de las operaciones diarias.

Si puede distinguir de forma fiable entre los tipos de datos mediante uno de los criterios de metadatos, puede usar estos criterios para definir una regla de ILM que solo se aplica a los datos migrados.

Antes de iniciar la migración de datos, asegúrese de comprender la política de gestión del ciclo de vida de la información del sistema StorageGRID y cómo se aplicará a los datos migrados, y de haber realizado y probado cualquier cambio en la política de ILM. Consulte "Gestión de objetos con ILM".

> Una política de ILM que se haya especificado incorrectamente puede provocar una pérdida de datos irrecuperable. Revise detenidamente todos los cambios realizados en una política de ILM antes de activarla para asegurarse de que la política funcione como se desee.

Evaluar el 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 cuidadosamente de acuerdo con las instrucciones de esta guía para evitar repercutir en las operaciones diarias del sistema o, en casos extremos, colocando los 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 continuamente el sistema StorageGRID para asegurarse de que no se excedan los distintos valores de atributos.

Programe y supervise la migración de datos

La migración de datos debe programarse y supervisarse según sea necesario para garantizar que los datos se coloquen según la política de ILM en el plazo estipulado.

Programar la migración de datos

Evite migrar datos durante las horas operativas del núcleo. Limite la migración de datos a noches, fines de semana y otras veces cuando el uso del sistema sea bajo.

Si es posible, no programe la migración de datos durante períodos de actividad alta. Sin embargo, si no es práctico evitar completamente el período de alta actividad, es seguro continuar siempre que usted supervise de cerca los atributos relevantes y tome medidas si exceden los valores aceptables.

Supervisar la migración de datos

En esta tabla, se enumeran los atributos que debe supervisar durante la migración de datos y los problemas que representan.

Si utiliza directivas de clasificación de tráfico con límites de tasa para acelerar el procesamiento, puede supervisar la tasa observada junto con las estadísticas descritas en la siguiente tabla y reducir los límites si es necesario.

Supervisar	Descripción
Número de objetos que están a la espera de la evaluación de ILM	1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. 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.

Gestión de objetos con ILM

Gestión de objetos con ILM: Información general

Para gestionar los objetos de un sistema StorageGRID, configure una política de gestión de la vida útil de la información (ILM) compuesta por una o más reglas de ILM. Las reglas de ILM indican a la StorageGRID cómo crear y distribuir copias de datos de objetos y cómo gestionar esas copias con el tiempo.

Acerca de estas instrucciones

El diseño e implementación de reglas de ILM y la política de ILM requiere una planificación cuidadosa. Debe comprender los requisitos operativos, la topología del sistema StorageGRID, las necesidades de protección de

objetos y los tipos de almacenamiento disponibles. A continuación, debe determinar cómo desea copiar, distribuir y almacenar diferentes tipos de objetos.

Utilice estas instrucciones para:

- Conozca más detalles sobre gestión de la vida útil de la información de StorageGRID "Funcionamiento de ILM a lo largo de la vida de un objeto".
- Aprenda a configurar "pools de almacenamiento", "Pools de almacenamiento en cloud", y. "Reglas de ILM".
- Aprenda cómo "Cree, simule y active una política de ILM" que protegerá los datos de objetos en uno o más sitios.
- Aprenda cómo "Gestionar objetos con S3 Object Lock", Que ayuda a garantizar que los objetos en cubos específicos de S3 no se borren o sobrescriban durante un período de tiempo específico.

Leer más

Para obtener más información, consulte estos vídeos:

- "Vídeo: Reglas de gestión del ciclo de vida de la información en StorageGRID 11,7".

- "Vídeo: Políticas de gestión del ciclo de vida de la información en StorageGRID 11,7"

ILM y ciclo de vida de los objetos

Cómo funciona ILM a lo largo de la vida de un objeto

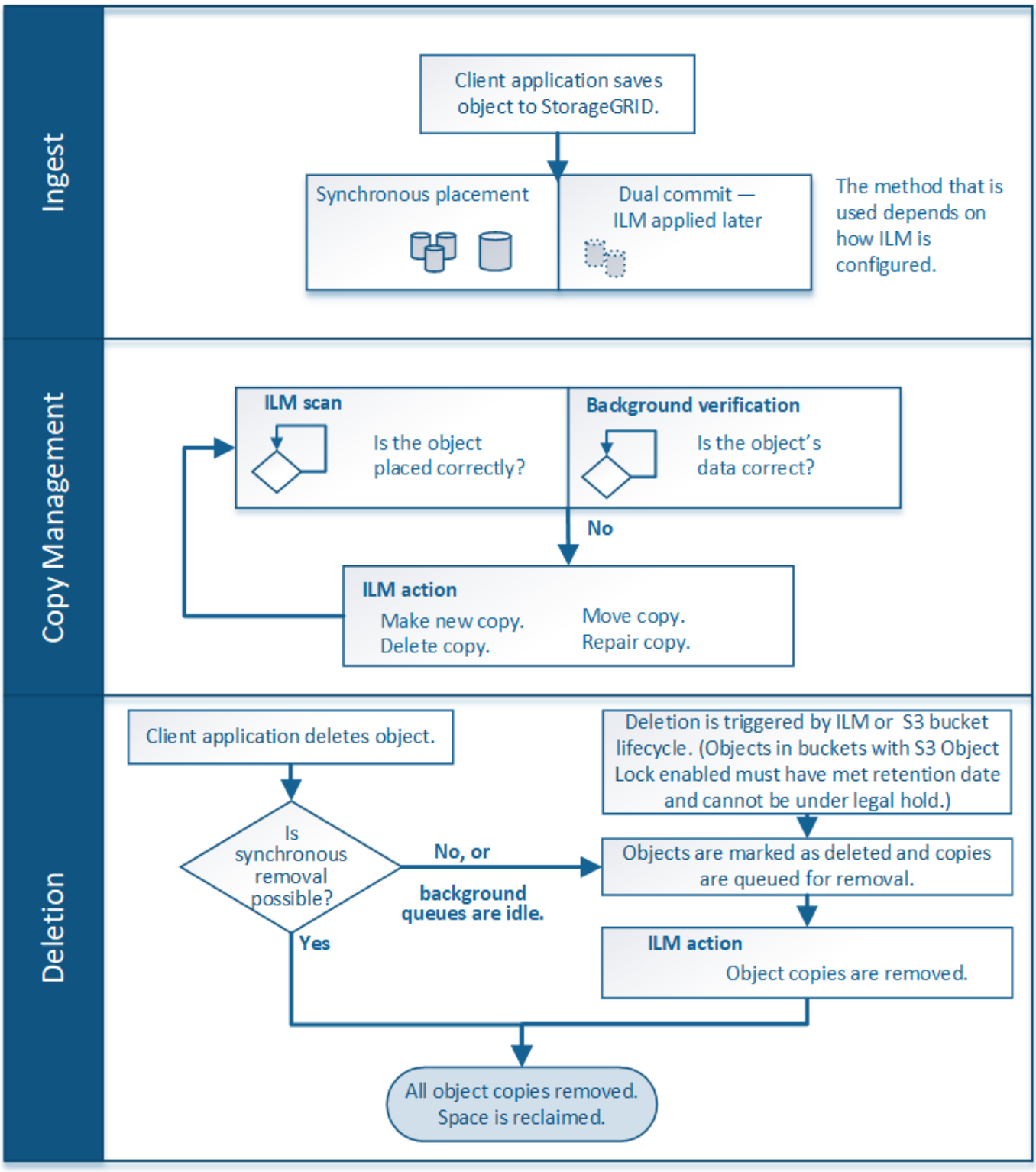
Comprender cómo utiliza StorageGRID ILM para gestionar objetos durante cada fase de su vida útil puede ayudarle a diseñar una política más eficaz.

- **Ingesta**: La ingesta comienza cuando una aplicación cliente S3 o Swift establece una conexión para guardar un objeto en el sistema StorageGRID, y se completa cuando StorageGRID devuelve un mensaje "'ingesta correcta'" al cliente. Los datos de objetos se protegen durante la ingesta aplicando instrucciones de ILM inmediatamente (ubicación síncrona) o creando copias provisionales y aplicando ILM más tarde (registro doble), según cómo se especifiquen los requisitos de ILM.
- **Administración de copias**: Después de crear el número y el tipo de copias de objetos que se especifican en las instrucciones de colocación de ILM, StorageGRID administra las ubicaciones de objetos y protege los objetos contra pérdidas.
  - Análisis y evaluación de ILM: StorageGRID analiza continuamente la lista de objetos almacenados en la cuadrícula y comprueba si las copias actuales cumplen los requisitos de ILM. Cuando se requieren diferentes tipos, números o ubicaciones de copias de objetos, StorageGRID crea, elimina o mueve copias según sea necesario.
  - Verificación en segundo plano: StorageGRID realiza de forma continua verificación en segundo plano para comprobar la integridad de los datos de objetos. Si se encuentra un problema, StorageGRID crea automáticamente una copia de objeto nueva o un fragmento de objeto con código de borrado de reemplazo en una ubicación que cumple los requisitos actuales de ILM. Consulte "Verifique la integridad del objeto".
- **Eliminación de objetos**: La gestión de un objeto finaliza cuando se eliminan todas las copias del sistema StorageGRID. Los objetos se pueden eliminar como resultado de una solicitud de eliminación por parte de

un cliente, o bien como resultado de la eliminación por ILM o la eliminación provocada por el vencimiento del ciclo de vida de un bloque de S3.

> Los objetos de un depósito que tiene S3 Object Lock activado no se pueden eliminar si están en una retención legal o si se ha especificado una fecha de retención hasta que no se cumple.

El diagrama resume el funcionamiento de ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

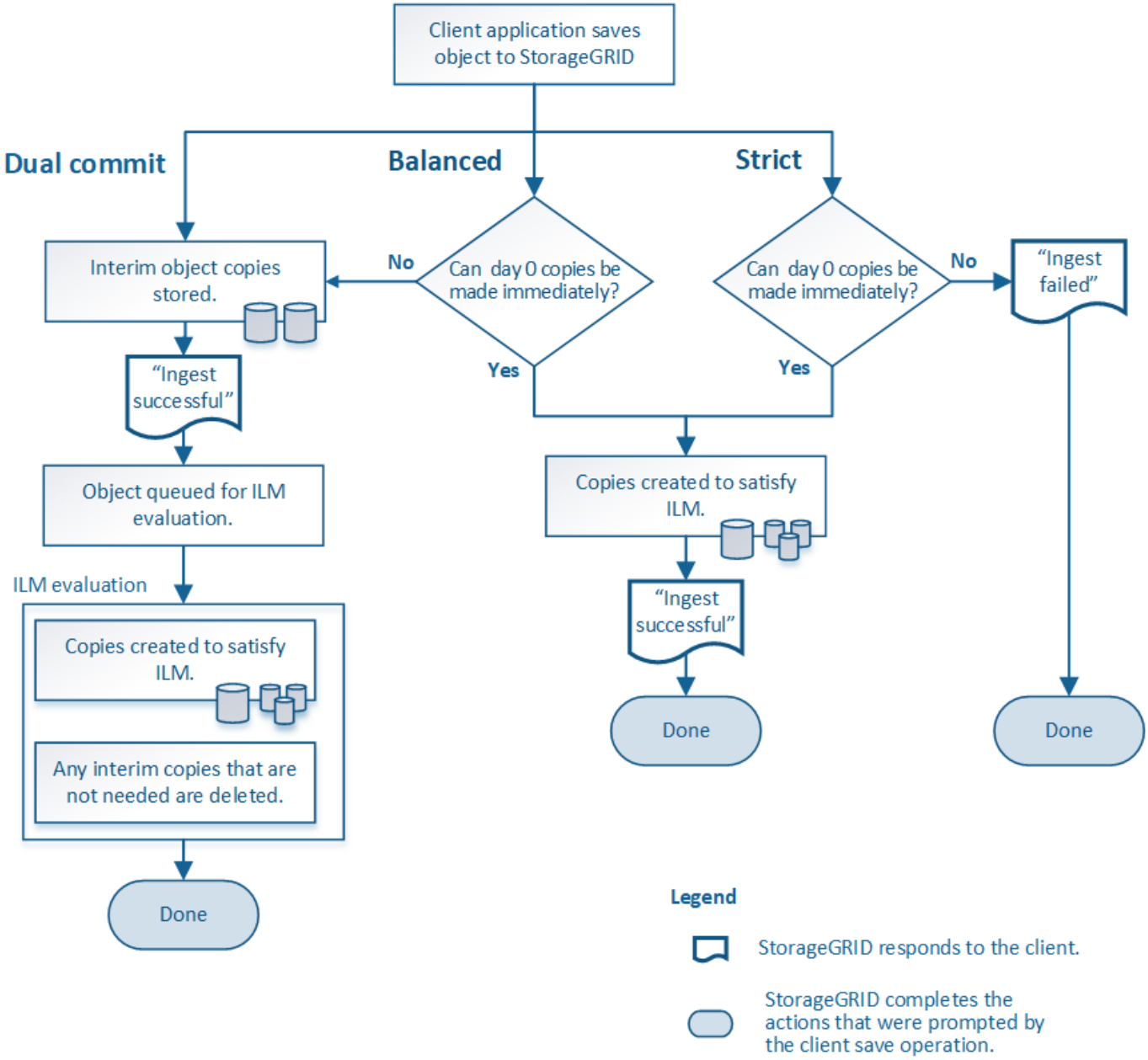
Opciones de procesamiento

Al crear una regla de ILM, se deben especificar una de estas tres opciones para proteger los objetos durante la ingesta: Dual commit, strict o balanced.

Según elija, StorageGRID realiza copias provisionales y pone en cola los objetos para la evaluación de ILM más tarde, o utiliza una ubicación síncrona y realiza copias inmediatamente para cumplir los requisitos de ILM.

Diagrama de flujo de opciones de ingesta

El diagrama de flujo muestra lo que ocurre cuando una regla de ILM se equipara con objetos que utiliza cada una de las tres opciones de ingesta.



Registro doble

Al seleccionar la opción de confirmación doble, StorageGRID realiza inmediatamente copias provisionales de objetos en dos nodos de almacenamiento diferentes y devuelve un mensaje «'ingesta correcta'» al cliente. El objeto se pone en cola para la evaluación de ILM, y se realicen copias que cumplan con las instrucciones de ubicación de la regla más adelante.

Cuándo utilizar la opción Dual COMMIT

Utilice la opción Dual Commit en uno de los siguientes casos:

- Está usando reglas de la ILM de varios sitios y la latencia de procesamiento de clientes es su principal consideración. Al utilizar la confirmación doble, debe asegurarse de que el grid pueda realizar el trabajo adicional de creación y eliminación de las copias de registro doble si no cumplen con el ciclo de vida de la información. Específicamente:
  - La carga en la cuadrícula debe ser lo suficientemente baja para evitar que se produzca una acumulación de ILM.
  - El grid debe tener un exceso de recursos de hardware (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Utiliza reglas de ILM de varios sitios y la conexión WAN entre los sitios suele tener una alta latencia o un ancho de banda limitado. En este escenario, el uso de la opción Dual commit puede ayudar a evitar los tiempos de espera de los clientes. Antes de elegir la opción Dual commit, debe probar la aplicación cliente con cargas de trabajo realistas.

Estricto

Al seleccionar la opción estricta, StorageGRID utiliza una ubicación síncrona al procesar y crea inmediatamente todas las copias de los objetos especificadas en las instrucciones de ubicación de la regla. La ingesta genera un error si StorageGRID no puede crear todas las copias, por ejemplo, porque no está disponible en estos momentos una ubicación de almacenamiento necesaria. El cliente debe volver a intentar la operación.

Cuándo usar la opción estricta

Utilice la opción estricta si tiene un requisito operativo y de normativa para almacenar inmediatamente objetos solo en las ubicaciones descritas en la regla de ILM. Por ejemplo, para satisfacer un requisito normativo, es posible que necesite utilizar la opción estricta y un filtro avanzado de restricción de ubicación para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Consulte "Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto".

Equilibrada (predeterminado)

Cuando selecciona la opción equilibrada, StorageGRID también utiliza la ubicación síncrona durante la ingesta y hace inmediatamente todas las copias especificadas en las instrucciones de ubicación de la regla. En contraste con la opción estricta, si StorageGRID no puede hacer todas las copias de inmediato, utiliza Confirmación doble en su lugar.

Cuándo utilizar la opción de equilibrio

Utilice la opción equilibrada para lograr la mejor combinación de protección de datos, rendimiento de grid y éxito de procesamiento. Equilibrada es la opción predeterminada del asistente Create ILM Rule.

Comprender las ventajas y las desventajas de cada una de las tres opciones de protección de datos en el procesamiento (confirmación equilibrada, estricta o doble) puede ayudarle a decidir cuál seleccionar para una regla de ILM.

Para obtener una descripción general de las opciones de ingesta, consulte "Opciones de procesamiento".

Ventajas de las opciones equilibradas y estrictas

En comparación con el registro doble, que crea copias provisionales durante la ingesta, las dos opciones de colocación sincrónica pueden proporcionar las siguientes ventajas:

- **Mejor seguridad de datos**: Los datos de objeto están protegidos inmediatamente como se especifica en las instrucciones de colocación de la regla ILM, que se pueden configurar para proteger contra una amplia variedad de condiciones de fallo, incluyendo la falla de más de una ubicación de almacenamiento. La confirmación doble solo puede protegerse contra la pérdida de una única copia local.
- **Funcionamiento de red más eficiente**: Cada objeto se procesa una sola vez, ya que se ingiere. Dado que el sistema StorageGRID no necesita realizar un seguimiento o eliminar copias provisionales, hay menos carga de procesamiento y se consume menos espacio de la base de datos.
- **(equilibrado) recomendado**: La opción equilibrada proporciona una eficiencia óptima de ILM. Se recomienda utilizar la opción Balanced a menos que se requiera un comportamiento de ingesta estricto o que el grid cumpla todos los criterios para utilizar Dual commit.
- **(estricta) certeza acerca de las ubicaciones de objetos**: La opción estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de colocación en la regla ILM.

Desventajas de las opciones equilibradas y estrictas

En comparación con la confirmación doble, las opciones equilibradas y estrictas tienen algunas desventajas:

- **Procesamiento de clientes más largos**: Las latencias de procesamiento de clientes pueden ser más largas. Cuando se utilizan las opciones equilibradas o estrictas, no se devuelve al cliente un mensaje ««ingerir correctamente» hasta que se creen y almacenen todos los fragmentos con código de borrado o las copias replicadas. Sin embargo, lo más probable es que los datos de objetos lleguen a su ubicación final mucho más rápido.
- **(Estrictas) mayores tasas de fallo de ingesta**: Con la opción estricta, la ingesta falla siempre que StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla de ILM. Es posible que observe tasas elevadas de error de procesamiento si una ubicación de almacenamiento necesaria está temporalmente sin conexión o si los problemas de red provocan retrasos en la copia de objetos entre sitios.
- * (Estricta) las ubicaciones de carga de varias partes de S3 pueden no ser las esperadas en algunas circunstancias*: Con estricta, se espera que los objetos se coloquen como se describe en la regla ILM o que falle el procesamiento. Sin embargo, con una carga de varias partes de S3 KB, se evalúa ILM para cada parte del objeto conforme se procesa, y para el objeto en su conjunto cuando se completa la carga de varias partes. En las siguientes circunstancias, esto podría dar lugar a colocaciones que son diferentes de lo esperado:
  - **Si ILM cambia mientras una carga multiparte de S3 está en curso**: Debido a que cada pieza se coloca según la regla que está activa cuando se ingiere la pieza, es posible que algunas partes del objeto no cumplan los requisitos actuales de ILM cuando se completa la carga de varias partes. En estos casos, la ingesta del objeto no falla. En su lugar, cualquier pieza que no se coloque correctamente se pone en cola para la reevaluación de ILM y posteriormente se mueve a la ubicación

correcta.

  - **Cuando las reglas de ILM filtran el tamaño**: Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplan con los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto, todas las partes del objeto se mueven a DC1.

- **(estricta) la ingesta no falla cuando las etiquetas de objeto o los metadatos se actualizan y las colocaciones recientemente requeridas no se pueden hacer**: Con estricto, se espera que los objetos se coloquen como se describe en la regla ILM o que falle el procesamiento. Sin embargo, cuando se actualizan metadatos o etiquetas de un objeto que ya está almacenado en la cuadrícula, el objeto no se vuelve a procesar. Esto significa que cualquier cambio en la ubicación del objeto que se desencadene por la actualización no se realiza inmediatamente. Los cambios de colocación se realizan cuando la ILM se vuelve a evaluar por los procesos normales de ILM en segundo plano. Si no se pueden realizar cambios de ubicación necesarios (por ejemplo, porque no está disponible una nueva ubicación requerida), el objeto actualizado conserva su ubicación actual hasta que los cambios de ubicación sean posibles.

Limitaciones en la ubicación de objetos con las opciones equilibradas y estrictas

Las opciones equilibradas o estrictas no se pueden usar para reglas de ILM que tengan alguna de estas instrucciones de ubicación:

- Ubicación en un pool de almacenamiento en cloud desde el día 0.
- Ubicación en un nodo de archivado en el día 0.
- Colocaciones en un pool de almacenamiento en la nube o en un nodo de archivado cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones se deben a que StorageGRID no puede realizar copias de forma síncrona en un grupo de almacenamiento en la nube o en un nodo de archivado, y una hora de creación definida por el usuario podría resolverse en el presente.

Cómo interactúan las reglas de ILM y los controles de coherencia para afectar a la protección de los datos

Tanto la regla de ILM como la elección del control de coherencia afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta la colocación inicial de las copias de objetos, mientras que el control de consistencia utilizado cuando se almacena un objeto afecta la colocación inicial de los metadatos de objetos. Dado que StorageGRID requiere acceso a los datos de un objeto y los metadatos para satisfacer las solicitudes del cliente, la selección de niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar mejor protección de datos inicial y respuestas del sistema más predecibles.

A continuación encontrará un breve resumen de los controles de consistencia disponibles en StorageGRID:

- **All**: Todos los nodos reciben metadatos de objeto inmediatamente o la solicitud falla.
- **Strong-global**: Los metadatos de objetos se distribuyen inmediatamente a todos los sitios. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
- **Strong-site**: Los metadatos del objeto se distribuyen inmediatamente a otros nodos en el sitio. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.

- **Read-after-new-write**: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

> Antes de seleccionar un nivel de coherencia, lea la descripción completa de los controles de coherencia en las instrucciones para "USE LA API DE REST DE S3". Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo puede interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **Norma ILM**: Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Se ha seleccionado el comportamiento de procesamiento estricto.
- **Nivel de coherencia**: "Strong-global" (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si en su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre los niveles de coherencia y las reglas del ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Información relacionada

- "Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto"

Cómo se almacenan los objetos (codificación de borrado o replicación)

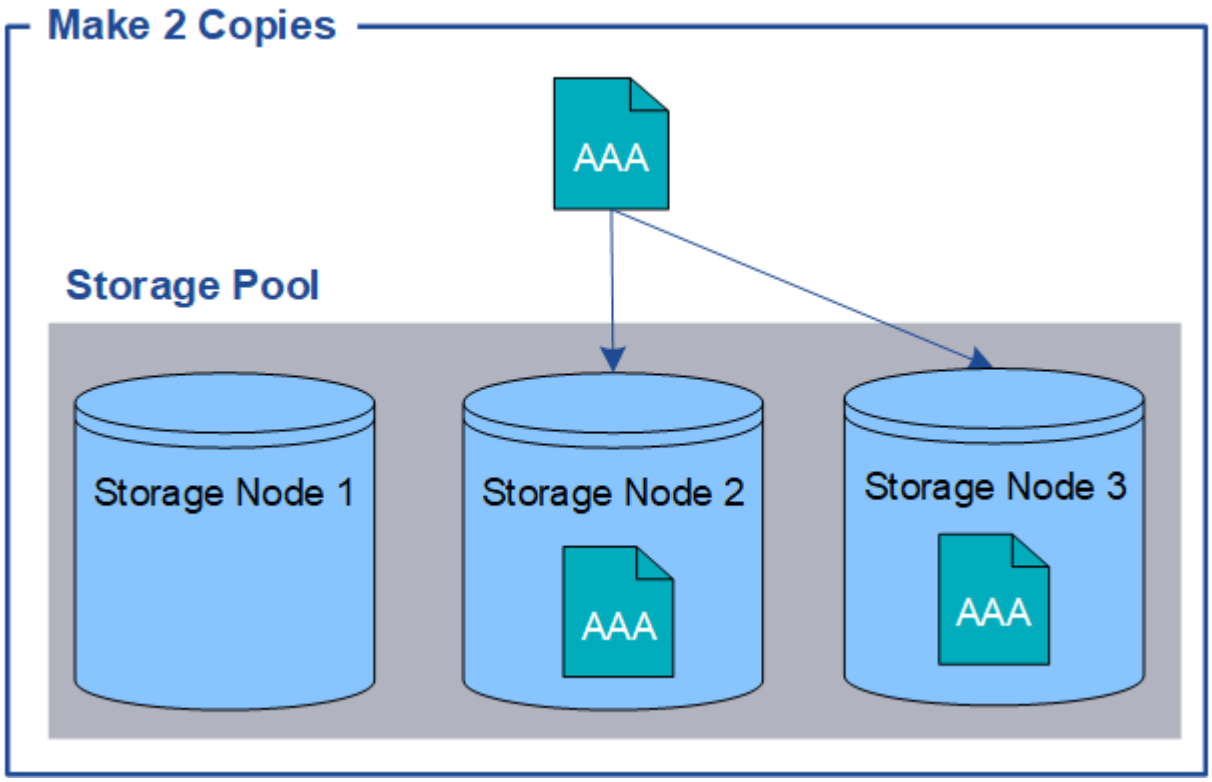
¿Qué es la replicación?

La replicación es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos. Cuando los objetos coinciden con una regla de ILM que usa la replicación, el sistema crea copias exactas de datos de objetos y almacena las copias en nodos de almacenamiento o nodos de archivado.

Cuando configura una regla de ILM para crear copias replicadas, especifica cuántas copias se deben crear,

dónde deben ubicarse y cuánto tiempo deben almacenarse las copias en cada ubicación.

En el ejemplo siguiente, la regla de ILM especifica que dos copias replicadas de cada objeto se coloquen en un pool de almacenamiento que contenga tres nodos de almacenamiento.



Cuando StorageGRID coincide con los objetos de esta regla, crea dos copias del objeto, colocando cada copia en un nodo de almacenamiento diferente en el pool de almacenamiento. Las dos copias pueden colocarse en dos de los tres nodos de almacenamiento disponibles. En este caso, la regla colocó copias de objetos en los nodos de almacenamiento 2 y 3. Debido a que hay dos copias, el objeto se puede recuperar si alguno de los nodos del pool de almacenamiento falla.

> StorageGRID solo puede almacenar una copia replicada de un objeto en un nodo de almacenamiento dado. Si el grid incluye tres nodos de almacenamiento y se crea una regla de gestión del ciclo de vida de la información de 4 copias, solo se crearán tres copias: Una por cada nodo de almacenamiento. Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

Información relacionada

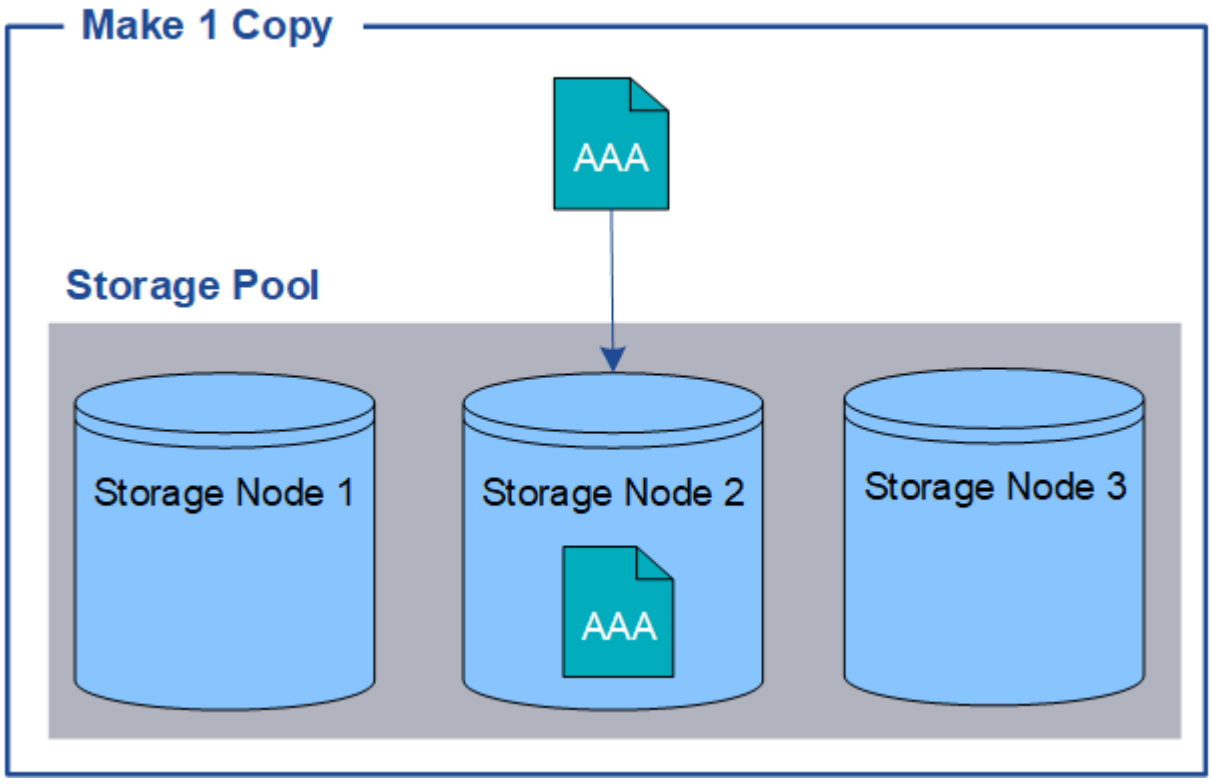
- "¿Qué es el código de borrado?"
- "¿Qué es un pool de almacenamiento?"
- "Habilite la protección contra pérdida de sitios mediante replicación y código de borrado"

Por qué no se debe utilizar la replicación de copia única

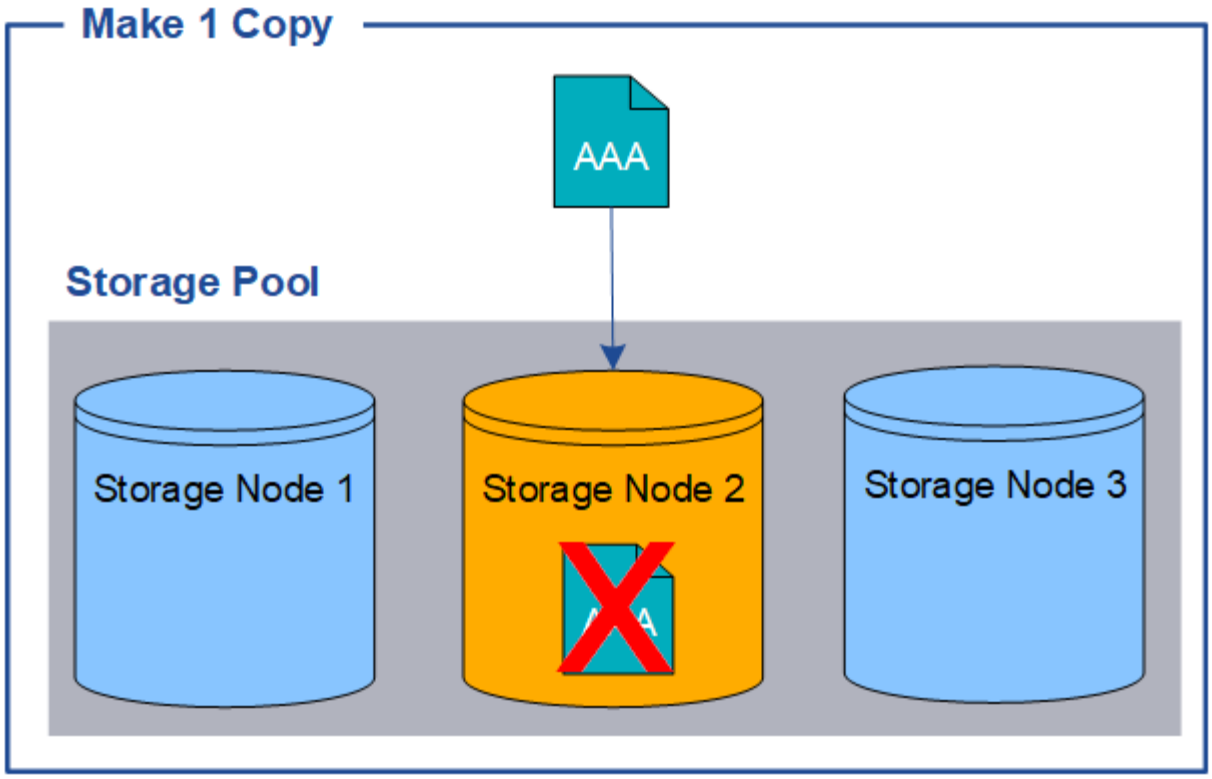
Al crear una regla de ILM para crear copias replicadas, debe especificar siempre al menos dos copias durante cualquier periodo de tiempo en las instrucciones de ubicación.

No utilice una regla de ILM que cree solo una copia replicada durante un período de tiempo. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

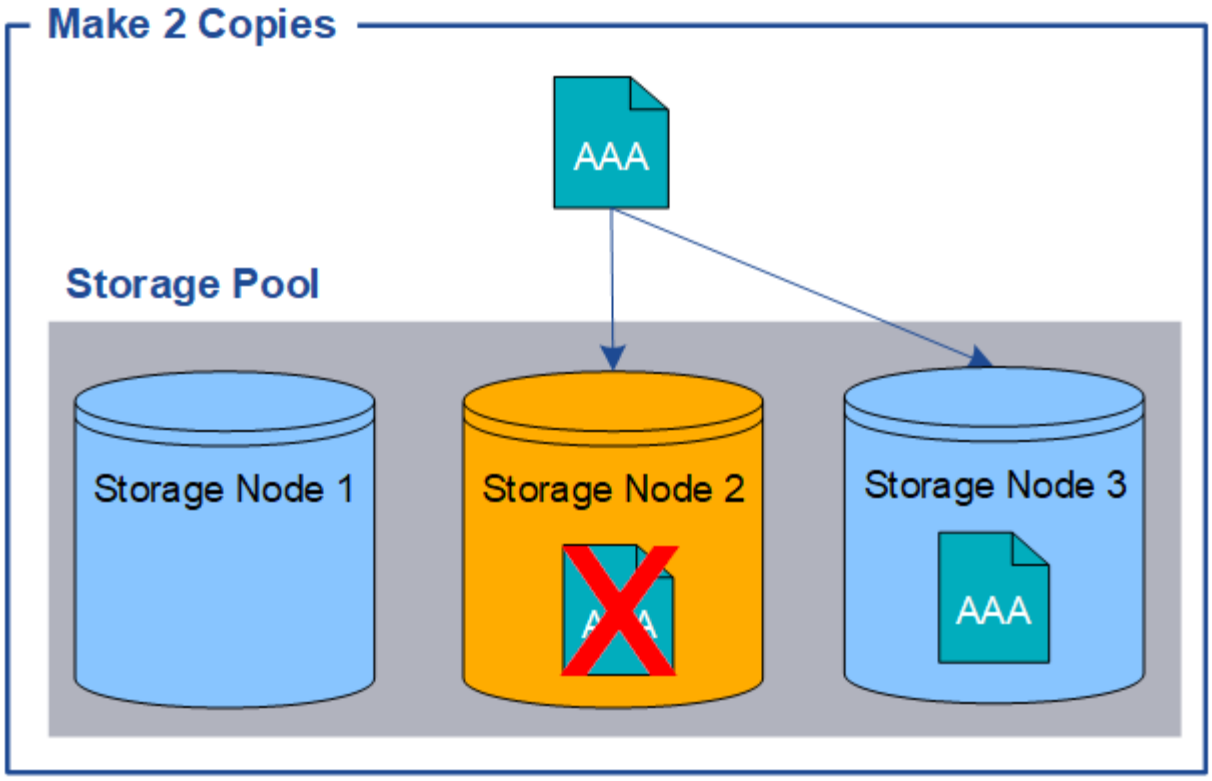
En el ejemplo siguiente, la regla Make 1 Copy ILM especifica que una copia replicada de un objeto se coloca en un pool de almacenamiento que contiene tres nodos de almacenamiento. Cuando se ingiere un objeto que coincida con esta regla, StorageGRID coloca una sola copia en un solo nodo de almacenamiento.



Cuando una regla de ILM crea solo una copia replicada de un objeto, se vuelve inaccesible cuando el nodo de almacenamiento no está disponible. En este ejemplo, perderá temporalmente el acceso al objeto AAA siempre que el nodo de almacenamiento 2 esté desconectado, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA completamente si falla el nodo de almacenamiento 2.



Para evitar la pérdida de datos de objetos, siempre debe realizar al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, puede seguir teniendo acceso al objeto si un nodo de almacenamiento falla o se desconecta.



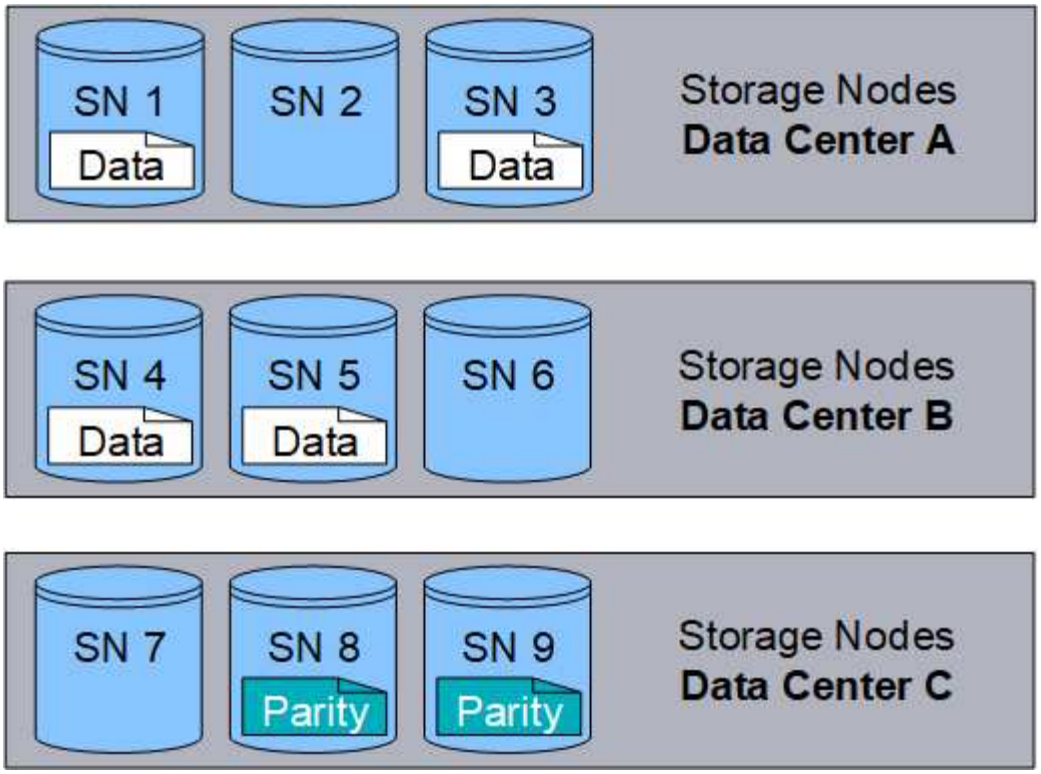
¿Qué es el código de borrado?

El código de borrado es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos. Cuando los objetos coinciden con una regla de ILM que utiliza código de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

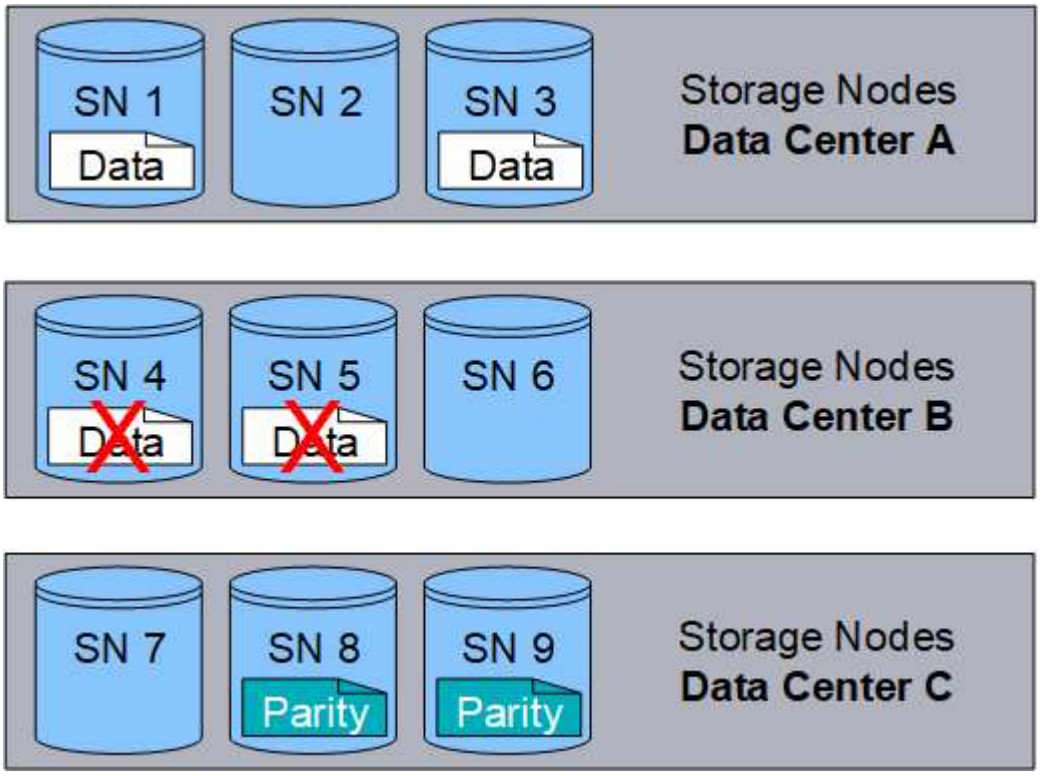
Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un dato o un fragmento de paridad se corrompen o se pierden, el algoritmo de código de borrado puede recrear ese fragmento con un subconjunto de los datos restantes y los fragmentos de paridad.

Al crear reglas de ILM, StorageGRID crea perfiles de código de borrado que admiten esas reglas. Puede ver una lista de perfiles de codificación de borrado, "cambie el nombre de un perfil de código de borrado", o. "Desactive un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM".

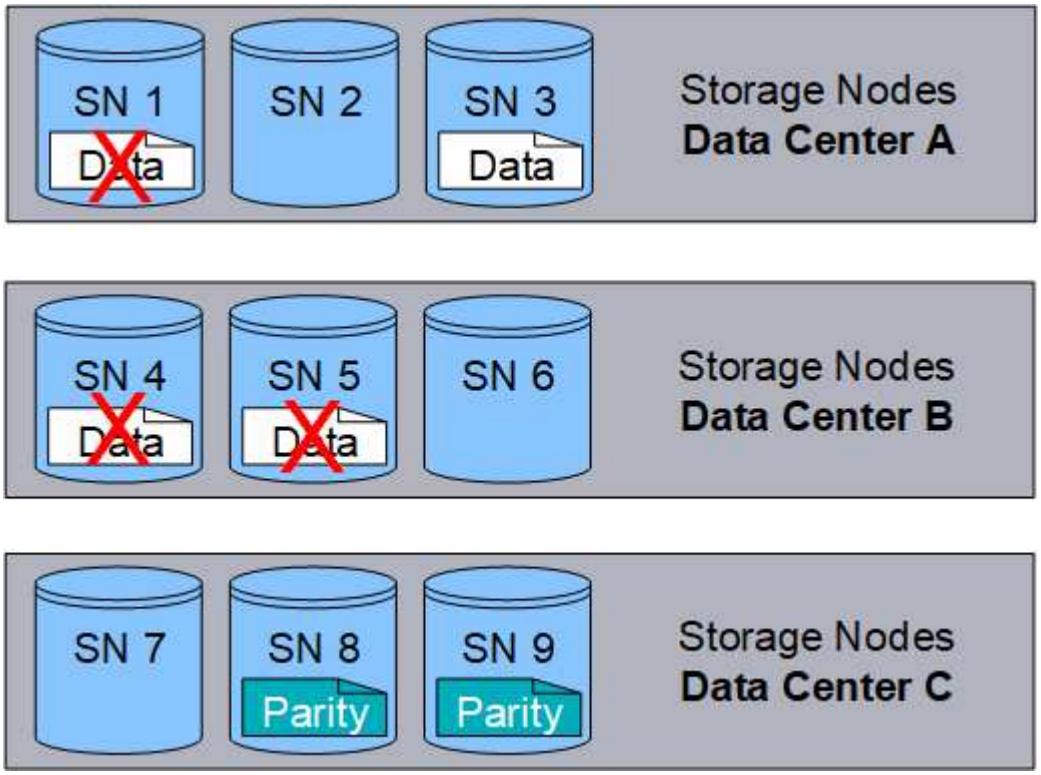
En el siguiente ejemplo, se muestra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir de los datos del objeto. Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centro de datos para proporcionar protección de datos ante fallos de nodos o pérdidas de sitios.



El esquema de codificación de borrado 4+2 se puede configurar de varias maneras. Por ejemplo, puede configurar un pool de almacenamiento de un único sitio que contenga seis nodos de almacenamiento. Para "protección contra pérdida de sitios", Puede utilizar un pool de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Un objeto se puede recuperar siempre que cuatro de los seis fragmentos (datos o paridad) permanezcan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio entero, el objeto aún puede recuperarse o repararse, siempre que se pueda acceder a todos los demás fragmentos.



Si se pierden más de dos nodos de almacenamiento, el objeto no se puede recuperar.



Información relacionada

- "¿Qué es la replicación?"
- "¿Qué es un pool de almacenamiento?"
- "¿Qué son los esquemas de código de borrado?"
- "Cambie el nombre de un perfil de código de borrado"
- "Desactivar un perfil de código de borrado"

¿Qué son los esquemas de código de borrado?

Los esquemas de codificación de borrado controlan cuántos fragmentos de datos se crean y cuántos fragmentos de paridad se crean para cada objeto.

Cuando configura el perfil de código de borrado para una regla de ILM, debe seleccionar un esquema de código de borrado disponible en función del número de nodos de almacenamiento y sitios que componen el pool de almacenamiento que piensa usar.

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo divide un objeto en `k` fragmentos de datos y cálculos `m` fragmentos de paridad. La `k + m = n` los fragmentos se distribuyen `n` Nodos de almacenamiento para proporcionar protección de datos. Un objeto puede soportar hasta `m` fragmentos perdidos o corruptos. Para recuperar o reparar un objeto, `k` se necesitan fragmentos.

Cuando seleccione el pool de almacenamiento que se utilizará en una regla que creará una copia con código de borrado, utilice las siguientes directrices para los pools de almacenamiento:

- El pool de almacenamiento debe incluir tres o más sitios, o exactamente un sitio.

No se puede usar código de borrado si el pool de almacenamiento incluye dos sitios.

  - Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios
  - Esquemas de codificación de borrado para pools de almacenamiento in situ

- No utilice un pool de almacenamiento que incluya el sitio predeterminado, Todos los sitios.
- El pool de almacenamiento debe incluir al menos *k+m* +1 Nodos de almacenamiento.

  El número mínimo necesario de nodos de almacenamiento es k+m. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a evitar fallos de ingesta o errores de gestión de la vida útil si un nodo de almacenamiento necesario no está disponible temporalmente.

La sobrecarga de almacenamiento de un esquema de código de borrado se calcula dividiendo el número de fragmentos de paridad (m) por el número de fragmentos de datos (k). Puede utilizar la sobrecarga del almacenamiento para calcular cuánto espacio en disco necesita cada objeto con código de borrado:

*disk space = object size + (object size * storage overhead)*

Por ejemplo, si almacena un objeto de 10 MB mediante el esquema 4+2 (que tiene un 50% de sobrecarga de almacenamiento), el objeto consume 15 MB de almacenamiento de cuadrícula. Si almacena el mismo objeto de 10 MB con el esquema 6+2 (que tiene un 33% de sobrecarga de almacenamiento), el objeto consume aproximadamente 13.3 MB.

Seleccione el esquema de código de borrado que tenga el valor total más bajo de k+m que satisface sus necesidades. Los esquemas de código de borrado con un número menor de fragmentos por lo general son más eficientes computacionalmente, ya que se crean y distribuyen menos fragmentos (o se recuperan) por objeto, pueden ofrecer un mejor rendimiento debido al tamaño de fragmento más grande y pueden requerir que se añadan menos nodos en una expansión cuando se necesita más almacenamiento. (Para obtener información sobre cómo planificar una expansión de almacenamiento, consulte "Instrucciones para ampliar StorageGRID".)

Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios

En la siguiente tabla se describen los esquemas de codificación de borrado que admite actualmente StorageGRID para pools de almacenamiento que incluyen tres o más sitios. Todos estos esquemas proporcionan protección contra pérdida de sitio. Se puede perder un sitio y el objeto seguirá siendo accesible.

Para esquemas de código de borrado que ofrecen protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el pool de almacenamiento supera *k+m* +1 Dado que cada sitio requiere un mínimo de tres nodos de almacenamiento.

Esquema de codificación de borrado (*k+m*)	Número mínimo de sitios implementados	Número recomendado de nodos de almacenamiento en cada sitio	Número total recomendado de nodos de almacenamiento	¿Protección contra pérdida de sitio?	Gastos generales de almacenamiento
4+2	3	3	9	Sí	50 %
6+2	4	3	12	Sí	33 %

Esquema de codificación de borrado (*k*+*m*)	Número mínimo de sitios implementados	Número recomendado de nodos de almacenamiento en cada sitio	Número total recomendado de nodos de almacenamiento	¿Protección contra pérdida de sitio?	Gastos generales de almacenamiento
8+2	5	3	15	Sí	25 %
6+3	3	4	12	Sí	50 %
9+3	4	4	16	Sí	33 %
2+1	3	3	9	Sí	50 %
4+1	5	3	15	Sí	25 %
6+1	7	3	21	Sí	17 %
7+5	3	5	15	Sí	71 %

> StorageGRID requiere un mínimo de tres nodos de almacenamiento por sitio. Para utilizar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda usar cinco nodos de almacenamiento por sitio.

Al seleccionar un esquema de codificación de borrado que proporcione protección al sitio, equilibre la importancia relativa de los siguientes factores:

- **Número de fragmentos**: El rendimiento y la flexibilidad de expansión son generalmente mejores cuando el número total de fragmentos es menor.
- **Tolerancia a fallos**: La tolerancia a fallos se incrementa al tener más segmentos de paridad (es decir, cuando `m` tiene un valor más alto.)
- **Tráfico de red**: Al recuperarse de fallos, utilizando un esquema con más fragmentos (es decir, un total más alto para `k+m`) crea más tráfico de red.
- **Gastos generales de almacenamiento**: Los esquemas con mayor sobrecarga requieren más espacio de almacenamiento por objeto.

Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3 (que ambos tienen un 50% de gastos generales de almacenamiento), seleccione el esquema 6+3 si se requiere tolerancia a fallos adicional. Seleccione el esquema 4+2 si los recursos de red están limitados. Si todos los demás factores son iguales, seleccione 4+2 porque tiene un número total menor de fragmentos.

> Si no está seguro de qué esquema usar, seleccione 4+2 o 6+3, o póngase en contacto con el servicio de asistencia técnica.

Esquemas de codificación de borrado para pools de almacenamiento in situ

Un pool de almacenamiento in situ admite todos los esquemas de codificación de borrado definidos para tres o más sitios, siempre y cuando el sitio tenga suficientes nodos de almacenamiento.

El número mínimo necesario de nodos de almacenamiento es `k+m`, pero una piscina de almacenamiento con `k+m +1` Se recomiendan los nodos de almacenamiento. Por ejemplo, el esquema de codificación de borrado 2+1 requiere un pool de almacenamiento con un mínimo de tres nodos de almacenamiento, pero se recomiendan cuatro nodos de almacenamiento.

Esquema de codificación de borrado (*k+m*)	Número mínimo de nodos de almacenamiento	Número recomendado de nodos de almacenamiento	Gastos generales de almacenamiento
4+2	6	7	50 %
6+2	8	9	33 %
8+2	10	11	25 %
6+3	9	10	50 %
9+3	12	13	33 %
2+1	3	4	50 %
4+1	5	6	25 %
6+1	7	8	17 %
7+5	12	13	71 %

Ventajas, desventajas y requisitos de codificación de borrado

Antes de decidir si se debe utilizar la replicación o el código de borrado para proteger los datos de objetos frente a pérdidas, debe comprender las ventajas, las desventajas y los requisitos para la codificación de borrado.

Ventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado ofrece una mayor fiabilidad, disponibilidad y eficiencia del almacenamiento.

- **Confiabilidad**: La fiabilidad se mide en términos de tolerancia a fallos, es decir, el número de fallos simultáneos que se pueden sostener sin pérdida de datos. Con la replicación, se almacenan varias copias idénticas en diferentes nodos y entre sitios. Con el código de borrado, un objeto se codifica en fragmentos de datos y de paridad, y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección frente a fallos del sitio y del nodo. En comparación con la replicación, la codificación de borrado proporciona una mayor fiabilidad con costes de almacenamiento comparables.
- **Disponibilidad**: La disponibilidad se puede definir como la capacidad de recuperar objetos si los nodos de almacenamiento fallan o se vuelven inaccesibles. En comparación con la replicación, la codificación de borrado proporciona una mayor disponibilidad con costes de almacenamiento comparables.
- **Eficiencia del almacenamiento**: Para niveles similares de disponibilidad y fiabilidad, los objetos protegidos mediante codificación de borrado consumen menos espacio en disco que los mismos objetos si

están protegidos mediante replicación. Por ejemplo, un objeto de 10 MB que se replica en dos sitios consume 20 MB de espacio en disco (dos copias), mientras que un objeto que se elimina en tres sitios con un esquema de codificación de borrado 6+3 solo consume 15 MB de espacio en disco.

> El espacio en disco para los objetos codificados de borrado se calcula como el tamaño del objeto más la sobrecarga del almacenamiento. El porcentaje de sobrecarga del almacenamiento es el número de fragmentos de paridad dividido por el número de fragmentos de datos.

Desventajas del código de borrado

En comparación con la replicación, los códigos de borrado tienen las siguientes desventajas:

- Se recomienda un mayor número de nodos de almacenamiento y sitios, en función del esquema de código de borrado. Por el contrario, si replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia. Consulte "Esquemas de código de borrado para pools de almacenamiento que contienen tres o más sitios" y.. "Esquemas de código de borrado para pools de almacenamiento de un sitio".
- Aumento del coste y de la complejidad de las ampliaciones del almacenamiento. Para expandir una implementación que utiliza replicación, debe agregar capacidad de almacenamiento en cada ubicación donde se realicen copias de objetos. Para ampliar una puesta en marcha que utilice código de borrado, debe tener en cuenta el esquema de codificación de borrado y el grado de llenado de los nodos de almacenamiento existentes. Por ejemplo, si espera a que los nodos existentes estén llenos al 100 %, debe agregar al menos `k+m` Nodos de almacenamiento, pero si amplía cuando los nodos existentes estén llenos al 70 %, puede añadir dos nodos por sitio y seguir maximizando la capacidad de almacenamiento útil. Para obtener más información, consulte "Añada capacidad de almacenamiento para objetos codificados de borrado".
- Al utilizar códigos de borrado en ubicaciones distribuidas geográficamente, aumenta la latencia de recuperación. Los fragmentos de objeto para un objeto que se codifica con borrado y se distribuyen en sitios remotos tardan más en recuperarse a través de conexiones WAN que los objetos que se replican y están disponibles localmente (el mismo sitio al que se conecta el cliente).
- Al utilizar la codificación de borrado en ubicaciones distribuidas geográficamente, se está utilizando más el tráfico de red WAN para restauraciones y reparaciones, especialmente en objetos que se recuperan con frecuencia o para reparaciones de objetos a través de conexiones de red WAN.
- Cuando se utiliza la codificación de borrado en varios sitios, el rendimiento máximo del objeto se reduce drásticamente a medida que aumenta la latencia de red entre sitios. Esta disminución se debe a la correspondiente disminución del rendimiento de la red TCP, que afecta a la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objeto.
- Mayor uso de recursos de computación.

Cuándo se debe utilizar la codificación de borrado

El código de borrado se ajusta mejor a los siguientes requisitos:

- Los objetos tienen un tamaño superior a 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

- Almacenamiento a largo plazo o en frío para contenido que se recupera con poca frecuencia.

- Alta disponibilidad y fiabilidad de los datos.
- Protección frente a fallos completos de sitios y nodos.
- Eficiencia del almacenamiento.
- Puestas en marcha de un único sitio que requieren protección de datos eficiente con solo una copia codificada por borrado en lugar de múltiples copias replicadas.
- Puestas en marcha de varios sitios en las que la latencia entre sitios es inferior a 100 ms.

Cómo se determina la retención de objetos

StorageGRID ofrece opciones tanto para los administradores de grid como para los usuarios individuales de inquilino para especificar el tiempo que se tarda en almacenar los objetos. En general, cualquier instrucción de retención proporcionada por un usuario inquilino tiene prioridad sobre las instrucciones de retención proporcionadas por el administrador de grid.

Cómo los usuarios de inquilinos controlan la retención de objetos

Los usuarios de inquilinos tienen tres formas principales de controlar cuánto tiempo se almacenan los objetos en StorageGRID:

- Si la configuración global de Object Lock está habilitada para el grid, los usuarios inquilinos S3 pueden crear bloques con S3 Object Lock habilitado y, a continuación, utilizar la API REST de S3 para especificar la configuración de retención hasta la fecha y la conservación legal de cada versión de objeto añadida a ese bloque.
  - Una versión de objeto que está bajo una conservación legal no se puede eliminar con ningún método.
  - Antes de que se alcance la fecha de retención hasta la versión de un objeto, esa versión no se puede eliminar con ningún método.
  - Los objetos en bloques con S3 Object Lock habilitado son mantenidos por ILM "'eternamente'". Sin embargo, una vez alcanzada la fecha de retención hasta la fecha, una solicitud de cliente puede eliminar una versión de objeto o la expiración del ciclo de vida de la cuchara. Consulte "Gestione objetos con S3 Object Lock".
- Los usuarios de inquilinos S3 pueden añadir una configuración del ciclo de vida a sus bloques que especifica una acción de caducidad. Si existe un ciclo de vida de un bloque, StorageGRID almacena un objeto hasta que se cumpla la fecha o el número de días especificados en la acción Expiración, a menos que el cliente elimine primero el objeto. Consulte "Cree una configuración del ciclo de vida de S3".
- Un cliente S3 o Swift puede emitir una solicitud de eliminación de objeto. StorageGRID siempre prioriza las solicitudes de eliminación de clientes por encima del ciclo de vida de los bloques S3 o ILM al determinar si se debe eliminar o conservar un objeto.

Cómo los administradores de grid controlan la retención de objetos

Los administradores de grid utilizan las instrucciones de colocación de ILM para controlar la duración de los objetos almacenados. Cuando una regla de ILM coincide con los objetos, StorageGRID almacena esos objetos hasta que haya transcurrido el último periodo de tiempo de la regla de ILM. Los objetos se conservan indefinidamente si se especifica "'eternamente'" para las instrucciones de colocación.

Independientemente de quién controle cuánto tiempo se retienen los objetos, la configuración de ILM controla qué tipos de copias de objetos (replicadas o codificadas de borrado) se almacenan y dónde se encuentran las copias (nodos de almacenamiento, pools de almacenamiento en cloud o nodos de archivado).

Cómo interaccionan el ciclo de vida de bloque y ILM de S3

La acción de caducidad en un ciclo de vida de bloque de S3 siempre anula la configuración de ILM. Como resultado, es posible que un objeto se conserve en la cuadrícula aunque hayan caducado las instrucciones de gestión del ciclo de vida de la información relativas a la ubicación del objeto.

Ejemplos para la retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, la configuración del ciclo de vida de bloques, las solicitudes de eliminación de clientes y ILM, tenga en cuenta los siguientes ejemplos.

Ejemplo 1: El ciclo de vida de un bloque de S3 mantiene los objetos durante más tiempo que ILM

ILM

Almacene dos copias por 1 año (365 días)

Ciclo de vida del cucharón

Caducidad de objetos en 2 años (730 días)

Resultado

StorageGRID almacena el objeto durante 730 días. StorageGRID utiliza la configuración del ciclo de vida de los bloques para determinar si se debe eliminar o conservar un objeto.

> Si el ciclo de vida de un bloque especifica que los objetos se deben conservar durante más tiempo del ciclo de vida de la información especificado por ILM, StorageGRID sigue usando las instrucciones de colocación de ILM al determinar el número y el tipo de copias que se deben almacenar. En este ejemplo, se seguirán almacenando dos copias del objeto en StorageGRID de los días 366 a 730.

Ejemplo 2: El ciclo de vida de bloque de S3 caduca los objetos antes de ILM

ILM

Almacene dos copias durante 2 años (730 días)

Ciclo de vida del cucharón

Caducar objetos en un año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: La eliminación de clientes anula el ciclo de vida del bloque y el ILM

ILM

Almacenar dos copias en nodos de almacenamiento «para siempre»

Ciclo de vida del cucharón

Caducidad de objetos en 2 años (730 días)

Solicitud de eliminación de cliente

Emitido el día 400

Resultado

StorageGRID elimina ambas copias del objeto el día 400 en respuesta a la solicitud de eliminación del cliente.

Ejemplo 4: El bloqueo de objetos S3 anula la solicitud de eliminación del cliente

Bloqueo de objetos de S3

La fecha de retención hasta la versión de un objeto es 2026-03-31. No existe un derecho legal.

Regla de ILM que cumpla con las normativas

Almacenar dos copias en nodos de almacenamiento «para siempre».

Solicitud de eliminación de cliente

Emitido el 2024-03-31.

Resultado

StorageGRID no eliminará la versión del objeto porque la fecha de retención hasta todavía está a 2 años.

Cómo se eliminan los objetos

StorageGRID puede eliminar objetos en respuesta directa a una solicitud del cliente o de forma automática como resultado del vencimiento del ciclo de vida de un bloque de S3 o de los requisitos de la política de ILM. Comprender las diferentes formas en que se pueden eliminar los objetos y el modo en que StorageGRID gestiona las solicitudes de eliminación puede ayudarle a gestionar los objetos de forma más eficaz.

StorageGRID puede utilizar uno de estos dos métodos para eliminar objetos:

- Eliminación síncrona: Cuando StorageGRID recibe una solicitud de eliminación de cliente, todas las copias de los objetos se eliminan de inmediato. Se informa al cliente de que la eliminación se ha realizado correctamente una vez eliminadas las copias.
- Los objetos se ponen en cola para eliminación: Cuando StorageGRID recibe una solicitud de eliminación, el objeto se pone en cola para su eliminación y se informa al cliente inmediatamente de que esta se ha eliminado correctamente. Las copias de objetos se eliminan más adelante mediante el procesamiento de ILM en segundo plano.

Cuando se eliminan objetos, StorageGRID utiliza el método que optimiza el rendimiento de eliminación, minimiza las posibles acumulaciones de eliminación y libera espacio que se libera con mayor rapidez.

La tabla resume cuándo StorageGRID utiliza cada método.

Método de eliminación	Cuando se utilice
Los objetos se mantienen en la cola para su eliminación	Cuando **cualquiera** de las siguientes condiciones se cumple: • La eliminación automática de objetos ha sido activada por uno de los siguientes eventos: ◦ Se ha alcanzado la fecha de caducidad o el número de días en la configuración del ciclo de vida de un bloque de S3. ◦ El último periodo de tiempo especificado en una regla de ILM transcurre. **Nota:** Los objetos en un depósito que tiene S3 Object Lock habilitado no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención hasta la fecha pero aún no se cumplen. • Un cliente de S3 o Swift solicita la eliminación y se debe cumplir una o varias de estas condiciones: ◦ Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, una ubicación de objetos no está disponible en este momento. ◦ Las colas de eliminación en segundo plano están inactivas.
Los objetos se quitan de inmediato (eliminación síncrona)	Cuando un cliente S3 o Swift realiza una solicitud de eliminación y **se cumplen todas** las siguientes condiciones: • Todas las copias se pueden eliminar en 30 segundos. • Las colas de eliminación en segundo plano contienen objetos que se van a procesar.

Cuando los clientes S3 o Swift realizan solicitudes de eliminación, StorageGRID empieza añadiendo objetos a la cola de eliminación. A continuación, cambia a realizar una eliminación síncrona. Asegurarse de que la cola de eliminación en segundo plano tiene objetos que procesar permite a StorageGRID procesar las eliminaciones de forma más eficaz, especialmente en los clientes de baja concurrencia, mientras que ayuda a evitar que los clientes eliminen las copias de seguridad.

Tiempo necesario para eliminar objetos

La forma en que StorageGRID elimina los objetos puede afectar a la forma en la que aparece el sistema:

- Cuando StorageGRID realiza la eliminación síncrona, StorageGRID puede tardar hasta 30 segundos en devolver un resultado al cliente. Esto significa que la eliminación puede parecer más lenta, aunque en realidad se eliminan copias más rápidamente de lo que están cuando StorageGRID pone en cola objetos para su eliminación.
- Si supervisa de cerca el rendimiento de eliminación durante una eliminación masiva, puede observar que la tasa de eliminación aparece como lenta después de eliminar un cierto número de objetos. Este cambio ocurre cuando StorageGRID pasa de poner objetos en cola para su eliminación a realizar una eliminación síncrona. La reducción aparente en la tasa de eliminación no significa que las copias de objetos se van a eliminar más lentamente. Por el contrario, indica que, en promedio, ahora se libera espacio con más rapidez.

Si elimina un gran número de objetos y la prioridad es liberar espacio rápidamente, considere la posibilidad de usar una solicitud de cliente para eliminar objetos en lugar de eliminarlos con ILM u otros métodos. En general, el espacio se libera más rápidamente cuando los clientes lo eliminan, ya que StorageGRID puede utilizar la eliminación síncrona.

La cantidad de tiempo necesario para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de objetos se eliminan de forma síncrona o se ponen en cola para su eliminación más adelante (para solicitudes de eliminación de clientes).
- Otros factores, como el número de objetos de la cuadrícula o la disponibilidad de los recursos de grid cuando las copias de objetos se colocan en cola para su eliminación (tanto para los eliminaciones del cliente como para otros métodos).

Cómo se eliminan los objetos con versiones de S3

Cuando se habilita el control de versiones para un bloque de S3, StorageGRID sigue el comportamiento de Amazon S3 al responder a las solicitudes de eliminación, ya provenga de un cliente S3, el vencimiento de un ciclo de vida de un bloque de S3 o los requisitos de la política de ILM.

Cuando los objetos se versionan, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto y no liberan espacio. En su lugar, una solicitud de eliminación de objetos crea un marcador de eliminación como la versión actual del objeto, lo que hace que la versión anterior del objeto sea “no actual”.

Aunque el objeto no se haya quitado, StorageGRID se comporta como si la versión actual del objeto ya no estuviera disponible. Las solicitudes a ese objeto devuelven 404 NotFound. Sin embargo, debido a que los datos de objeto no actuales no se han eliminado, las solicitudes que especifican una versión no actual del objeto pueden tener éxito.

Para liberar espacio al suprimir objetos con versiones, utilice una de las siguientes opciones:

- **Solicitud de cliente S3**: Especifique el ID de versión de objeto en la solicitud de ELIMINACIÓN DE objeto S3 (`DELETE /object?versionId=ID`). Tenga en cuenta que esta solicitud sólo elimina copias de objetos para la versión especificada (las otras versiones todavía ocupan espacio).
- **Ciclo de vida del cucharón**: Utilice `NoncurrentVersionExpiration` acción en la configuración del ciclo de vida del bloque. Cuando se cumple el número de días sin currentDays especificado, StorageGRID elimina permanentemente todas las copias de las versiones de objetos no actuales. Estas versiones de objetos no se pueden recuperar.

  La `NewerNoncurrentVersions` La acción en la configuración del ciclo de vida del bloque especifica el número de versiones no actuales retenidas en un segmento S3 con versiones. Si hay más versiones no corrientes que `NewerNoncurrentVersions` Especifica, StorageGRID elimina las versiones anteriores una vez transcurrido el valor NoncurrentDays. La `NewerNoncurrentVersions` El umbral anula las reglas de ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del `NewerNoncurrentVersions` El umbral se conserva si ILM solicita su eliminación.

- **ILM**: "Clone la política activa" Y añada dos reglas de ILM a la nueva política propuesta:
  - Primera regla: Use “Tiempo no corriente” como el Tiempo de referencia para coincidir con las versiones no actuales del objeto. Pulg "Paso 1 (introduzca detalles) del asistente Create an ILM Rule", Seleccione **Sí** para la pregunta, “`Aplica esta regla solo a versiones de objetos más antiguas (en cubos S3 con control de versiones activado)?”
  - Segunda regla: Utilice **tiempo de ingesta** para que coincida con la versión actual. La regla “Tiempo no corriente” debe aparecer en la política sobre la regla **Tiempo de ingesta**.

Cómo se eliminan los marcadores de borrado de S3

Cuando se elimina un objeto versionado, StorageGRID crea un marcador de eliminación como la versión actual del objeto. Para eliminar el marcador de eliminación de cero bytes del depósito, el cliente S3 debe eliminar explícitamente la versión del objeto. ILM, las reglas de ciclo de vida de los bloques no se quitan los marcadores de eliminación ni los objetos de las operaciones de bloque.

Información relacionada

- "USE LA API DE REST DE S3"
- "Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3"

Crear y asignar grados de almacenamiento

Los grados de almacenamiento identifican el tipo de almacenamiento que utiliza un nodo de almacenamiento. Puede crear grados de almacenamiento si desea que las reglas de ILM coloquen determinados objetos en ciertos nodos de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

Cuando instala StorageGRID por primera vez, el grado de almacenamiento **default** se asigna automáticamente a cada nodo de almacenamiento en su sistema. Como sea necesario, puede definir opcionalmente grados de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

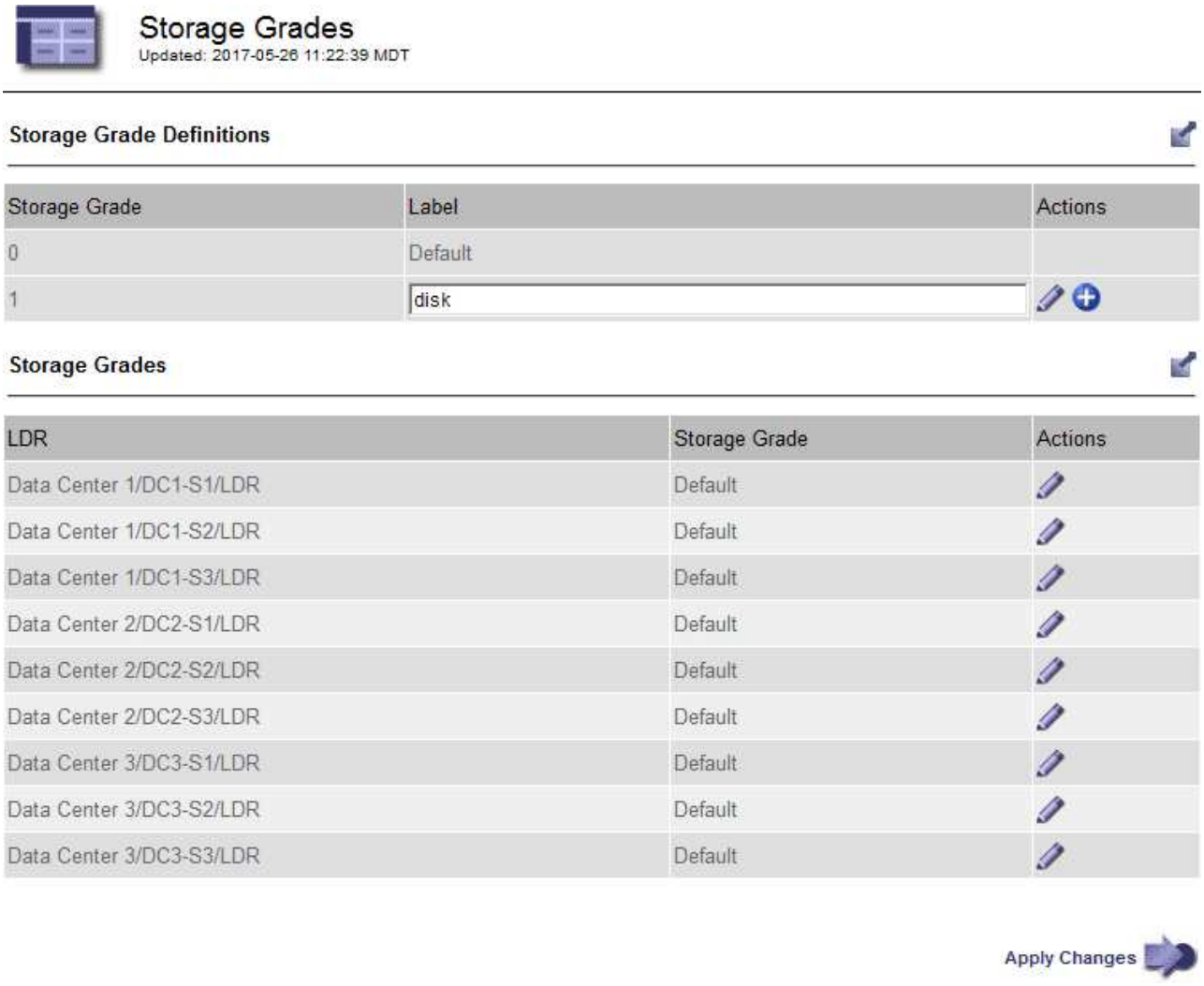
El uso de grados de almacenamiento personalizados permite crear pools de almacenamiento ILM que contienen solo un tipo específico de nodo de almacenamiento. Por ejemplo, quizás desee almacenar determinados objetos en los nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash StorageGRID.

Si el grado de almacenamiento no es una preocupación (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y usar la selección **Incluye todos los grados de almacenamiento** para el grado de almacenamiento cuando usted "cree pools de almacenamiento". El uso de esta selección garantiza que el pool de almacenamiento incluirá todos los nodos de almacenamiento en el sitio, independientemente de su grado de almacenamiento.

> No cree más grados de almacenamiento de los necesarios. Por ejemplo, no cree una categoría de almacenamiento para cada nodo de almacenamiento. En su lugar, asigne cada grado de almacenamiento a dos o más nodos. Las leyes de almacenamiento asignadas a un solo nodo pueden provocar reversiones de ILM si ese nodo deja de estar disponible.

Pasos

1. Seleccione **ILM** > **grados de almacenamiento**.
2. Definir grados de almacenamiento personalizados:
   a. Para cada grado de almacenamiento personalizado que desee agregar, seleccione **Insertar** para agregar una fila.
   b. Introduzca una etiqueta descriptiva.



c. Seleccione **aplicar cambios**.

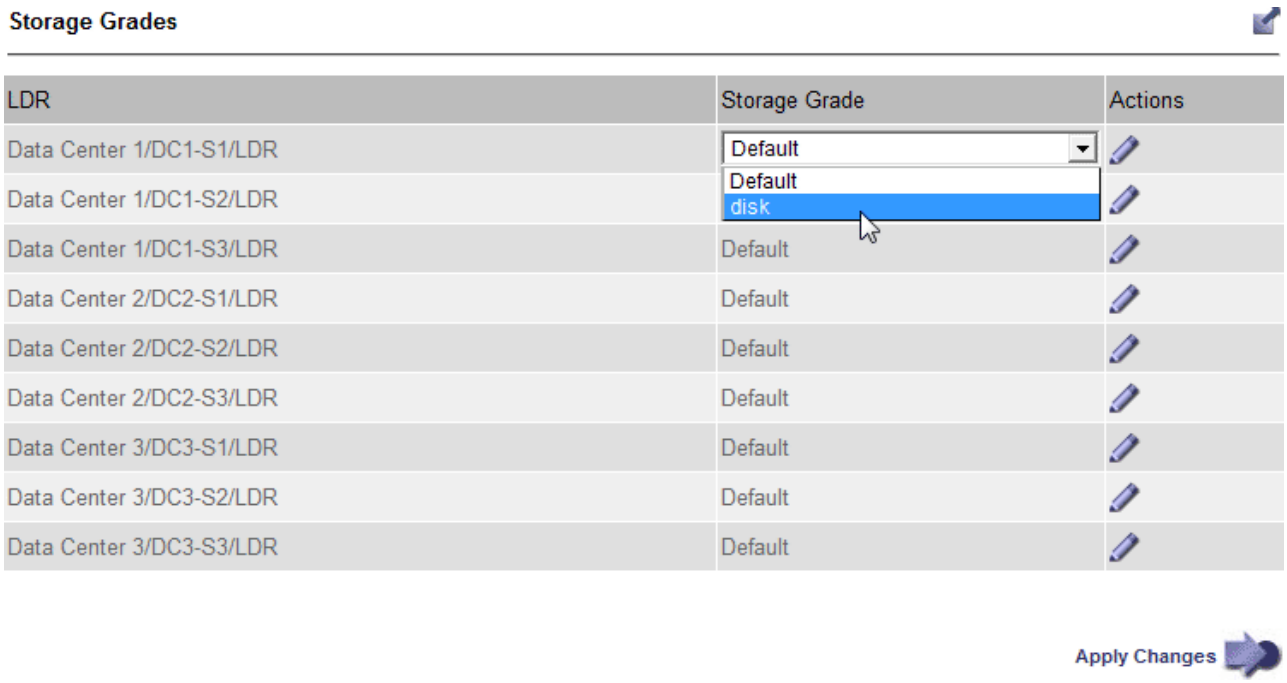
d. Opcionalmente, si necesita modificar una etiqueta guardada, seleccione **Editar** Y selecciona **Aplicar cambios**.

> No se pueden eliminar los grados de almacenamiento.

3. Asigne nuevos grados de almacenamiento a los nodos de almacenamiento:

a. Localice el nodo de almacenamiento en la lista LDR y seleccione su icono **Editar** .

b. Seleccione el grado de almacenamiento adecuado en la lista.



> Asigne un nivel de almacenamiento solo una vez a un nodo de almacenamiento determinado. Un nodo de almacenamiento recuperado del error mantiene el grado de almacenamiento anteriormente asignado. No cambie esta asignación después de activar la política de ILM. Si se modifica la asignación, los datos se almacenan según el nuevo grado de almacenamiento.

a. Seleccione **aplicar cambios**.

Usar pools de almacenamiento

¿Qué es un pool de almacenamiento?

Un pool de almacenamiento es una agrupación lógica de nodos de almacenamiento o nodos de archivado.

Al instalar StorageGRID, se crea automáticamente un pool de almacenamiento por sitio. Es posible configurar pools de almacenamiento adicionales según sea necesario para cumplir sus requisitos de almacenamiento.

> La compatibilidad con los nodos de archivo (tanto para archivar en la nube mediante la API S3 como para archivar en cinta mediante el middleware TSM) está obsoleta y se eliminará en una versión futura. Mover objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo ha sido reemplazado por ILM Cloud Storage Pools, que ofrecen más funcionalidad.
>
> Consulte "Utilice Cloud Storage Pools".

Los pools de almacenamiento tienen dos atributos:

- **Grado de almacenamiento**: Para nodos de almacenamiento, el rendimiento relativo del almacenamiento de respaldo.
- **Sitio**: El centro de datos donde se almacenarán los objetos.

Los pools de almacenamiento se utilizan en las reglas de ILM para determinar dónde se almacenan los datos de objetos y el tipo de almacenamiento utilizado. Cuando se configuran las reglas de ILM para la replicación, se deben seleccionar uno o varios pools de almacenamiento que incluyen nodos de almacenamiento o nodos de archivado. Cuando se crean perfiles de código de borrado, se selecciona un pool de almacenamiento que incluye nodos de almacenamiento.

Directrices para crear pools de almacenamiento

Configura y utiliza pools de almacenamiento para protegerse frente a la pérdida de datos distribuyendo los datos entre varios sitios. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de pools de almacenamiento.

Consulte "Ejemplos de habilitación de la protección contra pérdida de sitios mediante replicación y código de borrado".

Directrices para todos los pools de almacenamiento

- Mantenga las configuraciones del pool de almacenamiento de la forma más sencilla posible. No cree más pools de almacenamiento de los necesarios.
- Cree pools de almacenamiento con tantos nodos como sea posible. Cada pool de almacenamiento debe contener dos o más nodos. Un pool de almacenamiento con nodos insuficientes puede provocar registros de gestión del ciclo de vida de la información si un nodo deja de estar disponible.
- Evite crear o usar pools de almacenamiento que se solapen (contienen uno o varios de los mismos nodos). Si los pools de almacenamiento se solapan, es posible que se guarden más de una copia de datos de objetos en el mismo nodo.
- En general, no use el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) ni el sitio Todos los sitios. Estos elementos se actualizan automáticamente para incluir los nuevos sitios que agregue en una expansión, lo cual podría no ser el comportamiento que desea.

Directrices para los pools de almacenamiento utilizados para copias replicadas

- De protección contra pérdida de sitio con "replicación", especifique uno o más pools de almacenamiento específicos del sitio en la "Instrucciones de colocación para cada regla de ILM".

  Se crea automáticamente un pool de almacenamiento para cada sitio durante la instalación de StorageGRID.

  El uso de un pool de almacenamiento para cada sitio garantiza que las copias de objetos replicados se coloquen exactamente donde se espere (por ejemplo, una copia de cada objeto en cada sitio para la protección frente a pérdida de sitio).

- Si agrega un sitio en una expansión, cree un nuevo pool de almacenamiento que contenga solo el nuevo sitio. A continuación, "Actualice las reglas de ILM" para controlar qué objetos se almacenan en el nuevo sitio.
- Si la cantidad de copias es inferior a la cantidad de pools de almacenamiento, el sistema distribuye las copias para equilibrar el uso de disco entre los pools.
- Si los pools de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden en un solo sitio. Debe asegurarse de que los pools de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Directrices para los pools de almacenamiento utilizados para las copias con código de borrado

- De protección contra pérdida de sitio con "código de borrado", cree pools de almacenamiento que consten de al menos tres sitios. Si un pool de almacenamiento incluye solo dos sitios, no puede usar ese pool de almacenamiento para el código de borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.
- La cantidad de nodos de almacenamiento y sitios incluidos en el pool de almacenamiento determina cuáles "esquemas de código de borrado" están disponibles.
- Si es posible, un pool de almacenamiento debe incluir más de la cantidad mínima de nodos de almacenamiento necesarios para el esquema de codificación de borrado que seleccione. Por ejemplo, si utiliza un esquema de codificación de borrado 6+3, debe contar con al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuya nodos de almacenamiento en todos los sitios de la forma más equitativa posible. Por ejemplo, para admitir un esquema de codificación de borrado 6+3, configure un pool de almacenamiento que incluya al menos tres nodos de almacenamiento en tres sitios.
- Si tiene requisitos de alto rendimiento, no se recomienda el uso de un pool de almacenamiento que incluya varios sitios si la latencia de red entre los sitios es superior a 100 ms. A medida que aumenta la latencia, la velocidad a la que StorageGRID puede crear, colocar y recuperar fragmentos de objetos disminuye considerablemente debido al descenso del rendimiento de la red TCP.

  La disminución del rendimiento afecta a las tasas máximas alcanzables de ingesta y recuperación de objetos (cuando se seleccionan equilibrados o estrictos como comportamiento de procesamiento) o puede provocar retrasos en la cola de ILM (cuando se selecciona Dual commit como comportamiento de procesamiento). Consulte "Comportamiento de procesamiento de reglas de ILM".

  > Si su grid incluye solo un sitio, no podrá usar el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) o el sitio predeterminado Todos los sitios en un perfil de código de borrado. Este comportamiento evita que el perfil no sea válido si se agrega un segundo sitio.

- No se pueden usar nodos de archivo para datos con código de borrado.

Directrices para los pools de almacenamiento utilizados para copias archivadas

> La compatibilidad con los nodos de archivo (tanto para archivar en la nube mediante la API S3 como para archivar en cinta mediante el middleware TSM) está obsoleta y se eliminará en una versión futura. Mover objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo ha sido reemplazado por ILM Cloud Storage Pools, que ofrecen más funcionalidad.
>
> Consulte "Migrar objetos a un pool de almacenamiento en la nube".
>
> Además, debe quitar Nodos de archivo de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o anterior. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

- No puede crear un pool de almacenamiento que incluya nodos de almacenamiento y nodos de archivado. Las copias archivadas requieren un pool de almacenamiento que sólo incluya nodos de archivado.
- Cuando se utiliza un pool de almacenamiento que incluye nodos de archivado, también se debe mantener al menos una copia replicada o con código de borrado en un pool de almacenamiento que incluya nodos

de almacenamiento.

- Si la configuración global Bloqueo de objetos S3 está habilitada y está creando una regla de ILM compatible, no puede utilizar un pool de almacenamiento que incluya nodos de archivado. Consulte las instrucciones para gestionar objetos con el bloqueo de objetos de S3.
- Si el tipo de destino de un nodo de archivado es Cloud Tiering - simple Storage Service (S3), el nodo de archivado debe estar en su propio pool de almacenamiento.

Habilite la protección contra pérdida de sitio

Si la implementación de StorageGRID incluye más de un sitio, puede usar la replicación y el código de borrado con los pools de almacenamiento configurados correctamente para habilitar la protección contra pérdida de sitio.

La replicación y el código de borrado necesitan diferentes configuraciones de pools de almacenamiento:

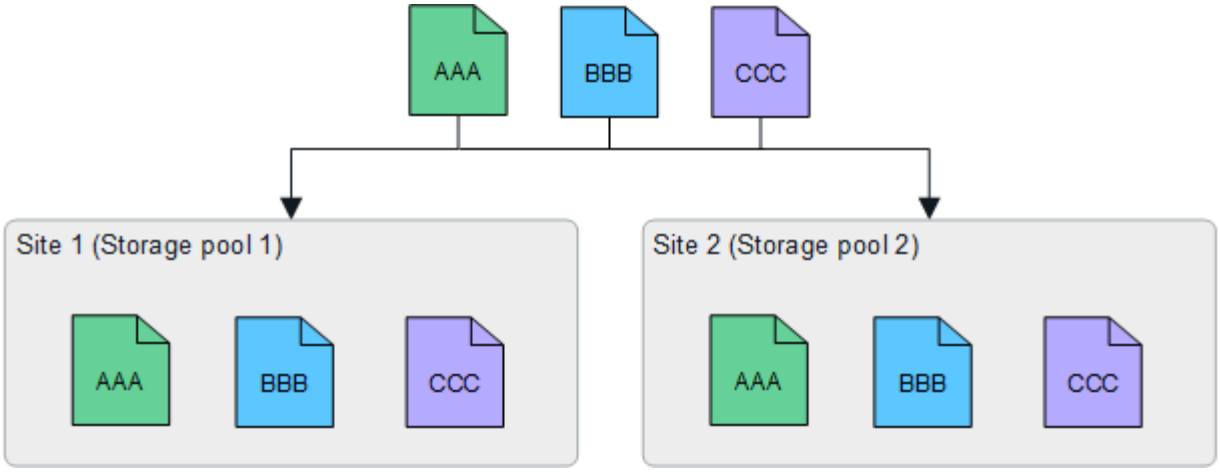
- Para utilizar la replicación para la protección contra pérdida de sitio, utilice los pools de almacenamiento específicos de sitios que se crean automáticamente durante la instalación de StorageGRID. A continuación, cree reglas de ILM con "instrucciones de colocación" esto especifica varios pools de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar código de borrado para la protección contra pérdida de sitio, "cree pools de almacenamiento que consten de varios sitios". A continuación, cree reglas de ILM que usen un pool de almacenamiento que conste de varios sitios y cualquier esquema de código de borrado disponible.

Ejemplo de replicación

De forma predeterminada, se crea un pool de almacenamiento para cada sitio durante la instalación de StorageGRID. Tener pools de almacenamiento compuestos solo por un sitio le permite configurar reglas de ILM que utilizan la replicación para la protección contra pérdida de sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene el sitio 1
- El grupo de almacenamiento 2 contiene el sitio 2
- La regla de ILM contiene dos ubicaciones:
  - Almacene objetos replicando la copia de 1 en el sitio 1
  - Almacene objetos replicando la copia de 1 en el sitio 2

Ubicaciones de reglas de ILM:



Si se pierde un sitio, hay copias de los objetos disponibles en el otro.

Ejemplo de código de borrado

Tener pools de almacenamiento compuestos por más de un sitio por pool de almacenamiento permite configurar reglas de ILM que utilicen código de borrado para la protección contra pérdida de sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene los sitios 1 a 3
- La regla de ILM contiene una ubicación: Almacenar objetos mediante código de borrado mediante un esquema EC 4+2 en el pool de almacenamiento 1, que contiene tres sitios

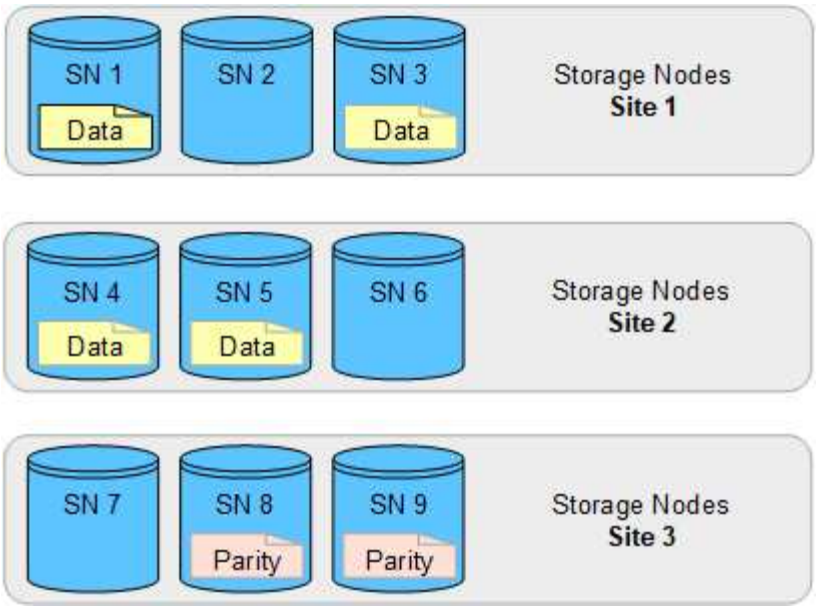
Ubicaciones de reglas de ILM:

En este ejemplo:

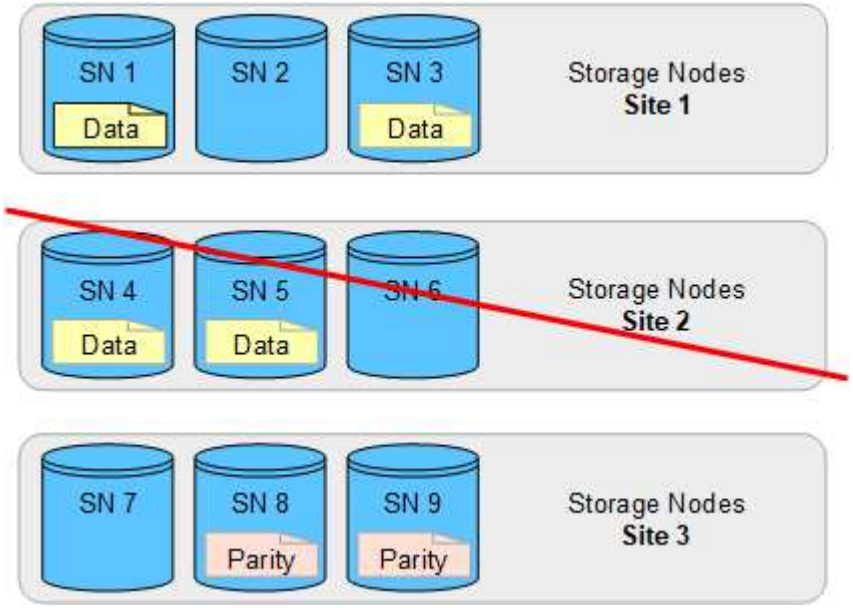
- La regla de ILM utiliza un esquema de código de borrado 4+2.
- Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir de los datos del objeto.
- Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centro de datos para proporcionar protección de datos ante fallos de nodos o pérdidas de sitios.

> Se permite el código de borrado en pools de almacenamiento que contienen cualquier número de sitios *excepto* dos sitios.

Regla de ILM que utiliza esquema de código de borrado 4+2:



Si se pierde un sitio, es posible recuperar los datos:



Cree un pool de almacenamiento

Se crean pools de almacenamiento para determinar dónde el sistema StorageGRID almacena los datos de objetos y el tipo de almacenamiento utilizado. Cada pool de almacenamiento incluye uno o más sitios y una o más calidades de almacenamiento.

> Al instalar StorageGRID 11,7 en un nuevo grid, se crean automáticamente pools de almacenamiento para cada sitio para reducir el número de pasos necesarios para crear nuevas reglas de ILM. Sin embargo, durante las actualizaciones a StorageGRID 11,7, no se crean pools de almacenamiento para cada sitio.

Si desea crear pools de almacenamiento en cloud para almacenar datos de objetos fuera del sistema StorageGRID, consulte "Información sobre el uso de Cloud Storage Pools".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Revisó las directrices para crear pools de almacenamiento.

Acerca de esta tarea

Los pools de almacenamiento determinan dónde se almacenan los datos de objeto. La cantidad de pools de almacenamiento que necesita depende del número de sitios del grid y de los tipos de copias que desee: Replicadas o codificadas por borrado.

- Para la replicación y la codificación de borrado a un solo sitio, cree un pool de almacenamiento para cada sitio. Por ejemplo, si desea almacenar copias de objetos replicados en tres sitios, cree tres pools de almacenamiento.
- Para la codificación de borrado en tres o más sitios, cree un pool de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si desea borrar objetos de código en tres sitios, cree un pool de almacenamiento.

> No incluya el sitio Todos los sitios en un grupo de almacenamiento que se utilizará en un perfil de código de borrado. En su lugar, añada una entrada independiente al pool de almacenamiento para cada instalación que almacenará los datos codificados de borrado. Consulte este paso por ejemplo.

- Si tiene más de un grado de almacenamiento, no cree un pool de almacenamiento que incluya diferentes grados de almacenamiento en un solo sitio. Consulte "Directrices para crear pools de almacenamiento".

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   En la pestaña Storage Pools, se muestra todos los pools de almacenamiento definidos.

   > Para las instalaciones nuevas de StorageGRID 11,6 o versiones anteriores, el pool de almacenamiento Todos los nodos de almacenamiento se actualiza automáticamente cada vez que se añaden sitios de centros de datos nuevos. No utilice este pool en reglas de ILM.

2. Para crear una nueva agrupación de almacenamiento, seleccione **Crear**.
3. Introduzca un nombre único para el pool de almacenamiento. Utilice un nombre que sea fácil de identificar cuando configure los perfiles de código de borrado y las reglas de ILM.
4. En la lista desplegable **Sitio**, seleccione un sitio para esta agrupación de almacenamiento.

   Cuando selecciona un sitio, el número de nodos de almacenamiento y nodos de archivado de la tabla se actualiza automáticamente.

   En general, no utilice el sitio Todos los sitios en ningún pool de almacenamiento. Las reglas de ILM que utilizan un pool de almacenamiento All Sites colocan los objetos en cualquier sitio disponible, lo que le otorga menos control de la ubicación de los objetos. Además, un pool de almacenamiento All Sites utiliza inmediatamente los nodos de almacenamiento en un sitio nuevo, lo que podría no ser el comportamiento esperado.

5. En la lista desplegable **Storage grade**, seleccione el tipo de almacenamiento que se utilizará si una regla de ILM utiliza este grupo de almacenamiento.

El nivel de almacenamiento, incluye todos los grados de almacenamiento, incluye todos los nodos de almacenamiento en el sitio seleccionado. El nivel de almacenamiento predeterminado de los nodos de archivado incluye todos los nodos de archivado en el sitio seleccionado. Si creó grados de almacenamiento adicionales para los nodos de almacenamiento del grid, estos se enumeran en el menú desplegable.

6. Si desea utilizar el grupo de almacenamiento en un perfil de codificación de borrado de varios sitios, seleccione **Agregar más nodos** para agregar una entrada para cada sitio al grupo de almacenamiento.

> Se le impide crear entradas duplicadas o crear un pool de almacenamiento que incluya tanto el grado de almacenamiento de los nodos de archivado como cualquier grado de almacenamiento que contenga nodos de almacenamiento.
>
> Se le advertirá si agrega más de una entrada con diferentes grados de almacenamiento para un sitio.

Para eliminar una entrada, seleccione el icono de eliminación ✕.

7. Cuando esté satisfecho con sus selecciones, seleccione **Guardar**.

El nuevo pool de almacenamiento se añadirá a la lista.

Ver detalles del pool de almacenamiento

Es posible ver los detalles de un pool de almacenamiento para determinar dónde se usa el pool de almacenamiento y para ver qué nodos y calidades de almacenamiento se incluyen.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

La tabla Storage Pools incluye la siguiente información para cada pool de almacenamiento que incluye nodos de almacenamiento:

- **Nombre**: El nombre exclusivo para mostrar de la agrupación de almacenamiento.
- **Node count**: El número de nodos en el pool de almacenamiento.
- **Uso de almacenamiento**: El porcentaje del espacio total utilizable que se ha utilizado para los datos de objetos en este nodo. Este valor no incluye metadatos de objetos.
- * Capacidad total*: El tamaño del pool de almacenamiento, que equivale a la cantidad total de espacio utilizable para los datos de objetos para todos los nodos del pool de almacenamiento.
- **Uso de ILM**: Cómo se está utilizando actualmente el pool de almacenamiento. Un pool de almacenamiento puede estar sin utilizar o puede utilizarse en una o más reglas de ILM, perfiles de código de borrado, o ambas.

> No se puede eliminar un pool de almacenamiento si se está utilizando.

2. Para ver los detalles de un pool de almacenamiento específico, seleccione su nombre.

   Se muestra la página de detalles del pool de almacenamiento.

3. Vea la pestaña * Nodos * para obtener información sobre los nodos de almacenamiento o los nodos de archivo incluidos en el grupo de almacenamiento.

   En la tabla se incluye la siguiente información para cada nodo:

   - Nombre del nodo
   - Nombre del sitio
   - Grado de almacenamiento
   - Uso de almacenamiento (%): El porcentaje del espacio útil total para los datos de objeto que se ha utilizado para el nodo de almacenamiento. Este campo no está visible para los pools de nodos de archivado.

   > El mismo valor de Uso de almacenamiento (%) también se muestra en el gráfico Almacenamiento usado - Datos de objeto para cada nodo de almacenamiento (seleccione **NODOS** > ***NODO de almacenamiento*** > **Almacenamiento**).

4. Seleccione la pestaña **ILM usage** para determinar si el pool de almacenamiento se está utilizando actualmente en cualquier regla de ILM o perfiles de codificación de borrado.
5. Opcionalmente, vaya a la página de reglas de ILM * para conocer y administrar las reglas que utilizan el grupo de almacenamiento.

   Consulte "Instrucciones para trabajar con reglas de ILM".

Editar pool de almacenamiento

Es posible editar un pool de almacenamiento para cambiar su nombre o para actualizar los sitios y las calificaciones de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Ha revisado el "directrices para crear pools de almacenamiento".
- Si prevé editar un pool de almacenamiento utilizado por una regla en la política de ILM activa, habrá pensado en cómo afectarán los cambios a la ubicación de los datos de los objetos.

Acerca de esta tarea

Si va a añadir un nuevo sitio o nivel de almacenamiento a un pool de almacenamiento que se usa en la política de ILM activa, tenga en cuenta que los nodos de almacenamiento del sitio nuevo o el grado de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a utilizar un sitio o nivel de almacenamiento nuevo, debe activar una nueva política de ILM después de guardar el pool de almacenamiento editado.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.
2. Seleccione la casilla de comprobación del pool de almacenamiento que desea editar.

No se puede editar el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y versiones anteriores).

3. Seleccione **Editar**.
4. Según sea necesario, cambie el nombre del pool de almacenamiento.
5. Según sea necesario, seleccione otros sitios y grados de almacenamiento.

> Se le impide cambiar el grado de sitio o de almacenamiento si el grupo de almacenamiento se utiliza en un perfil de código de borrado y el cambio provocaría que el esquema de código de borrado dejara de ser válido. Por ejemplo, si un pool de almacenamiento utilizado en un perfil de código de borrado incluye actualmente un grado de almacenamiento con un solo sitio, se le impide utilizar un grado de almacenamiento con dos sitios, ya que el cambio haría que el esquema de código de borrado no sea válido.

6. Seleccione **Guardar**.

Después de terminar

Si añadió un nuevo sitio o grado de almacenamiento a un pool de almacenamiento usado en la política de gestión del ciclo de vida de la información activa, active una nueva política de gestión del ciclo de vida de la información para forzar a StorageGRID a usar el nuevo sitio o el grado de almacenamiento. Por ejemplo, Clone la política de ILM existente y luego active el clon. Consulte "Trabaje con las reglas de ILM y las políticas de ILM".

Quitar un pool de almacenamiento

Es posible quitar un pool de almacenamiento que no se está usando.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.
2. Revise la columna Uso de ILM de la tabla para determinar si se puede quitar el pool de almacenamiento.

   No se puede quitar un pool de almacenamiento si se está utilizando en una regla de gestión de la vida útil de la información o en un perfil de código de borrado. Según sea necesario, seleccione ***storage pool name*** > **ILM usage** para determinar dónde se utiliza el pool de almacenamiento.

3. Si el pool de almacenamiento que desea quitar no se está utilizando, seleccione la casilla de comprobación.
4. Seleccione **Quitar**.
5. Seleccione **OK**.

Utilice Cloud Storage Pools

¿Qué es un pool de almacenamiento en cloud?

Un pool de almacenamiento en cloud permite utilizar ILM para mover datos de objetos fuera de su sistema StorageGRID. Por ejemplo, es posible que desee mover objetos a

los que se accede con poca frecuencia a un almacenamiento en cloud de bajo coste, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivado en el almacenamiento de Microsoft Azure Blob. O bien, puede que quiera mantener un backup en cloud de objetos de StorageGRID para mejorar la recuperación ante desastres.

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. Para almacenar objetos en cualquiera de las ubicaciones, debe seleccionar el pool al crear las instrucciones de ubicación para una regla de ILM. 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 externo (S3) o un contenedor (almacenamiento blob de Azure).

> El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API S3 está obsoleto y ha sido reemplazado por pools de almacenamiento en la nube de ILM, que ofrecen más funcionalidad. Si actualmente está utilizando un nodo de archivado con la opción Cloud Tiering - Simple Storage Service (S3), "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.

La tabla compara los pools de almacenamiento con los pools de almacenamiento en cloud y muestra las similitudes y las diferencias a alto nivel.

	Del banco de almacenamiento	**Pool de almacenamiento en cloud**
¿Cómo se crea?	Uso de la opción **ILM** > **agrupaciones de almacenamiento** en Grid Manager.	Usando la opción **ILM** > **Storage Pools** > **Cloud Storage Pools** en Grid Manager. Debe configurar el bloque o contenedor externo para poder crear el Cloud Storage Pool.
¿Cuántos pools se pueden crear?	Ilimitada.	Hasta 10.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento o nodos de archivado dentro de StorageGRID.	En el bloque de Amazon S3, el contenedor de almacenamiento de Azure Blob o Google Cloud externo al sistema StorageGRID. Si Cloud Storage Pool es un bloque de Amazon S3: • Opcionalmente, se puede configurar un ciclo de vida de bloque para pasar los objetos a un almacenamiento a largo plazo de bajo coste, como Amazon S3 Glacier o S3 Glacier Deep Archive. El sistema de almacenamiento externo debe admitir la clase de almacenamiento Glacier y la API DE restauración DE objetos S3. • Puede crear pools de almacenamiento en el cloud para usarlos con los servicios de cloud comercial (C2S) de AWS, compatibles con la región secreta de AWS. Si Cloud Storage Pool es un contenedor de almacenamiento de Azure Blob, StorageGRID realiza la transición del objeto al nivel de archivado. **Nota:** En general, no configure la gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor utilizado para un Cloud Storage Pool. Las operaciones POSTERIORES a la restauración de objetos en el Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.
¿Qué controla la ubicación de objetos?	Una regla de ILM en la política activa de ILM.	Una regla de ILM en la política activa de ILM.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.
¿Cuántas copias de cada objeto se permiten?	Múltiples.	Una copia en el pool de almacenamiento cloud y, opcionalmente, una o varias copias en StorageGRID. **Nota:** No puedes almacenar un objeto en más de un Pool de almacenamiento en la nube en un momento dado.
¿Cuáles son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
		Nota: Los datos de FabricPool no se pueden organizar en niveles en los grupos de almacenamiento en la nube. Los objetos con bloqueo de objetos S3 activado no se pueden colocar en pools de Cloud Storage.

Ciclo de vida de un objeto de Cloud Storage Pool

Antes de implementar Cloud Storage Pools, revise el ciclo de vida de los objetos que se almacenan en cada tipo de pool de almacenamiento en cloud.

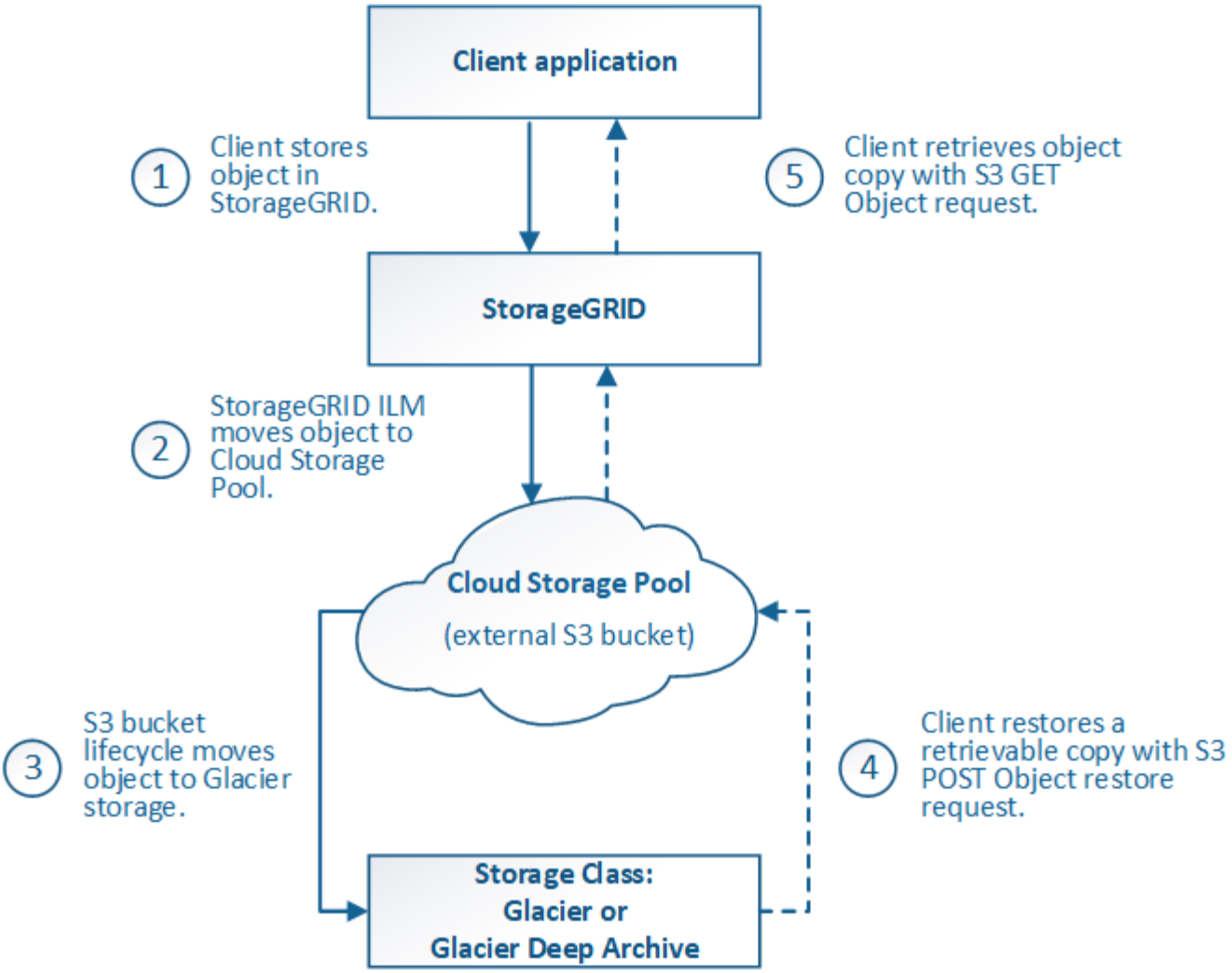
- S3: Ciclo de vida de un objeto de Cloud Storage Pool
- Azure: Ciclo de vida de un objeto de Cloud Storage Pool

S3: Ciclo de vida de un objeto de Cloud Storage Pool

En la figura, se muestran las etapas del ciclo de vida de un objeto almacenado en un pool de almacenamiento en cloud de S3.

> En la figura y las explicaciones, "'Glacier'" hace referencia tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: La clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración acelerada. Solo se admite la recuperación masiva o estándar.

> Google Cloud Platform (GCP) admite la recuperación de objetos de un almacenamiento a largo plazo sin necesidad de una operación POSTERIOR a la restauración.



1. **Objeto almacenado en StorageGRID**

   Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. **Objeto movido a S3 Cloud Storage Pool**
   - Cuando el objeto coincide con una regla de ILM que utiliza un S3 Cloud Storage Pool como ubicación, StorageGRID mueve el objeto al bloque de S3 externo especificado por el Cloud Storage Pool.
   - Cuando el objeto se haya movido a S3 Cloud Storage Pool, la aplicación cliente puede recuperarlo con una solicitud DE OBJETO GET de S3 de StorageGRID, a menos que el objeto se haya migrado al almacenamiento Glacier.
3. **Objeto que ha pasado a Glacier (estado no recuperable)**
   - Opcionalmente, se puede cambiar el objeto al almacenamiento Glacier. Por ejemplo, el bloque externo de S3 puede utilizar la configuración del ciclo de vida para mover un objeto al almacenamiento Glacier de inmediato o después de varios días.

> Si desea realizar la transición de objetos, debe crear una configuración de ciclo de vida para el bloque de S3 externo y debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API DE restauración DE objetos S3 POSTERIOR.

> No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. Swift no admite solicitudes DE restauración POSTERIOR de objetos, por lo que StorageGRID no podrá recuperar objetos Swift que se hayan migrado al almacenamiento S3 Glacier. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

  - Durante la transición, la aplicación cliente puede usar una solicitud DE objeto HEAD de S3 para supervisar el estado del objeto.

4. **Objeto restaurado desde el almacenamiento Glacier**

   Si se ha realizado la transición de un objeto al almacenamiento Glacier, la aplicación cliente puede emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable al pool de almacenamiento en cloud de S3. La solicitud especifica cuántos días debe estar disponible la copia en el Cloud Storage Pool y en el nivel de acceso a datos que se usará en la operación de restauración (acelerada, estándar o masiva). Cuando se alcanza la fecha de vencimiento de la copia recuperable, la copia se devuelve automáticamente a un estado no recuperable.

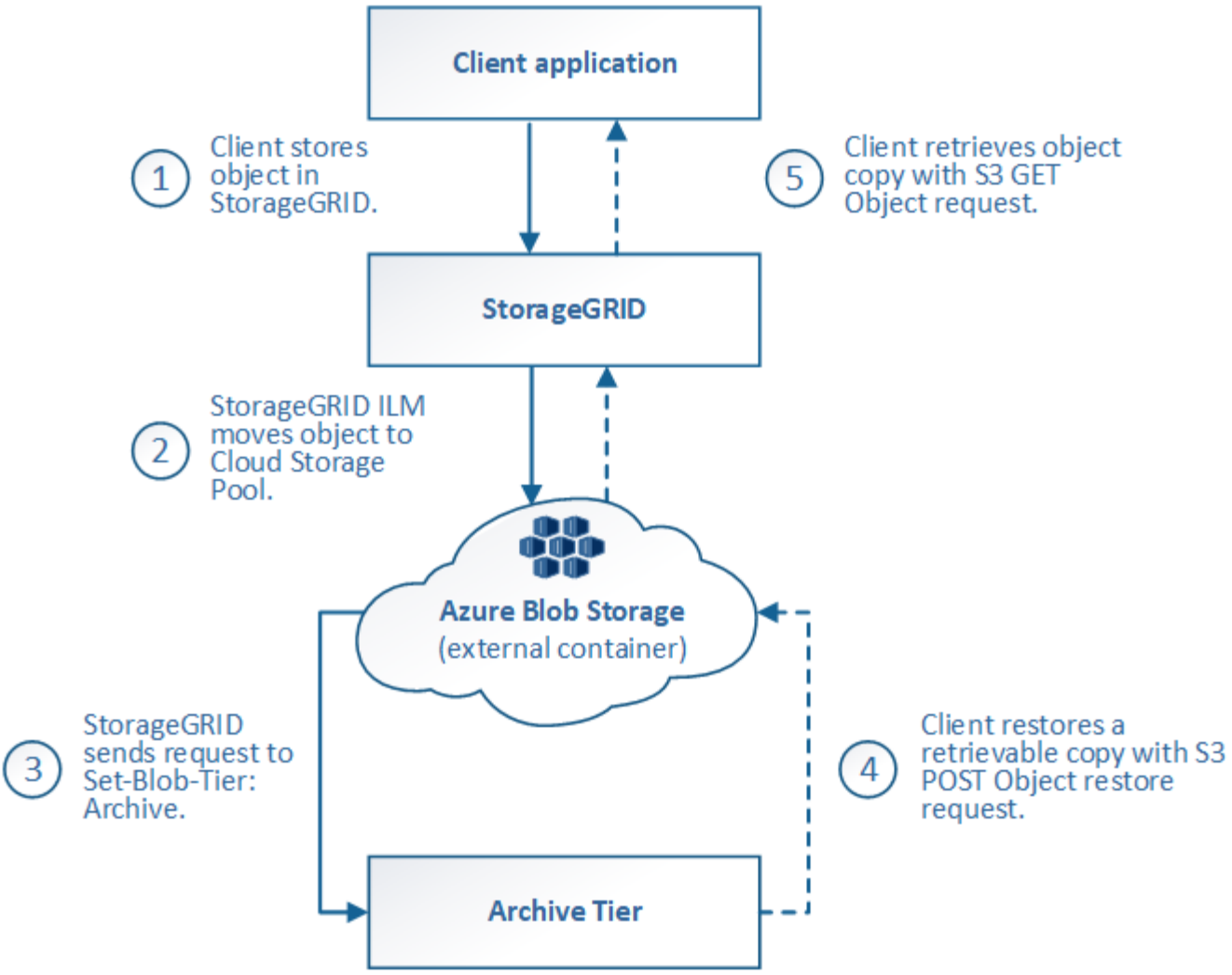
   > Si también hay una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier con una solicitud DE restauración POSTERIOR a objeto. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

   Una vez restaurado un objeto, la aplicación cliente puede emitir UNA solicitud GET Object para recuperar el objeto restaurado.

Azure: Ciclo de vida de un objeto de Cloud Storage Pool

En la figura, se muestran las etapas del ciclo de vida de un objeto almacenado en un pool de almacenamiento en cloud de Azure.



1. **Objeto almacenado en StorageGRID**

   Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. **Objeto movido a Azure Cloud Storage Pool**

   Cuando el objeto coincide con una regla de ILM que utiliza un Azure Cloud Storage Pool como ubicación de ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento externo de Azure Blob especificado por el Cloud Storage Pool

   > No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. Swift no admite solicitudes POSTERIORES a la restauración de objetos, por lo que StorageGRID no podrá recuperar objetos de Swift que se hayan migrado al nivel de archivado de almacenamiento de Azure Blob. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

3. **Objeto que ha pasado a la capa de archivado (estado no recuperable)**

   Inmediatamente después de mover el objeto a Azure Cloud Storage Pool, StorageGRID realiza una transición automática del objeto al nivel de archivado de almacenamiento de Azure Blob.

4. **Objeto restaurado desde el nivel de archivo**

Si se ha realizado la transición de un objeto al nivel de archivado, la aplicación cliente puede emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable a Azure Cloud Storage Pool.

Cuando StorageGRID recibe LA restauración DE objetos POSTERIOR, este realiza una transición temporal del objeto al nivel de refrigeración del almacenamiento de Azure Blob. Tan pronto como se alcanza la fecha de vencimiento de la solicitud DE restauración DE objeto POSTERIOR, StorageGRID realiza la transición del objeto de nuevo al nivel de archivado.

> Si también existen una o varias copias del objeto en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivado mediante la emisión de una solicitud DE restauración DE objetos POSTERIOR. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

   Una vez que se ha restaurado un objeto en Azure Cloud Storage Pool, la aplicación cliente puede emitir una solicitud GET Object para recuperar el objeto restaurado.

Información relacionada

"USE LA API DE REST DE S3"

Cuándo usar Cloud Storage Pools

Con Cloud Storage Pools, puede crear un backup o organizar los datos en niveles en una ubicación externa. Además, puede hacer backups o organizar los datos en más de un cloud.

Backup de datos de StorageGRID en ubicaciones externas

Puede usar un pool de almacenamiento en cloud para realizar backup de objetos StorageGRID en una ubicación externa.

Si no se puede acceder a las copias en StorageGRID, se pueden utilizar los datos de objetos en el pool de almacenamiento en cloud para atender las solicitudes de los clientes. Sin embargo, es posible que deba emitir la solicitud de restauración DE objetos S3 POST para acceder a la copia de objeto de backup en el Cloud Storage Pool.

Los datos del objeto en un pool de almacenamiento en cloud también se pueden utilizar para recuperar los datos perdidos de StorageGRID debido a un fallo del volumen de almacenamiento o del nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un pool de almacenamiento en el cloud, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Para implantar una solución de backup:

1. Cree un único pool de almacenamiento en el cloud.
2. Configure una regla de ILM que almacene copias de objetos en los nodos de almacenamiento de forma simultánea (como copias replicadas o codificadas por borrado) y una única copia de objetos en el Cloud Storage Pool.
3. Añada la regla a la política de ILM. A continuación, simule y active la directiva.

Organice los datos en niveles desde StorageGRID a ubicaciones externas

Puede utilizar un pool de almacenamiento en cloud para almacenar objetos fuera del sistema StorageGRID. Por ejemplo, supongamos que tiene un gran número de objetos que necesita retener, pero espera tener acceso a esos objetos rara vez, si es que alguna vez. Puede usar un pool de almacenamiento en cloud para organizar los objetos en niveles para reducir el almacenamiento y liberar espacio en StorageGRID.

Para implementar una solución por niveles:

1. Cree un único pool de almacenamiento en el cloud.
2. Configure una regla de ILM que mueva objetos que no se usen frecuentemente desde nodos de almacenamiento a Cloud Storage Pool.
3. Añada la regla a la política de ILM. A continuación, simule y active la directiva.

Mantenga varios extremos de cloud

Puede configurar varios extremos de Cloud Storage Pool si desea organizar en niveles o realizar backups de datos de objetos en más de una nube. Los filtros de las reglas de ILM permiten especificar los objetos que se almacenan en cada Cloud Storage Pool. Por ejemplo, es posible que desee almacenar objetos de algunos clientes o buckets en Amazon S3 Glacier y objetos de otros inquilinos o buckets en el almacenamiento de Azure Blob. O bien, es posible que desee mover datos entre el almacenamiento de Amazon S3 Glacier y Azure Blob.

> Cuando se utilizan varios extremos de Cloud Storage Pool, tenga en cuenta que un objeto se puede almacenar solo en un Cloud Storage Pool cada vez.

Para implementar varios extremos de cloud:

1. Cree hasta 10 pools de almacenamiento en cloud.
2. Configure las reglas de ILM para almacenar los datos de los objetos adecuados en el momento adecuado en cada pool de almacenamiento de cloud. Por ejemplo, almacene objetos del bloque A en el Cloud Storage Pool A y almacene objetos del bloque B en el Cloud Storage Pool B. O bien, almacene objetos en el pool de almacenamiento en cloud A durante cierto tiempo y muévalos a Cloud Storage Pool B.
3. Añada las reglas a la política de ILM. A continuación, simule y active la directiva.

Consideraciones para Cloud Storage Pools

Si planea utilizar un pool de almacenamiento en cloud para mover objetos desde el sistema StorageGRID, debe revisar las consideraciones que hay que tener en cuenta a la hora de configurar y utilizar pools de almacenamiento en cloud.

Consideraciones generales

- En general, el almacenamiento de archivado en cloud, como el almacenamiento de Amazon S3 Glacier o Azure Blob, es un lugar económico para almacenar datos de objetos. No obstante, los costes para recuperar datos del almacenamiento de archivado en el cloud son relativamente altos. Para alcanzar el coste general más bajo, debe tener en cuenta cuándo y con qué frecuencia accederá a los objetos en el pool de almacenamiento en cloud. El uso de un Cloud Storage Pool solo se recomienda para el contenido al que espera acceder con poca frecuencia.
- No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. Swift no admite solicitudes POSTERIORES a la restauración de objetos, por lo que StorageGRID no podrá recuperar objetos de Swift que se hayan migrado al almacenamiento S3 Glacier ni al nivel de almacenamiento de Azure Blob. La

emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

- No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.
- Los objetos con bloqueo de objetos S3 activado no se pueden colocar en pools de Cloud Storage.
- Si el bucket S3 de destino para un pool de almacenamiento en la nube tiene S3 Object Lock habilitado, el intento de configurar la replicación de bucket (PutBucketReplication) fallará con un error ACCESSDENIED.

Consideraciones sobre los puertos utilizados para Cloud Storage Pools

Para garantizar que las reglas de ILM puedan mover objetos desde y hacia el Cloud Storage Pool especificado, debe configurar la red o las redes que contienen los nodos de almacenamiento del sistema. Debe asegurarse de que los siguientes puertos puedan comunicarse con el pool de almacenamiento en cloud.

De forma predeterminada, los pools de almacenamiento en cloud utilizan los puertos siguientes:

- **80**: Para los URI de punto final que comienzan con http
- **443**: Para los URI de punto final que comienzan con https

Es posible especificar un puerto diferente cuando se crea o se edita un pool de almacenamiento en el cloud.

Si utiliza un servidor proxy no transparente, también debe hacerlo "Configure un proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

Consideraciones sobre los costos

El acceso al almacenamiento en el cloud por medio de un pool de almacenamiento en el cloud requiere conectividad de red al cloud. Debe tener en cuenta el coste de la infraestructura de red que utilizará para acceder al cloud y aprovisionarlo adecuadamente, en función de la cantidad de datos que espera mover entre StorageGRID y el cloud con el pool de almacenamiento en cloud.

Cuando StorageGRID se conecta al extremo externo de Flash Storage Pool, emite distintas solicitudes para supervisar la conectividad y garantizar que puede ejecutar las operaciones requeridas. Aunque se asociarán algunos costes adicionales con estas solicitudes, el coste de supervisar un Cloud Storage Pool solo debería ser una pequeña fracción del coste total de almacenar objetos en S3 o Azure.

Es posible que deba incurrir en costes más significativos si necesita mover objetos desde un extremo de almacenamiento en cloud externo a StorageGRID. Los objetos pueden moverse de nuevo a StorageGRID en cualquiera de estos casos:

- La única copia del objeto se encuentra en un Pool de almacenamiento en cloud y en su lugar decide almacenar el objeto en StorageGRID. En este caso, volverá a configurar las reglas y políticas de ILM. Cuando se produce la evaluación de la gestión de la vida útil de la información, StorageGRID emite varias solicitudes para recuperar el objeto desde el pool de almacenamiento en cloud. A continuación, StorageGRID crea el número especificado de copias replicadas o codificadas de borrado en forma local. Cuando el objeto se mueve de nuevo a StorageGRID, se elimina la copia en el pool de almacenamiento en el cloud.
- Se pierden los objetos debido a un fallo en el nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un pool de almacenamiento en el cloud, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Cuando se devuelven objetos a StorageGRID desde un pool de almacenamiento en el cloud, StorageGRID emite varias solicitudes al extremo de pool de almacenamiento en cloud para cada objeto. Antes de mover un gran número de objetos, póngase en contacto con el soporte técnico para obtener ayuda a la hora de calcular el plazo de tiempo y los costes asociados.

S3: Permisos necesarios para el bloque de Cloud Storage Pool

La política de bloque para el bloque externo de S3 usado para un Cloud Storage Pool debe otorgar permiso StorageGRID para mover un objeto al bloque, obtener el estado de un objeto, restaurar un objeto del almacenamiento Glacier cuando sea necesario y más. Lo ideal es que StorageGRID tenga acceso de control total al cucharón (`s3:*`); sin embargo, si esto no es posible, la directiva bucket debe conceder los siguientes permisos S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Consideraciones para el ciclo de vida del bloque externo

El movimiento de objetos entre StorageGRID y el bloque externo S3 especificado en el Cloud Storage Pool está controlado por las reglas de ILM y la política activa de ILM en StorageGRID. Por el contrario, la configuración del ciclo de vida de ese bloque controla la transición de objetos desde el bloque S3 externo especificado en Cloud Storage Pool a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implementa la clase de almacenamiento Glacier).

Si desea realizar la transición de objetos desde Cloud Storage Pool, debe crear la configuración de ciclo de vida adecuada en el bloque externo de S3. Debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible CON la API DE restauración POSTERIOR a objetos de S3.

Por ejemplo, supongamos que desea que se realice inmediatamente la transición de todos los objetos movidos de StorageGRID al pool de almacenamiento en cloud al almacenamiento Amazon S3 Glacier. Debe crear una configuración de ciclo de vida en el bloque S3 externo que especifique una única acción (**transición**) de la siguiente forma:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Esta regla transitaría todos los objetos de bloques al Amazon S3 Glacier el día en que se crearon (es decir, el día en que se movieron de StorageGRID a la agrupación de almacenamiento en cloud).

> Al configurar el ciclo de vida del cucharón externo, no utilice nunca acciones **Expiración** para definir cuándo caducan los objetos. Las acciones de caducidad hacen que el sistema de almacenamiento externo elimine los objetos caducados. Si más adelante intenta acceder a un objeto caducado de StorageGRID, no se encuentra el objeto eliminado.

Si desea realizar la transición de objetos del Cloud Storage Pool a S3 Glacier Deep Archive (en lugar de Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida de la cuchara. Sin embargo, tenga en cuenta que no puede utilizar el `Expedited` organice en niveles los objetos de S3 Glacier Deep Archive.

Azure: Consideraciones para el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puede configurar el nivel de acceso predeterminado en Hot o Cool. Al crear una cuenta de almacenamiento para usar con un pool de almacenamiento en el cloud, se debe usar el nivel de función como nivel predeterminado. Aunque StorageGRID establece inmediatamente el nivel Archivado cuando se mueven objetos al pool de almacenamiento en el cloud, el uso de una configuración predeterminada de caliente garantiza que no se cobrará una tarifa de eliminación anticipada de los objetos que se quitan del nivel de refrigeración antes del mínimo de 30 días.

Azure: Gestión del ciclo de vida no compatible

No use gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor que se usa con un pool de almacenamiento en cloud. Las operaciones de ciclo de vida pueden interferir en las operaciones de Cloud Storage Pool.

Información relacionada

- "Cree un pool de almacenamiento en el cloud"

Compare los pools de almacenamiento en cloud y la replicación de CloudMirror

Cuando comience a usar pools de almacenamiento en cloud, podría ser útil comprender las similitudes y diferencias entre los pools de almacenamiento en cloud y el servicio de

replicación CloudMirror de StorageGRID.

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Actúa como destino de archivado. La copia de objeto del Pool de almacenamiento en cloud puede ser la única copia del objeto, o bien puede ser una copia adicional. Esto es, en lugar de conservar dos copias en el sitio, puede conservar una copia dentro de StorageGRID y enviar una copia al Pool de almacenamiento en cloud.	Permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) a un bloque S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente.
¿Cómo se configura?	Se definen del mismo modo que los pools de almacenamiento, mediante Grid Manager o la API de gestión de grid. Se puede seleccionar como ubicación en una regla de ILM. Si bien un pool de almacenamiento consta de un grupo de nodos de almacenamiento, un pool de almacenamiento en el cloud se define mediante un extremo remoto de S3 o Azure (dirección IP, credenciales, etc.).	Un usuario inquilino "Configura la replicación de CloudMirror" Al definir un extremo de CloudMirror (dirección IP, credenciales, etc.) con el administrador de inquilinos o la API de S3. Una vez configurado el extremo de CloudMirror, se puede configurar cualquier bloque que sea propiedad de esa cuenta de inquilino para que apunte al extremo de CloudMirror.
¿Quién es responsable de su configuración ?	Normalmente, un administrador de grid	Normalmente, un usuario inquilino
¿Cuál es el destino?	• Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Nivel de Azure Blob Archive • Google Cloud Platform (GCP)	• Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Google Cloud Platform (GCP)
¿Qué hace que los objetos se muevan al destino?	Una o varias reglas de ILM en la política activa de ILM. Las reglas de ILM definen los objetos que StorageGRID se mueve al Cloud Storage Pool y cuándo se mueven los objetos.	Acción de ingerir un nuevo objeto en un depósito de origen que se haya configurado con un punto final de CloudMirror. Los objetos que existían en el bloque de origen antes de que se configurara con el extremo de CloudMirror no se replican, a menos que se modifiquen.

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones deben solicitar a StorageGRID para recuperar objetos que se hayan movido a un pool de almacenamiento en cloud. Si se transición la única copia de un objeto al almacenamiento de archivado, StorageGRID gestiona el proceso de restauración del objeto para que se pueda recuperar.	Debido a que la copia duplicada en el bloque de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes ya sea a StorageGRID o al destino de S3. Por ejemplo, supongamos que usa la replicación de CloudMirror para reflejar objetos en una organización asociada. El partner puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Puede leer directamente desde el destino?	No StorageGRID gestiona los objetos movidos a un pool de almacenamiento en cloud. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del pool de almacenamiento en cloud).	Sí, porque la copia duplicada es una copia independiente.
¿Qué ocurre si un objeto se elimina del origen?	El objeto también se elimina del Cloud Storage Pool.	La acción de eliminación no se replica. Un objeto eliminado ya no existe en el bloque StorageGRID, pero sigue existiendo en el bloque de destino. Del mismo modo, los objetos del bloque de destino se pueden eliminar sin que ello afecte al origen.
¿Cómo accede a los objetos tras un desastre (el sistema StorageGRID no está operativo)?	Los nodos StorageGRID con errores deben recuperarse. Durante este proceso, es posible que se restauren copias de los objetos replicados con las copias del Cloud Storage Pool.	Las copias de objetos en el destino de CloudMirror son independientes de la StorageGRID, por lo que se podrá acceder a ellas directamente antes de que se recuperen los nodos StorageGRID.

Cree un pool de almacenamiento en el cloud

Un Cloud Storage Pool especifica un único bloque externo de Amazon S3 u otro proveedor compatible con S3 o contenedor de almacenamiento de Azure Blob.

Al crear un grupo de almacenamiento en la nube, se especifica el nombre y la ubicación del contenedor o depósito externo que StorageGRID usará para almacenar objetos, el tipo de proveedor de nube (almacenamiento de Amazon S3/GCP o Azure Blob) y la información que StorageGRID necesita para acceder al contenedor o depósito externo.

StorageGRID valida el pool de almacenamiento en cloud tan pronto como lo guarde, por lo que debe asegurarse de que existe el bloque o contenedor especificado en el pool de almacenamiento en el cloud y sea posible acceder a él.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Ha revisado el "Consideraciones para Cloud Storage Pools".
- Ya existe el depósito o contenedor externo al que hace referencia Cloud Storage Pool y conoce su nombre y ubicación.
- Para acceder al depósito o contenedor, tiene la siguiente información para el tipo de autenticación que elegirá:

Tecla de acceso S3

Para el cubo externo S3

- El ID de clave de acceso de la cuenta que posee el bloque externo.
- La clave de acceso secreta asociada.

Como alternativa, puede especificar Anonymous para el tipo de autenticación.

Portal de acceso C2S

Para servicios en la nube comercial (C2S) S3 SERVICE

Tiene lo siguiente:

- URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor del portal de acceso C2S (CAP), incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
- Certificado de CA de servidor emitido por una entidad de certificación (CA) gubernamental apropiada. StorageGRID utiliza este certificado para comprobar la identidad del servidor CAP. El certificado de CA del servidor debe utilizar la codificación PEM.
- Certificado de cliente emitido por una autoridad de certificación gubernamental (CA) apropiada. StorageGRID utiliza este certificado para identificarse al servidor CAP. El certificado de cliente debe utilizar la codificación PEM y debe tener acceso a su cuenta C2S.
- Clave privada codificada con PEM para el certificado de cliente.
- Frase de acceso para descifrar la clave privada para el certificado de cliente, si está cifrada.

> Si el certificado de cliente se cifrará, utilice el formato tradicional para el cifrado. El formato cifrado PKCS #8 no es compatible.

Almacenamiento de Azure Blob

Para el contenedor externo

- Identificador de Recursos Uniforme (URI) utilizado para acceder al contenedor Blob Storage.
- Nombre de la cuenta de almacenamiento y la clave de cuenta. Puede usar el portal de Azure para encontrar estos valores.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Seleccione **Crear**, luego ingrese la siguiente información:

Campo	Descripción
Nombre de Cloud Storage Pool	Un nombre que describe brevemente el pool de almacenamiento en el cloud y su propósito. Utilice un nombre que será fácil de identificar al configurar las reglas de ILM.
Tipo de proveedor	Qué proveedor de cloud utilizará para este pool de almacenamiento en cloud: • **Amazon S3/GCP**: Seleccione esta opción para un proveedor compatible con Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • **Almacenamiento de Azure Blob**
Cubo o contenedor	El nombre del bloque externo de S3 o contenedor de Azure. No se puede cambiar este valor después de guardar Cloud Storage Pool.

3. Según la selección del tipo de proveedor, introduzca la información de punto final de servicio.

Amazon S3/GCP

a. Para el protocolo, seleccione HTTPS o HTTP.

> No utilice conexiones HTTP para datos confidenciales.

b. Introduzca el nombre de host. Ejemplo:

`s3-aws-region.amazonaws.com`

c. Seleccione el estilo de URL:

Opción	Descripción
Detección automática	Intente detectar automáticamente qué estilo de URL usar, en función de la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una dirección URL de tipo path. Seleccione esta opción sólo si no conoce el estilo específico que desea utilizar.
Estilo hospedado virtual	Use una URL de estilo alojada virtual para acceder al bloque. Las URL de estilo hospedado virtual incluyen el nombre del bucket como parte del nombre de dominio. Ejemplo: `https://bucket-name.s3.company.com/key-name`
Estilo de ruta	Utilice una dirección URL de estilo de ruta para acceder al bloque. Las URL de estilo de ruta incluyen el nombre del cubo al final Ejemplo: `https://s3.company.com/bucket-name/key-name` **Nota:** La opción de URL de estilo de ruta no se recomienda y se descartará en una futura versión de StorageGRID.

d. De manera opcional, introduzca el número de puerto o utilice el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de Azure Blob

a. Con uno de los siguientes formatos, introduzca el URI para el punto final de servicio.

- `https://host:port`
- `http://host:port`

Ejemplo: `https://myaccount.blob.core.windows.net:443`

Si no especifica un puerto, por defecto el puerto 443 se utiliza para HTTPS y el puerto 80 se utiliza para HTTP.

4. Seleccione **continuar**. A continuación, seleccione el tipo de autenticación e introduzca la información requerida para el extremo de Cloud Storage Pool:

Clave de acceso

Solo para el tipo de proveedor de Amazon S3/GCP

a. Para **ID de clave de acceso**, ingrese el ID de clave de acceso de la cuenta que posee el depósito externo.
b. Para **Clave de acceso secreta**, ingrese la clave de acceso secreta.

CAP (portal de acceso C2S)

Para servicios en la nube comercial (C2S) S3 SERVICE

a. Para **URL de credenciales temporales**, ingrese la URL completa que StorageGRID usará para obtener credenciales temporales del servidor CAP, incluyendo todos los parámetros API requeridos y opcionales asignados a su cuenta C2S.
b. Para **Certificado CA de servidor**, seleccione **Examinar** y cargue el certificado CA codificado con PEM que StorageGRID utilizará para verificar el servidor CAP.
c. Para **Certificado de cliente**, seleccione **Examinar** y cargue el certificado codificado con PEM que StorageGRID utilizará para identificarse en el servidor CAP.
d. Para **Clave privada del cliente**, seleccione **Examinar** y cargue la clave privada codificada con PEM para el certificado del cliente.
e. Si la clave privada del cliente está cifrada, introduzca la frase de acceso para descifrar la clave privada del cliente. De lo contrario, deje en blanco el campo **Client private key passphrase**.

Almacenamiento de Azure Blob

a. Para **Nombre de cuenta**, ingrese el nombre de la cuenta de almacenamiento de Blob que posee el contenedor de servicio externo.
b. Para **Clave de cuenta**, ingresa la clave secreta para la cuenta de almacenamiento de Blob.

Anónimo

No se requiere información adicional.

5. Seleccione **continuar**. A continuación, elija el tipo de verificación de servidor que desea utilizar:

Opción	Descripción
Utilice los certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utilice los certificados de CA de cuadrícula instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Seleccione **Browse** y cargue el certificado codificado PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

6. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el depósito o contenedor y el punto final del servicio existen y que se puede acceder a ellos mediante las credenciales que ha especificado.
- Escribe un archivo de marcador en el bloque o contenedor para identificarlo como un Cloud Storage Pool. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

  Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, puede que se informe un error si hay un error de certificado o si el bloque o el contenedor especificados no existen ya.

7. Si se produce un error, consulte "Instrucciones para solucionar problemas de Cloud Storage Pools", Resuelva cualquier problema y, a continuación, intente guardar el Pool de almacenamiento en cloud de nuevo.

Editar un pool de almacenamiento en el cloud

Puede editar un Pool de almacenamiento en la nube para cambiar su nombre, punto final de servicio u otros detalles; sin embargo, no puede cambiar el bucket de S3 o el contenedor de Azure para un Pool de almacenamiento en la nube.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Ha revisado el "Consideraciones para Cloud Storage Pools".

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.

   En la tabla Cloud Storage Pools, se enumera los pools de almacenamiento en el cloud.

2. Seleccione la casilla de verificación para el pool de almacenamiento en la nube que desea editar.
3. Selecciona **Acciones** > **Editar**.
4. Según sea necesario, cambie el nombre para mostrar, el extremo de servicio, las credenciales de autenticación o el método de validación de certificados.

   > No puede cambiar el tipo de proveedor, el bucket de S3 o el contenedor de Azure para un Cloud Storage Pool.

   Si cargó anteriormente un certificado de servidor o cliente, puede seleccionar **Detalles del certificado** para revisar el certificado que está en uso actualmente.

5. Seleccione **Guardar**.

   Cuando guarda un pool de almacenamiento en cloud, StorageGRID valida que el bloque o el contenedor y el extremo de servicio existen, y que se pueden acceder a ellos con las credenciales especificadas.

   Si la validación de Cloud Storage Pool falla, se muestra un mensaje de error. Por ejemplo, es posible que se informe un error si existe un error de certificado.

   Consulte las instrucciones para "Solución de problemas de Cloud Storage Pools", Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

Quitar un pool de almacenamiento en el cloud

Puede quitar un pool de almacenamiento en cloud si no se utiliza en una regla de gestión de la vida útil de la información y no contiene datos de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Si es necesario, utilice ILM para mover datos de objetos

Si el Cloud Storage Pool que desea quitar contiene datos de objetos, debe usar ILM para mover los datos a otra ubicación. Por ejemplo, puede mover los datos a Nodos de almacenamiento en el grid o a otro Pool de almacenamiento en la nube.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Observe la columna Uso de ILM en la tabla para determinar si puede quitar Cloud Storage Pool.

   No puede quitar un pool de almacenamiento de cloud si se está utilizando en una regla de gestión de la vida útil de la información o en un perfil de código de borrado.

3. Si se está utilizando Cloud Storage Pool, seleccione ***cloud storage pool name*** > **ILM usage**.
4. "Clone cada regla de ILM" Que actualmente coloca objetos en el Cloud Storage Pool que desea eliminar.
5. Determine dónde desea mover los objetos existentes gestionados por cada regla clonada.

   Puede utilizar uno o más pools de almacenamiento o un pool de almacenamiento en cloud diferente.

6. Edite cada una de las reglas clonadas.

   Para el Paso 2 del Asistente para crear reglas de ILM, seleccione la nueva ubicación en el campo **Copias en**.

7. "Cree una nueva política de ILM propuesta" y reemplace cada una de las reglas antiguas por una regla clonada.
8. Activar la nueva política.
9. Espere a que ILM elimine objetos del Cloud Storage Pool y colóquelos en la nueva ubicación.

Eliminar Pool de Almacenamiento en Nube

Cuando el pool de almacenamiento en cloud está vacío y no se usa en ninguna regla de ILM, puede eliminarlo.

Antes de empezar

- Quitó todas las reglas de ILM que pueden haber utilizado el pool.
- Ha confirmado que el bloque de S3 o el contenedor de Azure no contienen ningún objeto.

  Se produce un error si intenta quitar un Pool de almacenamiento en cloud si contiene objetos. Consulte "Solucione problemas de Cloud Storage Pools".

Cuando se crea un pool de almacenamiento en el cloud, StorageGRID escribe un archivo marcador en el bloque o contenedor para identificarlo como un pool de almacenamiento en el cloud. No elimine este archivo, que tiene el nombre `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Si la columna ILM usage indica que Cloud Storage Pool no se está usando, seleccione la casilla de comprobación.
3. Seleccione **acciones** > **Quitar**.
4. Seleccione **OK**.

Solucione problemas de Cloud Storage Pools

Utilice estos pasos de solución de problemas para resolver los errores que puede encontrar al crear, editar o eliminar un pool de almacenamiento en la nube.

Determine si se ha producido un error

StorageGRID realiza una comprobación simple del estado de cada pool de almacenamiento en cloud una vez por minuto para garantizar que se pueda acceder al pool de almacenamiento en cloud y que funciona correctamente. Si la comprobación del estado detecta un problema, se muestra un mensaje en la última columna de error de la tabla Cloud Storage Pools de la página Storage Pools.

En la tabla, se muestra el error más reciente detectado para cada pool de almacenamiento en cloud e indica cuánto tiempo se produjo el error.

Además, se activa una alerta de error * de conectividad del grupo de almacenamiento en cloud* si la comprobación del estado detecta que se han producido uno o varios errores nuevos de Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya a la página Grupos de almacenamiento (seleccione **ILM** > **Grupos de almacenamiento**), revise los mensajes de error en la última columna de error y consulte las directrices para la solución de problemas que aparecen a continuación.

Compruebe si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. En la página Cloud Storage Pool, seleccione el punto final y seleccione **Borrar error**. Un mensaje de confirmación indica que StorageGRID borró el error para el pool de almacenamiento en el cloud.

Si se ha resuelto el problema subyacente, ya no se muestra el mensaje de error. Sin embargo, si el problema subyacente no se ha solucionado (o si se encuentra un error diferente), el mensaje de error se mostrará en la última columna de error en unos pocos minutos.

Error: Este pool de almacenamiento en cloud contiene contenido inesperado

Es posible ver este mensaje de error cuando se intenta crear, editar o eliminar un pool de almacenamiento en cloud. Este error se produce si el cucharón o el contenedor incluye `x-ntap-sgws-cloud-pool-uuid` Archivo marcador, pero ese archivo no tiene el UUID esperado.

Por lo general, solo verá este error si crea un nuevo pool de almacenamiento en el cloud y otra instancia de StorageGRID ya utiliza el mismo pool de almacenamiento en el cloud.

Intente realizar estos pasos para corregir el problema:

- Compruebe que nadie de su organización utiliza también este pool de almacenamiento en el cloud.
- Elimine el `x-ntap-sgws-cloud-pool-uuid` Archivo e intente configurar de nuevo el Pool de almacenamiento en la nube.

Error: No se pudo crear o actualizar Cloud Storage Pool. Error desde el punto final

Es posible ver este mensaje de error cuando se intenta crear o editar un pool de almacenamiento en el cloud. Este error indica que algún problema de conectividad o configuración impide que StorageGRID escriba en el pool de almacenamiento en el cloud.

Para corregir el problema, revise el mensaje de error desde el punto final.

- Si el mensaje de error contiene `Get *url*: EOF`, Compruebe que el punto final de servicio utilizado para el pool de almacenamiento en la nube no utiliza HTTP para un contenedor o depósito que requiere HTTPS.
- Si el mensaje de error contiene `Get *url*: net/http: request canceled while waiting for connection`, Compruebe que la configuración de red permite a los nodos de almacenamiento acceder al extremo de servicio utilizado para el grupo de almacenamiento en la nube.
- Para todos los demás mensajes de error de punto final, intente uno o más de los siguientes:
  - Cree un contenedor o bloque externo con el mismo nombre que introdujo para el Cloud Storage Pool e intente guardar de nuevo el nuevo Cloud Storage Pool.
  - Corrija el nombre de contenedor o bloque que especificó para Cloud Storage Pool e intente guardar de nuevo el nuevo pool de almacenamiento en cloud.

Error: No se pudo analizar el certificado de CA

Es posible ver este mensaje de error cuando se intenta crear o editar un pool de almacenamiento en el cloud. El error se produce si StorageGRID no pudo analizar el certificado introducido al configurar el pool de almacenamiento en cloud.

Para corregir el problema, compruebe el certificado de CA que proporcionó para los problemas.

Error: No se encontró un pool de almacenamiento en cloud con este ID

Es posible ver este mensaje de error cuando se intenta editar o eliminar un pool de almacenamiento en el cloud. Este error se produce si el extremo devuelve una respuesta 404, que puede significar cualquiera de las siguientes:

- Las credenciales utilizadas para Cloud Storage Pool no tienen permiso de lectura para el depósito.
- El bloque utilizado para el pool de almacenamiento en cloud no incluye el `x-ntap-sgws-cloud-pool-uuid` archivo de marcador.

Intente uno o más de estos pasos para corregir el problema:

- Compruebe que el usuario asociado a la clave de acceso configurada tenga los permisos necesarios.
- Edite el pool de almacenamiento cloud con credenciales que tengan los permisos necesarios.
- Si los permisos son correctos, póngase en contacto con el servicio de soporte técnico.

Error: No se ha podido comprobar el contenido del pool de almacenamiento en cloud. Error desde el punto final

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. Este error indica que algún problema de conectividad o configuración impide que StorageGRID lea el contenido del bucket de Cloud Storage Pool.

Para corregir el problema, revise el mensaje de error desde el punto final.

Error: Los objetos ya se han colocado en este cucharón

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. No puede eliminar un pool de almacenamiento en cloud si contiene datos que se movieron allí mediante ILM, datos que estaban en el depósito antes de configurar el pool de almacenamiento en cloud o datos que algún otro origen puso en el depósito después de crear el pool de almacenamiento en cloud.

Intente uno o más de estos pasos para corregir el problema:

- Siga las instrucciones para devolver objetos a StorageGRID en «"ciclo de vida de un objeto de agrupación de almacenamiento en cloud"».
- Si está seguro de que ILM no colocó los objetos restantes en el Cloud Storage Pool, elimine manualmente los objetos del bloque.

> No elimine nunca manualmente objetos de un pool de almacenamiento en cloud que haya colocado allí ILM. Si más adelante intenta acceder a un objeto eliminado manualmente desde StorageGRID, no se encuentra el objeto eliminado.

Error: El proxy encontró un error externo al intentar acceder al pool de almacenamiento de cloud

Es posible ver este mensaje de error si se configuró un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el extremo externo de S3 utilizado para el pool de almacenamiento en el cloud. Este error se produce si el servidor proxy externo no puede alcanzar el punto final de Cloud Storage Pool. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externo.

Intente uno o más de estos pasos para corregir el problema:

- Compruebe la configuración de Cloud Storage Pool (**ILM** > **agrupaciones de almacenamiento**).
- Compruebe la configuración de red del servidor proxy de almacenamiento.

Información relacionada

"Ciclo de vida de un objeto de Cloud Storage Pool"

Gestione los perfiles de código de borrado

Si es necesario, puede cambiar el nombre de un perfil de código de borrado. Es posible desactivar un perfil de código de borrado si actualmente no se está utilizando en ninguna regla de ILM.

Cambie el nombre de un perfil de código de borrado

Es posible que desee cambiar el nombre de un perfil de codificación de borrado para que sea más obvio lo que hace el perfil.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Pasos

1. Seleccione **ILM** > **codificación de borrado**.
2. Seleccione el perfil al que desea cambiar el nombre.
3. Seleccione **Cambiar nombre**.
4. Introduzca un nombre único para el perfil de código de borrado.

   El nombre del perfil de codificación de borrado se añade al nombre del pool de almacenamiento en la instrucción de ubicación para una regla de ILM.

   > Los nombres de perfil de código de borrado deben ser únicos. Se produce un error de validación si utiliza el nombre de un perfil existente, incluso si dicho perfil se ha desactivado.

5. Seleccione **Guardar**.

Desactivar un perfil de código de borrado

Puede desactivar un perfil de código de borrado si ya no tiene pensado utilizarlo y si el perfil no se está utilizando en ninguna regla de ILM.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Ha confirmado que no hay operaciones de reparación de datos codificados para borrado ni procedimientos de retirada en curso. Se devuelve un mensaje de error si intenta desactivar un perfil de código de borrado mientras se realiza alguna de estas operaciones.

Acerca de esta tarea

Al desactivar un perfil de codificación de borrado, el perfil sigue apareciendo en la página Perfiles de codificación de borrado, pero su estado es **Desactivado**.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

Ya no puede utilizar un perfil de código de borrado desactivado. No se muestra un perfil desactivado al crear las instrucciones de colocación para una regla de ILM. No puede reactivar un perfil desactivado.

StorageGRID evita que desactive un perfil de código de borrado si se cumple alguna de las siguientes condiciones:

- El perfil de código de borrado se utiliza actualmente en una regla de ILM.
- El perfil de código de borrado ya no se usa en ninguna regla de ILM, pero los datos de los objetos y los fragmentos de paridad del perfil siguen existiendo.

Pasos

1. Seleccione **ILM** > **código de borrado**.
2. Revise la columna **Status** para confirmar que el perfil de codificación de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

   No es posible desactivar un perfil de código de borrado si se utiliza en alguna regla de ILM. En el ejemplo, el perfil del Centro de datos **2+1 1** se utiliza en al menos una regla de ILM.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

3. Si el perfil se utiliza en una regla de ILM, siga estos pasos:
   a. Seleccione **ILM** > **Reglas**.
   b. Seleccione cada regla y revise el diagrama de retención para determinar si la regla utiliza el perfil de código de borrado que desea desactivar.
   c. Si la regla de ILM utiliza el perfil de código de borrado que desea desactivar, determine si la regla se utiliza en la política de ILM activa o en una política propuesta.
   d. Complete los pasos adicionales de la tabla, según el lugar en el que se utilice el perfil de código de borrado.

¿Dónde se ha utilizado el perfil?	**Pasos adicionales que se deben realizar antes de desactivar el perfil**	**Consulte estas instrucciones adicionales**
No se usa nunca en ninguna regla de ILM	No se requieren pasos adicionales. Continúe con este procedimiento.	*Ninguno*
En una regla de ILM que nunca se haya usado en ninguna política de ILM	i. Edite o elimine todas las reglas de ILM afectadas. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. ii. Continúe con este procedimiento.	"Trabaje con las reglas de ILM y las políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla de ILM que esté actualmente en la política activa de ILM	i. Clonar la política activa. ii. Quite la regla de ILM que utilice el perfil de código de borrado. iii. Añada una o varias reglas nuevas de ILM para garantizar la protección de los objetos. iv. Guarde, simule y active la nueva directiva. v. Espere a que se aplique la nueva directiva y a que los objetos existentes se muevan a nuevas ubicaciones en función de las nuevas reglas que haya agregado. **Nota:** dependiendo del número de objetos y del tamaño de su sistema StorageGRID, las operaciones de ILM pueden tardar semanas o incluso meses en mover los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Aunque puede intentar desactivar de forma segura un perfil de codificación de borrado mientras aún está asociado a los datos, la operación de desactivación fallará. Un mensaje de error le informará si el perfil aún no está listo para ser desactivado. vi. Edite o elimine la regla que ha eliminado de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. vii. Continúe con este procedimiento.	"Cree una política de ILM" "Trabaje con las reglas de ILM y las políticas de ILM"
En una regla de ILM que se encuentra actualmente en una política de ILM propuesta	i. Edite la directiva propuesta. ii. Quite la regla de ILM que utilice el perfil de código de borrado. iii. Añada una o varias reglas nuevas de ILM para garantizar que todos los objetos estén protegidos. iv. Guarde la directiva propuesta. v. Edite o elimine la regla que ha eliminado de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. vi. Continúe con este procedimiento.	"Cree una política de ILM" "Trabaje con las reglas de ILM y las políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla de ILM que está en una política histórica de ILM	i. Edite o elimine la regla. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. (La regla aparecerá ahora como una regla histórica en la política histórica.) ii. Continúe con este procedimiento.	"Trabaje con las reglas de ILM y las políticas de ILM"

e. Actualice la página Perfiles de código de borrado para asegurarse de que el perfil no se utilice en una regla de ILM.

4. Si el perfil no se utiliza en una regla de ILM, seleccione el botón de opción y seleccione **Desactivar**.

   Aparece el cuadro de diálogo Desactivar perfil de EC.

5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.
   - Si StorageGRID puede desactivar el perfil de codificación de borrado, su estado es **desactivado**. Ya no puede seleccionar este perfil para ninguna regla de ILM.
   - Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto siguen asociados a este perfil. Es posible que deba esperar varias semanas antes de volver a intentar el proceso de desactivación.

Configurar regiones (opcional solo S3)

Las reglas de ILM pueden filtrar objetos en función de las regiones donde se crean bloques S3, lo que permite almacenar objetos de diferentes regiones en distintas ubicaciones de almacenamiento.

Si desea usar una región de bloque de S3 como filtro de una regla, primero debe crear las regiones que pueden usar los bloques del sistema.

> No puede cambiar la región de un depósito después de haber creado el depósito.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

Al crear un bloque de S3, puede especificar que el bloque se cree en una región determinada. El establecimiento de una región permite que el bloque se aproxime geográficamente a los usuarios, lo que ayuda a optimizar la latencia, minimizar los costes y cumplir con los requisitos normativos.

Cuando se crea una regla de ILM, se recomienda utilizar la región asociada con un bloque de S3 como filtro avanzado. Por ejemplo, puede diseñar una regla que solo se aplique a los objetos en cubos S3 creados en la región US-West-2. Luego, puede especificar que las copias de esos objetos se coloquen en nodos de almacenamiento en un centro de datos dentro de la región para optimizar la latencia.

Al configurar regiones, siga estas directrices:

- De forma predeterminada, se considera que todos los cucharones pertenecen a la región US-East-1.
- Debe crear las regiones mediante Grid Manager para poder especificar una región no predeterminada al crear cubos con el Administrador de inquilinos o la API de Gestión de inquilinos, o con el elemento de solicitud LocationConstraint para las solicitudes de la API PUT Bucket de S3. Se produce un error si una solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.
- Debe usar el nombre exacto de la región cuando cree el bloque de S3. Los nombres de región distinguen entre mayúsculas y minúsculas. Los caracteres válidos son números, letras y guiones.

> ⓘ No se considera que la UE sea un alias para la ue-oeste-1. Si desea utilizar la región UE o eu-West-1, debe usar el nombre exacto.

- No se puede eliminar ni modificar una región si se está utilizando actualmente dentro de la política de ILM activa o la propuesta.
- Si la región utilizada como filtro avanzado en una regla de ILM no es válida, todavía es posible agregar esa regla a la directiva propuesta. Sin embargo, se produce un error si intenta guardar o activar la directiva propuesta.

  Se puede producir una región no válida si utiliza una región como filtro avanzado en una regla de ILM, pero posteriormente la elimina, o si utiliza la API de gestión de grid para crear una regla y especificar una región que no haya definido.

- Si elimina una región después de utilizarla para crear un bloque de S3, deberá volver a agregar la región si alguna vez desea utilizar el filtro avanzado restricción de ubicaciones para buscar objetos en ese bloque.

Pasos

1. Seleccione **ILM** > **Regiones**.

   Aparece la página Regiones, con las regiones definidas actualmente en la lista. **Región 1** muestra la región predeterminada, `us-east-1`, que no se puede modificar o eliminar.

2. Para agregar una región:
   a. Seleccione el icono de inserción ➕ a la derecha de la última entrada.
   b. Introduzca el nombre de una región que desea utilizar al crear bloques de S3.

      Debe utilizar este nombre de región exacto como elemento de solicitud LocationConstraint al crear el bloque de S3 correspondiente.

3. Para eliminar una región no utilizada, seleccione el icono de eliminación ✕.

   Aparece un mensaje de error si intenta eliminar una región que se utiliza actualmente en la directiva activa o la directiva propuesta.

4. Cuando haya terminado de realizar los cambios, seleccione **Guardar**.

   Ahora puede seleccionar estas regiones en la sección Advanced Filters en el paso 1 del asistente de creación de reglas de ILM. Consulte "Usar filtros avanzados en las reglas de ILM".

Cree la regla de ILM

Cree una regla de ILM: Información general

Para gestionar objetos, debe crear un conjunto de reglas de gestión de ciclo de vida de la información (ILM) y organizarlas en una política de ILM.

Cada objeto ingerido en el sistema se evalúa según la política activa. Cuando una regla de la política coincide con los metadatos de un objeto, las instrucciones de la regla determinan las acciones que StorageGRID lleva a cabo para copiar y almacenar ese objeto.

> Los metadatos de objetos no se gestionan por las reglas de ILM. En su lugar, los metadatos de objetos se almacenan en una base de datos de Cassandra en lo que se conoce como almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de objetos en cada sitio para proteger los datos frente a pérdidas.

Elementos de una regla de ILM

Una regla de ILM consta de tres elementos:

- **Criterios de filtrado**: Los filtros básicos y avanzados de una regla definen a qué objetos se aplica la regla. Si un objeto coincide con todos los filtros, StorageGRID aplica la regla y crea las copias de objeto especificadas en las instrucciones de colocación de la regla.
- **Instrucciones de colocación**: Las instrucciones de colocación de una regla definen el número, el tipo y la ubicación de las copias de objetos. Cada regla puede incluir una secuencia de instrucciones de colocación para cambiar el número, el tipo y la ubicación de las copias de objetos a lo largo del tiempo. Cuando expira el período de tiempo para una ubicación, la siguiente evaluación de ILM aplica automáticamente las instrucciones en la siguiente ubicación.
- **Comportamiento de ingesta**: El comportamiento de ingesta de una regla le permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 o Swift guarda un objeto en la cuadrícula).

Filtrado de reglas de ILM

Al crear una regla de ILM, puede especificar filtros para identificar a qué objetos se aplica la regla.

En el caso más sencillo, es posible que una regla no utilice ningún filtro. Cualquier regla que no utilice filtros se aplica a todos los objetos, por lo que debe ser la última regla (predeterminada) de una política de ILM. La regla predeterminada proporciona instrucciones de almacenamiento para objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Estos filtros le permiten aplicar una regla a cuentas de inquilino específicas, cubos S3 específicos o contenedores Swift, o ambos.

  Los filtros básicos le dan una manera sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que los registros financieros de su empresa deban almacenarse para cumplir con requisitos normativos; en cambio, los datos del departamento de marketing pueden necesitar almacenarse para facilitar las operaciones diarias. Tras crear cuentas de inquilino independientes para cada departamento o al separar los datos de los diferentes departamentos en bloques S3 independientes, puede crear fácilmente una regla que se aplique a todos los registros financieros y a una segunda regla que se aplique a todos los datos de marketing.

- Los filtros avanzados le proporcionan un control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades de objeto:
  - Tiempo de ingesta
  - Hora del último acceso
  - Todo o parte del nombre del objeto (clave)
  - Restricción de ubicación (sólo S3)
  - Tamaño del objeto
  - Metadatos del usuario
  - Etiqueta de objeto (solo S3)

Puede filtrar objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de imágenes de un hospital pueden usarse con frecuencia cuando tienen menos de 30 días de antigüedad y no suelen hacerlo después, mientras que los objetos que contienen información de visita del paciente pueden necesitar copiarse al departamento de facturación de la sede de la red sanitaria. Puede crear filtros que identifiquen cada tipo de objeto en función del nombre del objeto, el tamaño, las etiquetas de objetos de S3 o cualquier otro criterio relevante para, a continuación, crear reglas independientes para almacenar cada conjunto de objetos de la forma adecuada.

Puede combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imagen de gran tamaño de forma diferente a sus registros de proveedor, mientras que el departamento de recursos humanos podría necesitar almacenar registros de personal en una región específica e información de políticas de forma centralizada. En este caso, puede crear reglas que filtren por cuenta de arrendatario para segregar los registros de cada departamento, mientras utiliza filtros en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

Instrucciones para colocar las reglas de ILM

Las instrucciones de colocación determinan dónde, cuándo y cómo se almacenan los datos de objetos. Una regla de ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo.

Al crear instrucciones de colocación:

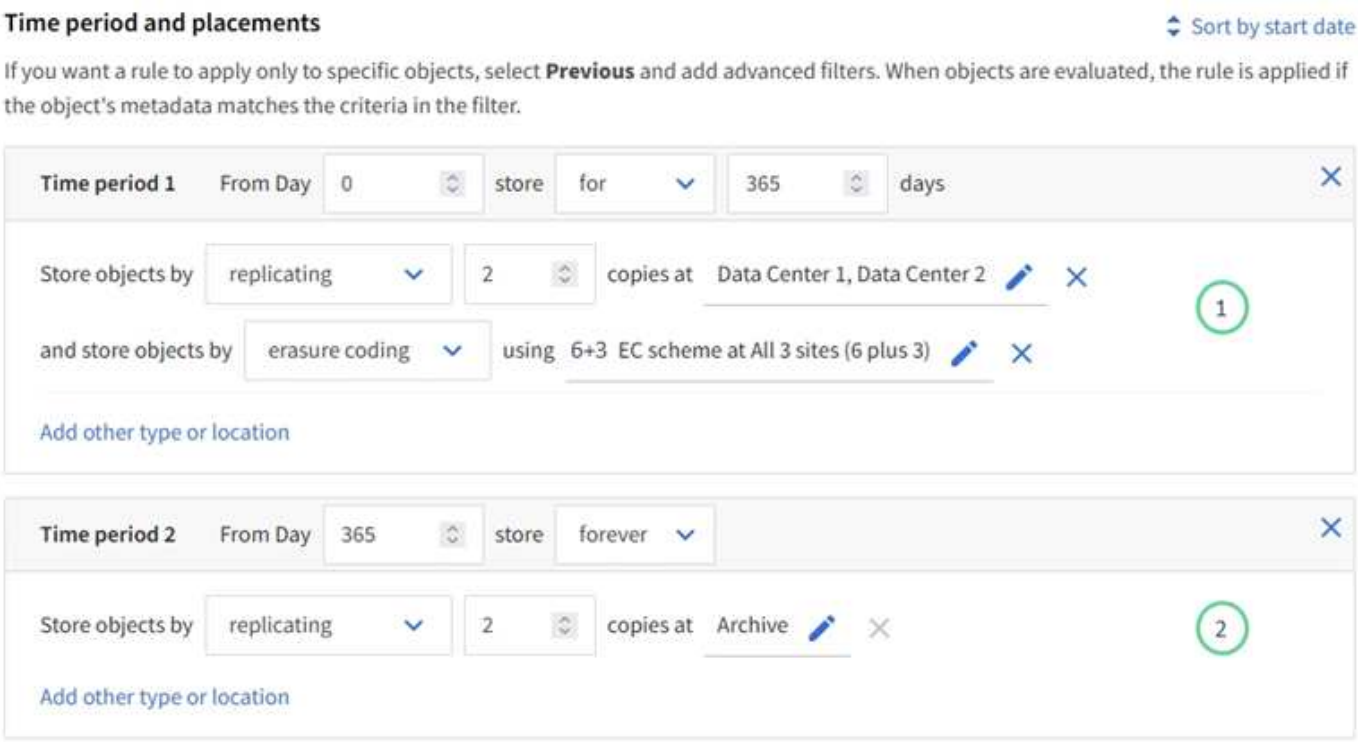
- Para empezar, especifique el tiempo de referencia, que determina cuándo se inician las instrucciones de colocación. El tiempo de referencia podría ser el momento en que un objeto se ingiere, cuando se accede a un objeto, cuando un objeto con versiones se convierte en no actual o en un tiempo definido por el usuario.
- A continuación, especifique cuándo se aplicará la ubicación en relación con el tiempo de referencia. Por ejemplo, una ubicación podría comenzar en el día 0 y continuar durante 365 días, en relación con el momento en que se ingirió el objeto.
- Por último, debe especificar el tipo de copias (codificación de replicación o borrado) y la ubicación donde se almacenan las copias. Por ejemplo, puede que desee almacenar dos copias replicadas en dos sitios diferentes.

Cada regla puede definir varias ubicaciones para un único período de tiempo y ubicaciones diferentes para diferentes períodos de tiempo.

- Para colocar objetos en varias ubicaciones durante un solo período de tiempo, seleccione **Añadir otro tipo o ubicación** para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione **Agregar otro**

período de tiempo para agregar el siguiente período de tiempo. A continuación, especifique una o más líneas dentro del período de tiempo.

En el ejemplo se muestran dos instrucciones de colocación en la página Definir ubicaciones del asistente Crear reglas de ILM.



La primera instrucción de colocación (1) tiene dos líneas para el primer año:

- La primera línea crea dos copias de objetos replicadas en dos sitios de centro de datos.
- La segunda línea crea una copia con código de borrado de 6+3 utilizando tres centros de datos.

La segunda instrucción de colocación (2) crea dos copias archivadas al cabo de un año y guarda esas copias para siempre.

Cuando defina el conjunto de instrucciones de colocación para una regla, debe asegurarse de que al menos una instrucción de colocación comienza en el día 0, de que no haya espacios entre los períodos de tiempo definidos. y que la instrucción de colocación final continúa para siempre o hasta que ya no se requiere ninguna copia de objeto.

Cuando cada período de tiempo de la regla caduca, se aplican las instrucciones de colocación del contenido para el próximo período de tiempo. Se crean nuevas copias de objetos y se eliminan todas las copias innecesarias.

Comportamiento de procesamiento de reglas de ILM

El comportamiento de la ingesta controla si las copias de objetos se colocan inmediatamente según las instrucciones de la regla o si se realizan copias provisionales y se aplican las instrucciones de colocación más adelante. Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Balanceado**: StorageGRID intenta hacer todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve éxito al cliente. Las copias especificadas

en la regla ILM se realizan cuando es posible.

- **Estricto**: Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **Confirmación doble**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Información relacionada

- "Opciones de procesamiento"
- "Ventajas, desventajas y limitaciones de las opciones de ingesta"
- "Cómo interactúan los controles de consistencia y las reglas de ILM para afectar a la protección de datos"

Regla de ILM de ejemplo

Por ejemplo, una regla de ILM podría especificar lo siguiente:

- Aplicar solo a los objetos que pertenecen al inquilino A..
- Realice dos copias replicadas de dichos objetos y almacene cada copia en un sitio diferente.
- Conservar las dos copias «`para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que se eliminen mediante una solicitud de eliminación del cliente o cuando finalice el ciclo de vida de un bloque.
- Use la opción Equilibrada para el comportamiento de ingesta: La instrucción de ubicación de dos sitios se aplica en cuanto el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible hacer inmediatamente las dos copias requeridas.

  Por ejemplo, si el sitio 2 no se puede acceder cuando el inquilino A guarda un objeto, StorageGRID realizará dos copias provisionales en los nodos de almacenamiento del sitio 1. En cuanto el sitio 2 esté disponible, StorageGRID realizará la copia necesaria en ese sitio.

Información relacionada

- "¿Qué es un pool de almacenamiento?"
- "¿Qué es un pool de almacenamiento en cloud?"

Acceda al asistente Create an ILM Rule

Las reglas de ILM permiten gestionar la ubicación de los datos de objetos con el tiempo. Para crear una regla de ILM, debe usar el asistente Create an ILM Rule.

> Si desea crear la regla de ILM predeterminada para una política, siga el "Instrucciones para crear una regla de ILM predeterminada" en su lugar.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.
- Si desea especificar a qué cuentas de arrendatario se aplica esta regla, tiene el permiso Cuentas de arrendatario o conoce el ID de cuenta de cada cuenta.
- Si desea que la regla filtre objetos en los metadatos de la última hora de acceso, las actualizaciones de la última hora de acceso deben habilitarse mediante bloque para S3 o por contenedor para Swift.

- Ha configurado los pools de Cloud Storage que desee utilizar. Consulte "Cree el pool de almacenamiento en el cloud".
- Usted está familiarizado con el "opciones de procesamiento".
- Si necesita crear una regla conforme para usarla con el bloqueo de objetos S3, ya está familiarizado con la "Requisitos para el bloqueo de objetos de S3".
- Opcionalmente, ha visto el vídeo: "Vídeo: Reglas de gestión del ciclo de vida de la información en StorageGRID 11,7".

Acerca de esta tarea

Al crear reglas de ILM:

- Considere la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Considere qué tipos de copias de objetos desea hacer (replicadas o codificadas por borrado) y el número de copias de cada objeto que se necesitan.
- Determinar qué tipos de metadatos de objetos se usan en las aplicaciones que se conectan al sistema StorageGRID. Las reglas de ILM filtran los objetos en función de sus metadatos.
- Considere dónde desea que las copias de objetos se coloquen a lo largo del tiempo.
- Decida qué opción de ingesta utilizar (Compromiso equilibrado, estricto o doble).

Pasos

1. Seleccione **ILM** > **Reglas**.

   En función del número de sitios de la cuadrícula, la regla Hacer 2 copias o la regla 1 copia por sitio se muestran en la lista de reglas.

   > Si se ha habilitado la configuración de bloqueo de objetos S3 global para el sistema StorageGRID, la tabla de resumen incluye una columna **Compatible** y los detalles de la regla seleccionada incluyen un campo **Compatible**.

2. Seleccione **Crear**. "Paso 1 (Introducir detalles)" Se mostrará el asistente Crear una regla de ILM.

Paso 1 de 3: Introduzca los detalles

El paso **Introducir detalles** del asistente Crear una regla de ILM le permite introducir un nombre y una descripción para la regla y definir filtros para la regla.

La introducción de una descripción y la definición de filtros para la regla son opcionales.

Acerca de esta tarea

Al evaluar un objeto contra un "Regla de ILM", StorageGRID compara los metadatos del objeto con los filtros de la regla. Si los metadatos del objeto coinciden con todos los filtros, StorageGRID utiliza la regla para colocar el objeto. Puede diseñar una regla para aplicarla a todos los objetos, o puede especificar filtros básicos, como uno o más nombres de cuentas de arrendatario o de bloques, o filtros avanzados, como el tamaño del objeto o los metadatos de usuario.

Pasos

1. Introduzca un nombre único para la regla en el campo **Nombre**.

2. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.

   Debe describir el propósito o la función de la regla para poder reconocerla más adelante.

3. De manera opcional, seleccione una o varias cuentas de inquilino de S3 o Swift a las que se aplica esta regla. Si esta regla se aplica a todos los inquilinos, deje este campo en blanco.

   Si no tiene el permiso de acceso raíz o las cuentas de inquilino, no puede seleccionar arrendatarios de la lista. En su lugar, introduzca el ID de inquilino o introduzca varios ID como una cadena delimitada por comas.

4. De manera opcional, especifique los bloques de S3 o los contenedores Swift a los que se aplica esta regla.

   Si se selecciona **coincide con All** (valor predeterminado), la regla se aplica a todos los bloques S3 o contenedores Swift.

5. Para los inquilinos S3, opcionalmente seleccione **Sí** para aplicar la regla solo a versiones de objetos más antiguas en cubos S3 que tienen el control de versiones activado.

   Si selecciona **Sí**, se seleccionará automáticamente la “Hora no corriente” para el Tiempo de referencia en "Paso 2 del asistente Crear una regla de ILM".

   > La hora no actual se aplica solo a objetos S3 en bloques con control de versiones activado. Consulte "Operaciones en bloques, PUT Bucket Versioning" y.. "Gestione objetos con S3 Object Lock".

   Puede utilizar esta opción para reducir el impacto del almacenamiento de objetos con versiones mediante el filtrado de versiones de objetos no actuales. Consulte "Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3".

6. Opcionalmente, seleccione **Agregar un filtro avanzado** para especificar filtros adicionales.

   Si no configura el filtrado avanzado, la regla se aplica a todos los objetos que coincidan con los filtros básicos. Para obtener más información sobre el filtrado avanzado, consulte Usar filtros avanzados en las reglas de ILM y.. Especifique varios tipos y valores de metadatos.

7. Seleccione **continuar**. "Paso 2 (Definir ubicaciones)" Se mostrará el asistente Crear una regla de ILM.

Usar filtros avanzados en las reglas de ILM

El filtrado avanzado permite crear reglas de ILM que se aplican solo a objetos específicos en función de sus metadatos. Al configurar el filtrado avanzado para una regla, debe seleccionar el tipo de metadatos que desea que coincidan, seleccionar un operador y especificar un valor de metadatos. Cuando se evalúan objetos, la regla de ILM se aplica solo a los objetos que tienen metadatos que coincidan con el filtro avanzado.

En la tabla se muestran los tipos de metadatos que se pueden especificar en los filtros avanzados, los operadores que se pueden utilizar para cada tipo de metadatos y los valores de metadatos esperados.

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tiempo de ingesta	• es • no lo es • es antes • es el o antes • es posterior • es el o después	Hora y fecha en la que se ingirió el objeto. **Nota:** Para evitar problemas de recursos al activar una nueva política de ILM, puede usar el filtro avanzado de tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de procesamiento en mayor o igual que el tiempo aproximado en el que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.
Clave	• es igual a • no es igual • contiene • no contiene • comienza con • no empieza por • termina con • no termina con	Todo o parte de una clave de objeto S3 o Swift única. Por ejemplo, quizás desee hacer coincidir los objetos que terminan con `.txt` o empiece por `test-object/`.
Hora del último acceso	• es • no lo es • es antes • es el o antes • es posterior • es el o después	Hora y fecha en la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** Si planeas hacerlo "utilizar la hora del último acceso" Como filtro avanzado, las actualizaciones de la hora del último acceso deben estar habilitadas para el depósito S3 o el contenedor Swift.
Restricción de ubicación (sólo S3)	• es igual a • no es igual	Región en la que se creó un bloque de S3. Utilice **ILM** > **Regiones** para definir las regiones que se muestran. **Nota:** un valor de US-East-1 coincidirán con objetos en cubos creados en la región US-East-1 así como con objetos en cubos que no tienen una región especificada. Consulte "Configurar regiones (opcional solo S3)".

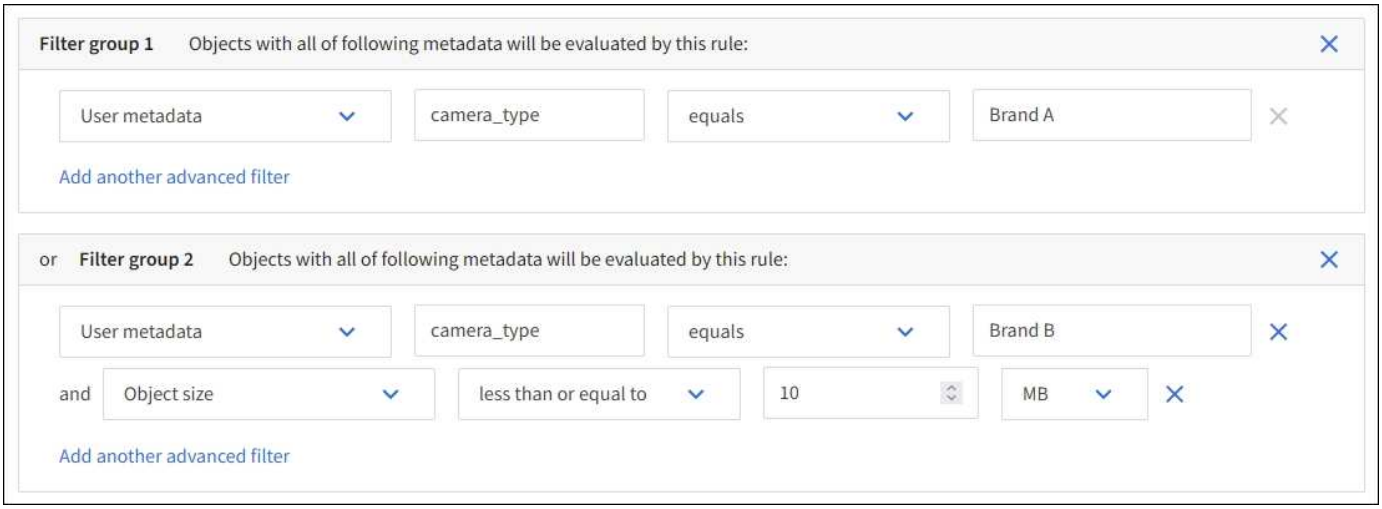
Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tamaño del objeto	• es igual a • no es igual • menor que • menor o igual que • mayor que • mayor o igual que	Tamaño del objeto. El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños. **Nota:** Para filtrar en tamaños de objetos menores de 1 MB, introduzca un valor decimal. El tipo de navegador y la configuración regional controlan si necesita utilizar un punto o una coma como separador decimal.
Metadatos del usuario	• contiene • termina con • es igual a • existe • no contiene • no termina con • no es igual • no existe • no empieza por • comienza con	Par clave-valor, donde **Nombre de metadatos de usuario** es la clave y **Valor de metadatos** es el valor. Por ejemplo, para filtrar objetos con metadatos de usuario de `color=blue`, especifique `color` Para **Nombre de metadatos de usuario**, `equals` para el operador, y. `blue` Para **Valor de metadatos**. **Nota:** Los nombres de metadatos de usuario no son sensibles a mayúsculas/minúsculas; los valores de metadatos de usuario son sensibles a mayúsculas/minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual a • existe • no contiene • no termina con • no es igual • no existe • no empieza por • comienza con	Par clave-valor, donde **Object tag name** es la clave y **Object tag value** es el valor. Por ejemplo, para filtrar objetos que tienen una etiqueta de objeto de `Image=True`, especifique `Image` Para **Nombre de etiqueta de objeto**, `equals` para el operador, y. `True` Para **Object tag value**. **Nota:** los nombres de las etiquetas de objeto y los valores de las etiquetas de objeto distinguen entre mayúsculas y minúsculas. Debe introducir estos elementos exactamente como se definieron para el objeto.

Especifique varios tipos y valores de metadatos

Al definir un filtrado avanzado, es posible especificar varios tipos de metadatos y varios valores de metadatos. Por ejemplo, si desea que una regla coincida con objetos de entre 10 MB y 100 MB de tamaño, debe seleccionar el tipo de metadatos **Tamaño de objeto** y especificar dos valores de metadatos.

- El primer valor de metadatos especifica objetos mayores o iguales a 10 MB.
- El segundo valor de metadatos especifica objetos inferiores o iguales a 100 MB.

El uso de múltiples entradas permite tener un control preciso sobre qué objetos coinciden. En el ejemplo siguiente, la regla se aplica a los objetos que tienen una Marca A o una Marca B como valor de los metadatos de usuario camera_TYPE. Sin embargo, la regla sólo se aplica a los objetos de Marca B que son menores de 10 MB.



Paso 2 de 3: Definir colocaciones

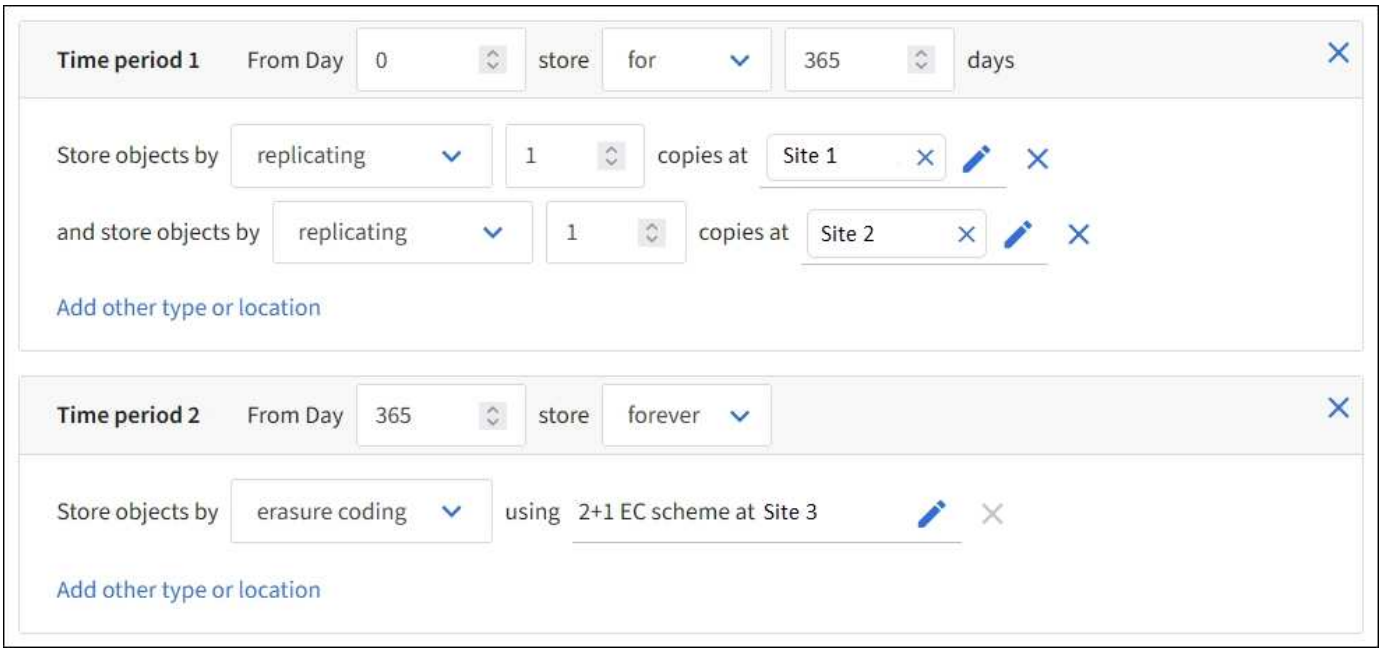
El paso **Definir ubicaciones** del asistente Crear regla de ILM le permite definir las instrucciones de colocación que determinan cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y el número de copias.

Acerca de esta tarea

Una regla de ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo. Cuando utilice más de una instrucción, los períodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar en el día 0. Las instrucciones pueden continuar para siempre o hasta que ya no necesite ninguna copia de objeto.

Cada instrucción de colocación puede tener varias líneas si desea crear diferentes tipos de copias o utilizar diferentes ubicaciones durante ese período de tiempo.

En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y una copia replicada en el sitio 2 durante el primer año. Después de un año, se realiza y se guarda una copia con código de borrado al 2+1 en una sola instalación.



Pasos

1. Para **Tiempo de referencia**, seleccione el tipo de tiempo que se utilizará al calcular la hora de inicio de una instrucción de colocación.

Opción	Descripción
Tiempo de ingesta	Hora a la que se ingirió el objeto.
Hora del último acceso	Hora a la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** Para usar esta opción, las actualizaciones de la hora de último acceso deben estar habilitadas para el cubo S3 o el contenedor Swift. Consulte "Utilice la última hora de acceso en las reglas de ILM".
Hora de creación definida por el usuario	Hora especificada en los metadatos definidos por el usuario.
Hora no corriente	"Hora no corriente" se selecciona automáticamente si seleccionaste **Sí** para la pregunta, "¿Aplicar esta regla solo a versiones de objetos anteriores (en bloques S3 con control de versiones activado)?" pulg "Paso 1 del asistente Crear una regla de ILM".

> Si desea crear una regla compatible, debe seleccionar **tiempo de ingesta**. Consulte "Gestione objetos con S3 Object Lock".

2. En la sección **Período de tiempo y ubicaciones**, introduzca una hora de inicio y una duración para el primer período de tiempo.

   Por ejemplo, puede especificar dónde almacenar objetos para el primer año (*from día 0 store for 365 days*). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:
   a. En la lista desplegable **Store objects by**, selecciona **Replicating**.
   b. Seleccione el número de copias que desea realizar.

      Aparecerá una advertencia si cambia el número de copias a 1. Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Consulte "Por qué no se debe utilizar la replicación de copia única".

      Para evitar el riesgo, realice una o más de las siguientes acciones:

      - Aumentar el número de copias durante el período de tiempo.
      - Añada copias a otros pools de almacenamiento o a un pool de almacenamiento en cloud.
      - Seleccione **código de borrado** en lugar de **Replicating**.

        Puede ignorar con toda tranquilidad esta advertencia si esta regla ya crea varias copias para todos los períodos de tiempo.

   c. En el campo **Copias en**, seleccione los pools de almacenamiento que desea agregar.

      Si especifica sólo un pool de almacenamiento, tenga en cuenta que StorageGRID sólo puede almacenar una copia replicada de un objeto en un nodo de almacenamiento dado. Si el grid incluye tres nodos de almacenamiento y selecciona 4 como número de copias, solo se crearán tres copias—una copia para cada nodo de almacenamiento.

      > Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

      Si especifica más de una agrupación de almacenamiento, tenga en cuenta estas reglas:

      - La cantidad de copias no puede ser mayor que la cantidad de pools de almacenamiento.
      - Si el número de copias es igual al número de pools de almacenamiento, se almacena una copia del objeto en cada pool de almacenamiento.
      - Si el número de copias es inferior al número de pools de almacenamiento, se almacena una copia en el sitio de procesamiento y, a continuación, el sistema distribuye las copias restantes para mantener el uso del disco entre los pools equilibrados, a la vez que se garantiza que ningún sitio obtenga más de una copia de un objeto.
      - Si los pools de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden en un solo sitio. Por este motivo, no se especifica el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) y otro pool de almacenamiento.
4. Si desea crear una copia con código de borrado:
   a. En la lista desplegable **Almacenar objetos por**, selecciona **código de borrado**.

      > El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

   b. Si no agregaste un filtro Tamaño de objeto para un valor superior a 0,2 MB, selecciona **Anterior** para volver al Paso 1. Luego, selecciona **Agregar un filtro avanzado** y establece un filtro **Tamaño de objeto** en cualquier valor mayor que 0,2 MB.

c. Seleccione el pool de almacenamiento que desea añadir y el esquema de código de borrado que desea usar.

   La ubicación de almacenamiento para una copia con código de borrado incluye el nombre del esquema de código de borrado, seguido del nombre del pool de almacenamiento.

5. Opcionalmente:
   a. Seleccione **Añadir otro tipo o ubicación** para crear copias adicionales en diferentes ubicaciones.
   b. Seleccione **Añadir otro período** para agregar diferentes períodos de tiempo.

      > Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que el período de tiempo final finalice con **para siempre**.

6. Si desea almacenar objetos en un pool de almacenamiento en cloud:
   a. En la lista desplegable **Store objects by**, selecciona **Replicating**.
   b. Seleccione el campo **Copias en** y, a continuación, seleccione un Pool de almacenamiento en la nube.

      Cuando utilice Cloud Storage Pools, tenga en cuenta estas reglas:

      - No se puede seleccionar más de un Cloud Storage Pool en una sola instrucción de colocación. De forma similar, no puede seleccionar un Cloud Storage Pool y un pool de almacenamiento en las mismas instrucciones de colocación.
      - Solo puede almacenar una copia de un objeto en cualquier Cloud Storage Pool en concreto. Aparece un mensaje de error si configura **copias** en 2 o más.
      - No es posible almacenar más de una copia de objeto en ningún pool de almacenamiento en cloud al mismo tiempo. Aparecerá un mensaje de error si varias ubicaciones que utilizan un Cloud Storage Pool tienen fechas superpuestas o si varias líneas en la misma ubicación utilizan un Cloud Storage Pool.
      - Puede almacenar un objeto en un pool de almacenamiento en cloud al mismo tiempo que el objeto se almacena como copias replicadas o codificadas de borrado en StorageGRID. Sin embargo, debe incluir más de una línea en la instrucción de colocación para el período de tiempo, de modo que pueda especificar el número y los tipos de copias para cada ubicación.

7. En el diagrama de retención, confirme las instrucciones de colocación.

   Cada línea del diagrama muestra dónde y cuándo se colocarán las copias de objeto. El color de una línea representa el tipo de copia:

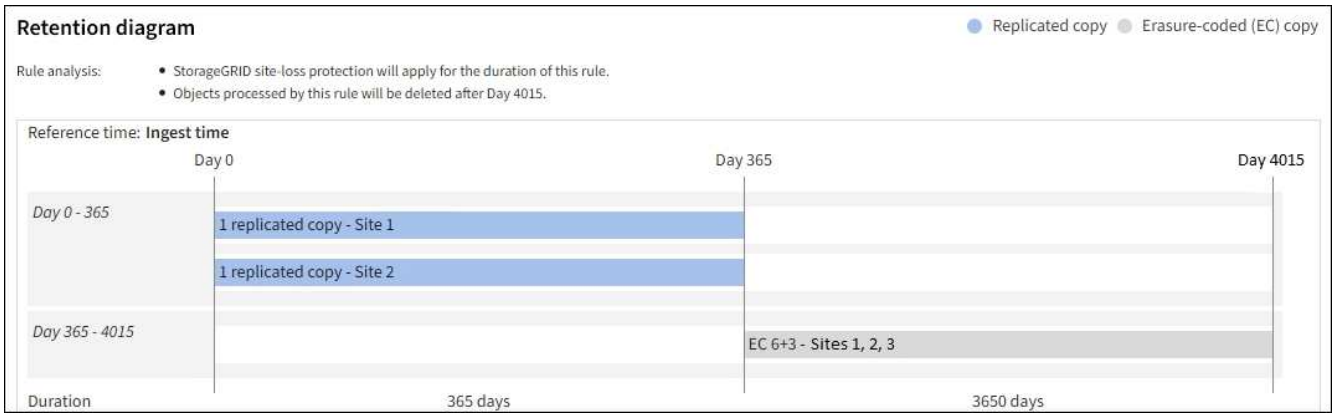
	Copia replicada
	Copia con código de borrado
	Copia de Cloud Storage Pool

   En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y una copia replicada en el sitio 2 durante el primer año. Transcurrido un año y durante 10 años más, se guardará una copia con código de borrado de 6+3 en tres instalaciones. Después de 11 años en total, los objetos se eliminarán de StorageGRID.

   La sección de análisis de reglas del diagrama de retención indica lo siguiente:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- Los objetos procesados por esta regla se eliminarán después del día 4015.

> Consulte "Habilite la protección contra pérdida de sitio."



8. Seleccione **continuar**. "Paso 3 (Seleccionar comportamiento de ingesta)" Se mostrará el asistente Crear una regla de ILM.

Utilice la última hora de acceso en las reglas de ILM

Puede utilizar la última hora de acceso como hora de referencia en una regla de ILM. Por ejemplo, quizás desee dejar objetos que se han visto en los últimos tres meses en nodos de almacenamiento local, mientras mueve objetos que no se han visto recientemente a una ubicación externa. También puede usar la última hora de acceso como filtro avanzado si desea que una regla de ILM se aplique únicamente a los objetos a los que se accedió por última vez en una fecha específica.

Acerca de esta tarea

Antes de utilizar la última hora de acceso en una regla de ILM, revise las siguientes consideraciones:

- Cuando se utiliza el último tiempo de acceso como hora de referencia, tenga en cuenta que el cambio de la hora del último acceso de un objeto no desencadena una evaluación inmediata del ciclo de vida de la información útil de la información. En su lugar, las ubicaciones del objeto se evalúan y el objeto se mueve según sea necesario cuando el ILM de segundo plano evalúa el objeto. Esto podría tardar dos semanas o más después de acceder al objeto.

  Tenga en cuenta esta latencia al crear reglas de ILM basadas en el último tiempo de acceso y evite ubicaciones que utilicen períodos de tiempo cortos (menos de un mes).

- Al utilizar la última hora de acceso como filtro avanzado o como hora de referencia, debe habilitar las actualizaciones de la última hora de acceso para los bloques S3. Puede utilizar el "Administrador de inquilinos" o la "API de gestión de inquilinos".

> Las actualizaciones del último tiempo de acceso siempre están habilitadas para contenedores Swift, pero están deshabilitadas de forma predeterminada en bloques S3.

Tenga en cuenta que habilitar las actualizaciones del tiempo de último acceso puede reducir el rendimiento, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento se produce porque StorageGRID debe actualizar los objetos con marcas de tiempo nuevas cada vez que se recuperan los objetos.

En la siguiente tabla se resume si se actualiza la hora del último acceso para todos los objetos del depósito para distintos tipos de solicitudes.

Tipo de solicitud	Si se actualiza la hora del último acceso cuando se desactivan las actualizaciones de la última hora de acceso	Si se actualiza la hora del último acceso cuando se activan las actualizaciones de la última hora de acceso
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Paso 3 de 3: Seleccione el comportamiento de ingesta

El paso **Seleccionar comportamiento de ingesta** del asistente Crear regla de ILM le permite elegir cómo se protegen los objetos filtrados por esta regla a medida que se ingieren.

Acerca de esta tarea

StorageGRID puede hacer copias provisionales y poner en cola los objetos para la evaluación de ILM más tarde, o puede hacer copias para cumplir las instrucciones de colocación de la regla de forma inmediata.

Pasos

1. Seleccione la "comportamiento de ingesta" para utilizar.

   Para obtener más información, consulte "Ventajas, desventajas y limitaciones de las opciones de ingesta".

No puede utilizar la opción Equilibrado o Estricto si la regla utiliza una de estas ubicaciones:

- Un pool de almacenamiento en cloud desde el día 0
- Un nodo de archivado al día 0
- Un pool de almacenamiento en nube o un nodo de archivado cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia

Consulte "Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto".

2. Seleccione **Crear**.

   Se crea la regla de ILM. La regla no se activa hasta que se agrega a un "Política de ILM" y esa política se activa.

   Para ver los detalles de la regla, seleccione el nombre de la regla en la página de reglas de ILM.

Cree una regla de ILM predeterminada

Antes de crear una política de ILM, debe crear una regla predeterminada para colocar los objetos que no coincidan con otra regla en la política. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los grupos y todas las versiones del objeto.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Acerca de esta tarea

La regla predeterminada es la última regla que se debe evaluar en una política de ILM, por lo que no puede utilizar ningún filtro. Las instrucciones de colocación para la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla de la política.

En esta política de ejemplo, la primera regla se aplica solo a los objetos que pertenecen a test-tenant-1. La regla predeterminada, que es última, se aplica a los objetos que pertenecen a todas las demás cuentas de arrendatario.

Al crear la regla predeterminada, tenga en cuenta estos requisitos:

- La regla predeterminada se coloca automáticamente como última regla en la directiva.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones de objetos.
- La regla predeterminada debe crear copias replicadas.

> No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deberían utilizar un filtro avanzado para evitar que los objetos más pequeños se codifiquen con el borrado.

- En general, la regla predeterminada debería retener objetos para siempre.
- Si está utilizando (o tiene previsto habilitar) la configuración de bloqueo de objetos global S3, la regla predeterminada para la directiva activa o propuesta debe ser compatible.

Pasos

1. Seleccione **ILM** > **Reglas**.
2. Seleccione **Crear**.

   Se muestra el paso 1 (introduzca detalles) del asistente Crear regla de ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre de regla**.
4. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.
5. Deja el campo **Cuentas de inquilino** en blanco.

   La regla predeterminada debe aplicarse a todas las cuentas de arrendatario.

6. Deje la selección desplegable Nombre del cucharón como **coincide con todos**.

   La regla predeterminada debe aplicarse a todos los bloques de S3 y contenedores Swift.

7. Mantenga la respuesta predeterminada, **No**, para la pregunta, "¿Aplicar esta regla solo a versiones de objetos más antiguas (en cubos S3 con control de versiones habilitado)?"
8. No agregue filtros avanzados.

   La regla predeterminada no puede especificar ningún filtro.

9. Seleccione **Siguiente**.

   Aparece el paso 2 (Definir ubicaciones).

10. En Tiempo de referencia, seleccione cualquier opción.

    Si mantuviste la respuesta predeterminada, **No**, para la pregunta "¿Aplica esta regla solo a versiones de objetos más antiguas?" La hora no actual no se incluirá en la lista desplegable. La regla predeterminada debe aplicar todas las versiones del objeto.

11. Especifique las instrucciones de colocación para la regla predeterminada.
    - La regla predeterminada debería retener objetos para siempre. Aparece una advertencia cuando activa una nueva directiva si la regla predeterminada no conserva objetos para siempre. Debe confirmar que éste es el comportamiento que espera.
    - La regla predeterminada debe crear copias replicadas.

      > No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deben incluir el filtro avanzado **Tamaño de objeto (MB) mayor que 0,2** para evitar que los objetos más pequeños sean codificados de borrado.

    - Si está utilizando (o tiene previsto habilitar) la configuración global de bloqueo de objetos S3, la regla predeterminada debe ser compatible:
      - Debe crear al menos dos copias de objetos replicados o una copia con código de borrado.
      - Estas copias deben existir en los nodos de almacenamiento durante todo el tiempo que dure cada línea en las instrucciones de colocación.
      - Las copias de objetos no se pueden guardar en un pool de almacenamiento en la nube.
      - Las copias de objetos no se pueden guardar en los nodos de archivado.
      - Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, utilizando el tiempo de ingesta como hora de referencia.
      - Al menos una línea de las instrucciones de colocación deberá ser «'para siempre».
12. Consulte el diagrama de retención para confirmar las instrucciones de colocación.
13. Seleccione **continuar**.

    Aparece el paso 3 (Seleccionar comportamiento de ingesta).

14. Seleccione la opción de ingesta que desea utilizar y seleccione **Crear**.

Cree una política de ILM

Cree una política de ILM: Información general

Una política de gestión de ciclo de vida de la información (ILM) es un conjunto ordenado de reglas de ILM que determinan el modo en que el sistema StorageGRID gestiona los datos de objetos a lo largo del tiempo.

Al crear una política de ILM, para comenzar, debe seleccionar y organizar las reglas de ILM. A continuación, se comprueba el comportamiento de la directiva propuesta simulándola de objetos ingeridos previamente. Cuando esté satisfecho de que la directiva propuesta funcione según lo previsto, puede activarla para crear la directiva activa.

> Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Política de ILM predeterminada

Al instalar StorageGRID y añadir sitios, se crea automáticamente una política de ILM predeterminada. Si su grid contiene un sitio, la política predeterminada contiene una regla predeterminada que replica dos copias de cada objeto del sitio. Si la cuadrícula contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

Si la política predeterminada no cumple con sus requisitos de almacenamiento, puede crear sus propias reglas y políticas. Consulte "Qué es una regla de ILM" y.. "Creación de una política de ILM propuesta".

¿Cómo evalúa objetos una política de ILM?

La política activa de ILM para su sistema StorageGRID controla la ubicación, la duración y la protección de datos de todos los objetos.

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan según el conjunto ordenado de reglas de ILM en la política activa, de la siguiente manera:

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se procesa según el comportamiento de procesamiento de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa con cada regla subsiguiente de la política hasta que se realiza una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican las instrucciones de comportamiento de procesamiento y colocación de la regla predeterminada de la directiva. La regla predeterminada es la última regla de una directiva. La regla predeterminada debe aplicarse a todos los inquilinos, todos los cubos y todas las versiones de objetos y no puede utilizar ningún filtro avanzado.

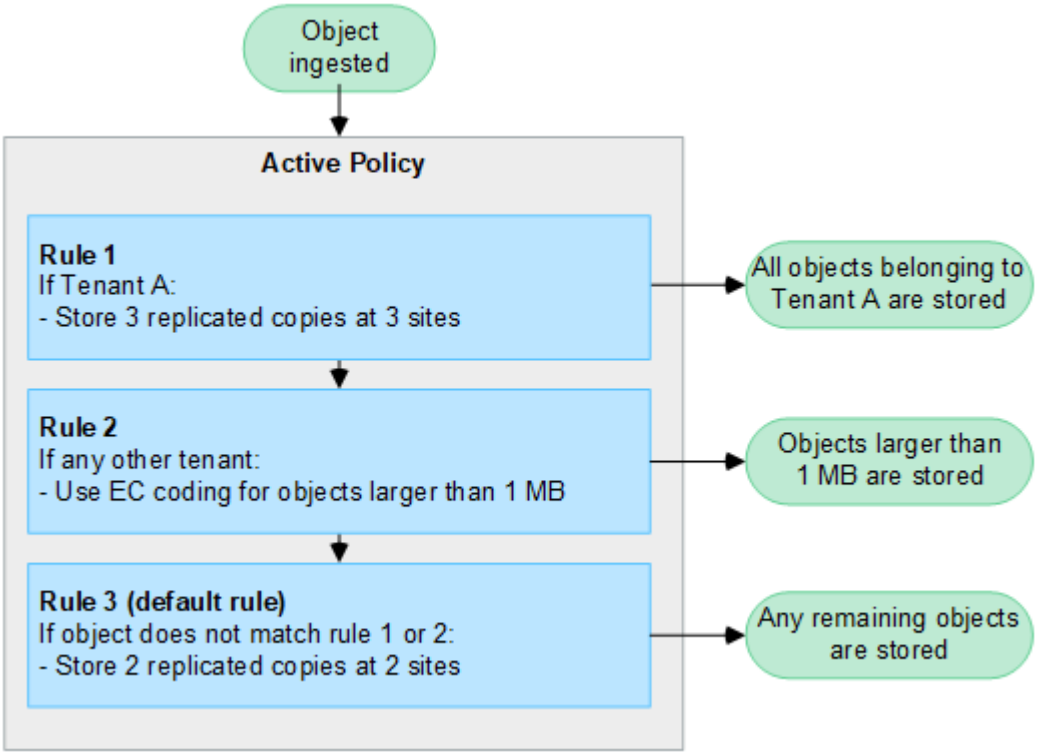
Ejemplo de política de ILM

Por ejemplo, una política de ILM podría contener tres reglas de ILM que especifiquen lo siguiente:

- **Regla 1: Copias replicadas para el Inquilino A**
  - Haga coincidir todos los objetos que pertenecen al inquilino A..

- Almacene estos objetos como tres copias replicadas en tres sitios.
- Los objetos que pertenecen a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.

- **Regla 2: Codificación de borrado para objetos mayores de 1 MB**
  - Hacer coincidir todos los objetos de otros inquilinos, pero solo si son mayores de 1 MB. Estos objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones.
  - No coincide con los objetos de 1 MB o menos, por lo que estos objetos se evalúan con la Regla 3.
- **Regla 3: 2 copias 2 data centers** (predeterminado)
  - Es la última regla y la predeterminada de la política. No utiliza filtros.
  - Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenezcan al arrendatario A que tengan 1 MB o menos).



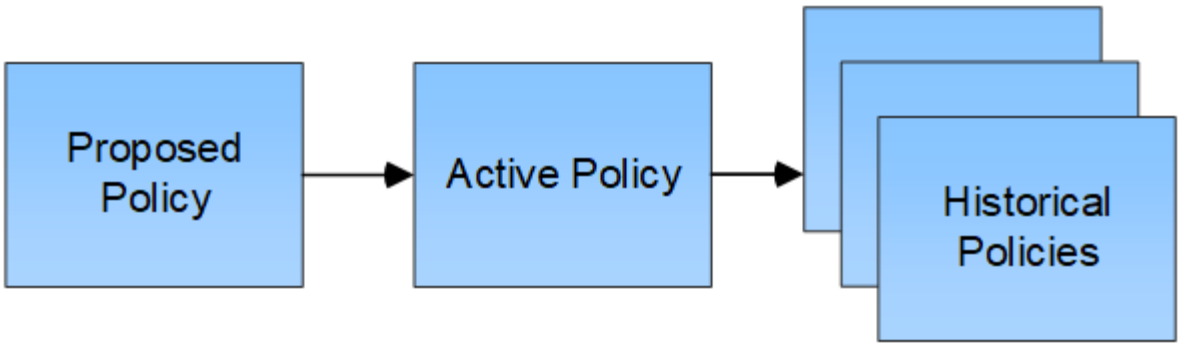
¿Qué son las políticas propuestas, activas e históricas?

Todos los sistemas StorageGRID deben tener una política de ILM activa. Un sistema StorageGRID también puede tener una política de ILM propuesta y cualquier número de políticas históricas.

Cuando se crea por primera vez una política de ILM, se crea una política propuesta seleccionando una o varias reglas de ILM y ordenándolas en un orden específico. Después de simular la política propuesta para confirmar su comportamiento, la activa para crear la política activa.

Cuando se activa una nueva política de ILM, StorageGRID utiliza esa política para gestionar todos los objetos, incluidos los objetos existentes y los objetos recién procesados. Es posible que los objetos existentes se muevan a nuevas ubicaciones cuando se implementen las reglas de ILM en la nueva política.

La activación de la directiva propuesta hace que la directiva previamente activa se convierta en una directiva histórica. Las políticas históricas de ILM no se pueden eliminar.



Consideraciones que tener en cuenta para crear una política de ILM

- Utilice únicamente la política proporcionada por el sistema, la política de copias de línea base 2, en los sistemas de prueba. Para StorageGRID 11,6 y versiones anteriores, la regla Crear 2 copias en esta política utiliza el pool de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

> El pool de almacenamiento Todos los nodos de almacenamiento se crea automáticamente durante la instalación de StorageGRID 11,6 y versiones anteriores. Si actualiza a una versión posterior de StorageGRID, el pool de Todos los nodos de almacenamiento seguirá existiendo. Si instala StorageGRID 11,7 o una versión posterior como una instalación nueva, no se crea el pool Todos los nodos de almacenamiento.

- Al diseñar una nueva política, tenga en cuenta todos los diferentes tipos de objetos que se podrían procesar en el grid. Asegúrese de que la política incluye reglas para coincidir y colocar estos objetos según sea necesario.
- Mantenga la política de ILM de la forma más sencilla posible. Esto evita situaciones potencialmente peligrosas en las que los datos de objetos no se protegen como se deben realizar cambios en el sistema StorageGRID a lo largo del tiempo.
- Asegúrese de que las reglas de la política están en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior. Por ejemplo, si la primera regla de una política coincide con un objeto, ese objeto no será evaluado por ninguna otra regla.
- La última regla de todas las políticas de ILM es la regla de ILM predeterminada, que no puede usar ningún filtro. Si un objeto no ha sido coincidente con otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se retiene.
- Antes de activar una nueva política, revise los cambios que realice la política en la ubicación de objetos existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Cree una política de ILM propuesta

Puede crear una política de ILM propuesta desde cero o clonar la política activa actual si desea empezar con el mismo conjunto de reglas.

Antes de crear su propia política, compruebe que "Política de ILM predeterminada" no cumple los requisitos de almacenamiento.

Si la "Se ha activado la configuración de bloqueo de objeto global S3", Debe asegurarse de que la política de ILM cumple con los requisitos de los depósitos que tienen S3 Object Lock activado. En esta sección, siga las instrucciones que mencionan tener S3 Object Lock habilitado.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Ya tienes "Reglas de ILM creadas" En función de si el bloqueo de objetos S3 está activado.

S3 Bloqueo de objetos no activado

- Ya tienes "Se han creado las reglas de ILM" desea agregar a la política propuesta. Según sea necesario, puede guardar una directiva propuesta, crear reglas adicionales y, a continuación, editar la directiva propuesta para agregar las nuevas reglas.
- Ya tienes "Se ha creado una regla de ILM predeterminada" que no contiene ningún filtro.

S3 Bloqueo de objetos activado

- La "La configuración de bloqueo de objetos global S3 ya está activada" Para el sistema StorageGRID.
- Ya tienes "Se han creado las reglas de ILM conforme a las normativas y no conformes" desea agregar a la política propuesta. Según sea necesario, puede guardar una directiva propuesta, crear reglas adicionales y, a continuación, editar la directiva propuesta para agregar las nuevas reglas.
- Ya tienes "Se ha creado una regla de ILM predeterminada" para la directiva que cumple con las normativas.

- Opcionalmente, ha visto el vídeo: "Vídeo: Políticas de gestión del ciclo de vida de la información en StorageGRID 11,7"

Consulte también "Cree una política de ILM: Información general".

Acerca de esta tarea

Algunos de los motivos típicos para crear una política de ILM propuesta son:

- Ha añadido un sitio nuevo y debe utilizar nuevas reglas de ILM para colocar objetos en dicho sitio.
- Está decomisionado un sitio y debe eliminar todas las reglas de ILM que hacen referencia al sitio.
- Se ha agregado un nuevo inquilino que tiene requisitos especiales de protección de datos.
- Comenzó a utilizar un pool de almacenamiento en el cloud.

Utilice únicamente la política proporcionada por el sistema, la política de copias de línea base 2, en los sistemas de prueba. Para StorageGRID 11,6 y versiones anteriores, la regla predeterminada de esta política utiliza el pool de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

Pasos

1. Seleccione **ILM** > **políticas**.

   Si la configuración global Bloqueo de objetos S3 está habilitada, la página de políticas de ILM indica qué reglas de ILM son compatibles.

2. Determine cómo desea crear la política de ILM propuesta.

Empieza desde cero

1. Si actualmente existe una política de ILM propuesta, selecciona **Política propuesta** > **Acciones** > **Eliminar**.

   No puede crear una nueva política propuesta si ya existe una política propuesta.

2. Selecciona **Crear política propuesta** > **Crear nueva política**.

Comience con reglas de la política activa

1. Si actualmente existe una política de ILM propuesta, selecciona **Política propuesta** > **Acciones** > **Eliminar**.

   No puede clonar la política activa si ya existe una política propuesta.

2. Selecciona **Crear política propuesta** > **Clonar política activa**.

Edite la política propuesta existente

1. Selecciona **Política propuesta** > **Acciones** > **Editar**.

1. En el campo **Nombre de política propuesto**, introduzca un nombre único para la política propuesta.
2. En el campo **Motivo del cambio**, introduzca el motivo por el que está creando una nueva política propuesta.
3. Para agregar reglas a la política, selecciona **Seleccionar reglas**. Seleccione un nombre de regla para ver la configuración de esa regla.

   Periódicamente, la lista de reglas se actualiza automáticamente para reflejar las adiciones o eliminaciones. Si una regla se elimina después de seleccionarla, aparece un mensaje de error.

   Si está clonando una política:

   - Se seleccionan las reglas que utiliza la política que se está clonando.
   - Si la política que está clonando usa reglas sin filtros que no sean la regla predeterminada, se le solicitará que elimine todas las reglas, excepto una de ellas.
   - Si la regla predeterminada usa un filtro, se le solicitará que seleccione una nueva regla predeterminada.
   - Si la regla predeterminada no es la última regla, puede mover la regla al final de la nueva política.

S3 Bloqueo de objetos no activado

1. Seleccione una regla predeterminada para la política propuesta. Para crear una nueva regla predeterminada, seleccione **ILM rules page**.

   La regla predeterminada se aplica a cualquier objeto que no coincida con otra regla de la política. La regla predeterminada no puede utilizar ningún filtro y siempre se evalúa en último lugar.

   > No utilice la regla Make 2 copies como regla predeterminada para una política. La regla make 2 copies utiliza un único pool de almacenamiento, todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

S3 Bloqueo de objetos activado

1. Seleccione una regla predeterminada para la política propuesta. Para crear una nueva regla predeterminada, seleccione **ILM rules page**.

   La lista de reglas contiene solo las reglas que son compatibles y no utilizan ningún filtro.

   > No utilice la regla Make 2 copies como regla predeterminada para una política. La regla make 2 copies utiliza un único pool de almacenamiento, todos los nodos de almacenamiento, que contiene todos los sitios. Si utiliza esta regla, es posible que se coloquen varias copias de un objeto en el mismo sitio.

2. Si necesita una regla diferente para los objetos en cubos S3 no compatibles, seleccione **Incluir una regla sin filtros para cubos S3 no compatibles** y seleccione una regla no compatible que no use un filtro.

   Por ejemplo, es posible que desee utilizar un pool de almacenamiento en la nube para almacenar objetos en depósitos que no tienen S3 Object Lock habilitado.

   > Sólo puede seleccionar una regla no compatible que no utilice un filtro.

Consulte también "Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3".

1. Cuando haya terminado de seleccionar la regla predeterminada, seleccione **Continuar**.
2. Para el paso Otras reglas, seleccione cualquier otra regla que desee agregar a la política. Estas reglas utilizan al menos un filtro (cuenta de arrendatario, nombre de depósito, filtro avanzado o tiempo de referencia no actual). Luego selecciona **Seleccionar**.

   La ventana Crear una política propuesta muestra ahora las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima.

   Si el bloqueo de objetos S3 está activado y también seleccionó una regla “predeterminado” no compatible, esa regla se agrega como la última regla de la política.

   > Aparece una advertencia si alguna regla no retiene los objetos para siempre. Al activar esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurran las instrucciones de colocación de la regla por defecto (a menos que un ciclo de vida del depósito mantenga los objetos durante un período de tiempo más largo).

3. Arrastre las filas de las reglas no predeterminadas para determinar el orden en el que se evaluarán estas reglas.

   No puede mover la regla predeterminada. Si el bloqueo de objetos S3 está activado, tampoco puede mover la regla “predeterminado” no compatible si se ha seleccionado una.

   > Debe confirmar que las reglas de ILM se encuentran en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior.

4. Según sea necesario, seleccione **Seleccionar reglas** para agregar o eliminar reglas.
5. Cuando haya terminado, seleccione **Guardar**.
6. Vaya a. "Simule una política de gestión de la vida útil". Siempre debe simular una política propuesta antes de activarla para asegurarse de que funciona como se esperaba.

Simule una política de gestión de la vida útil

Simule una política propuesta sobre objetos de prueba antes de activar la política y aplicarla a sus datos de producción. La ventana de simulación proporciona un entorno independiente que es seguro para las políticas de prueba antes de que se activen y apliquen a los datos en el entorno de producción.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Conoce el bloque/clave-objeto de S3 o el contenedor/nombre-objeto Swift para cada objeto que desea probar.

Acerca de esta tarea

Seleccione cuidadosamente los objetos que desea que pruebe la política propuesta. Para simular una política completamente, debe probar al menos un objeto para cada filtro en cada regla.

Por ejemplo, si una política incluye una regla para que coincida con los objetos del bloque A y otra regla para que coincidan con los objetos del bloque B, debe seleccionar al menos un objeto del bloque A y un objeto del bloque B para probar la política a fondo. También debe seleccionar al menos un objeto de otro bloque para probar la regla predeterminada.

Al simular una directiva, se aplican las siguientes consideraciones:

- Después de realizar cambios en una directiva, guarde la directiva propuesta. A continuación, simule el comportamiento de la directiva propuesta guardada.
- Cuando se simula una política, las reglas de ILM en la política filtran los objetos de prueba, de modo que se puede ver qué regla se aplicó a cada objeto. Sin embargo, no se crean copias de objeto y no se coloca ningún objeto. Al ejecutar una simulación no se modifican los datos, las reglas ni la política de ningún modo.
- La ventana de política propuesta de simulación conserva los objetos que ha probado hasta que seleccione **Borrar todo** o el icono Eliminar ✕ Para cada objeto de la lista de resultados de Simulation.
- Simulation devuelve el nombre de la regla coincidente. Para determinar qué pool de almacenamiento o perfil de código de borrado está en vigor, seleccione el nombre de la regla para ir a la página de detalles de la regla, donde puede ver el diagrama de retención y otros detalles sobre la regla.

- Si el control de versiones S3 está activado, puede introducir el ID de versión para la versión del objeto que desea utilizar para la simulación.

Pasos

1. "Crear una política propuesta".
2. Use un cliente S3 o Swift o el "Consola de S3 de experimental", Que está disponible en el Administrador de arrendatarios para cada arrendatario, procese los objetos necesarios para probar cada regla.
3. En la página de política de ILM, pestaña Política propuesta, seleccione **Simular**.
4. En el campo **Object**, ingrese el S3 `bucket/object-key` O el Swift `container/object-name` para un objeto de prueba. Por ejemplo: `bucket-01/filename.png`.
5. Opcionalmente, introduzca un ID de versión para el objeto en el campo **ID de versión**.
6. Seleccione **simular**.
7. En la sección Resultados de Simulation, confirme que la regla correcta coincide con cada objeto.

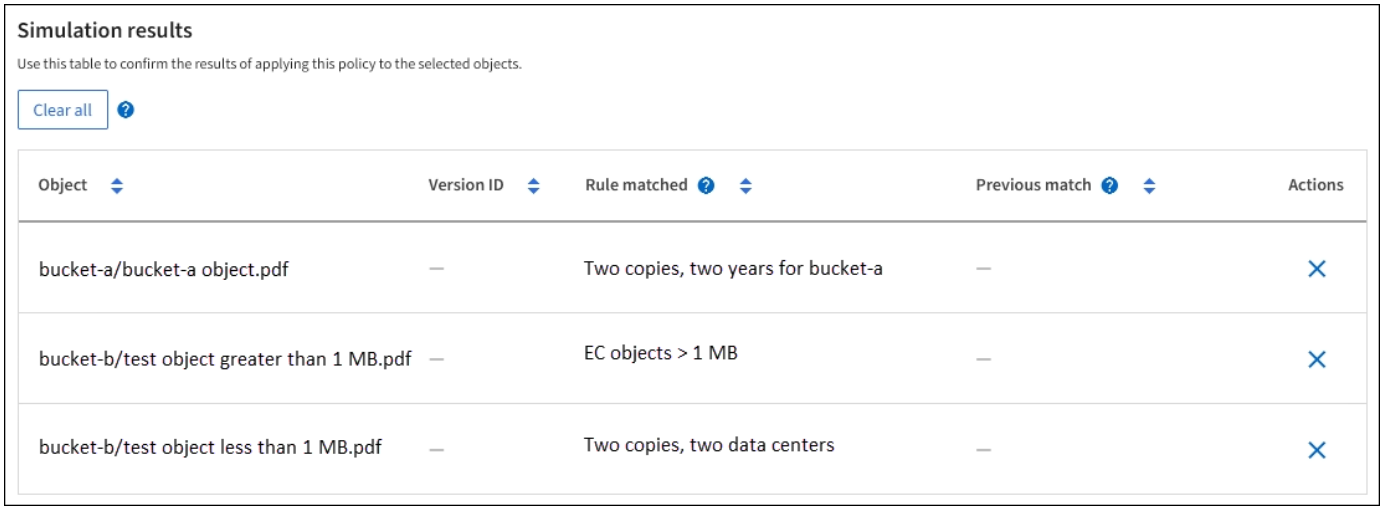
Ejemplo 1: Verifique las reglas al simular una política de ILM propuesta

En este ejemplo se describe cómo verificar reglas al simular una política propuesta.

En este ejemplo, la **política de ILM de ejemplo** se está simulando contra los objetos ingeridos en dos bloques. La política incluye tres reglas, como sigue:

- La primera regla, **dos copias, dos años para el segmento a**, se aplica sólo a los objetos en el bloque a.
- La segunda regla, **objetos EC > 1 MB**, se aplica a todos los cubos pero filtra a los objetos superiores a 1 MB.
- La tercera regla, **dos copias, dos centros de datos**, es la regla por defecto. No incluye ningún filtro ni utiliza el tiempo de referencia no corriente.

Después de simular la política, confirme que cada objeto ha coincidido con la regla correcta.



En este ejemplo:

- `bucket-a/bucket-a object.pdf` coincide correctamente con la primera regla, que filtra los objetos de `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` está en `bucket-b`, así que no coincide con la

primera regla. En lugar de ello, la segunda regla coincide correctamente, que filtra los objetos de más de 1 MB.

- `bucket-b/test object less than 1 MB.pdf` no coincide con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye ningún filtro.

Ejemplo 2: Reordenación de reglas al simular una política de ILM propuesta

En este ejemplo se muestra cómo puede reordenar las reglas para cambiar los resultados al simular una directiva.

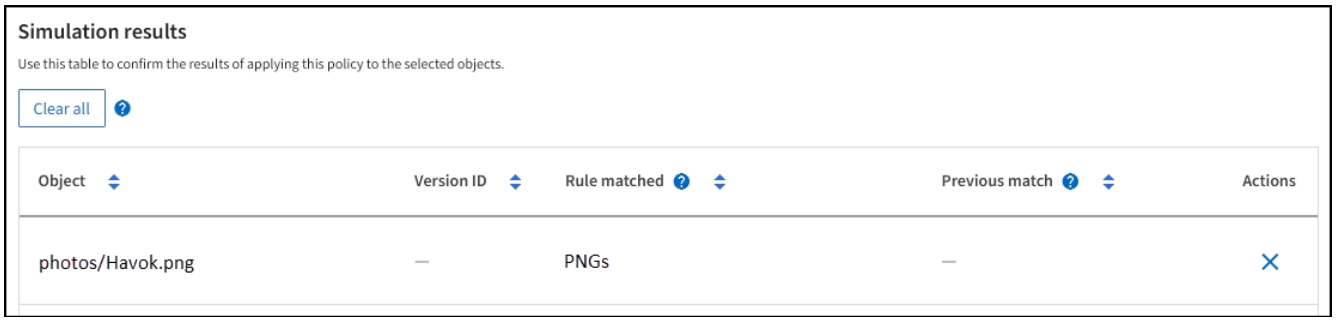
En este ejemplo, se está simulando la política **Demo**. Esta política, que está destinada a encontrar objetos que tienen metadatos de usuario de series=x-men, incluye tres reglas de la siguiente manera:

- La primera regla, **PNgs**, filtra los nombres de clave que terminan en `.png`.
- La segunda regla, **X-men**, se aplica sólo a los objetos para el arrendatario A y filtros para `series=x-men` metadatos del usuario.
- La última regla, **dos copias de dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.

Pasos

1. Después de agregar las reglas y guardar la directiva, seleccione **simular**.
2. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

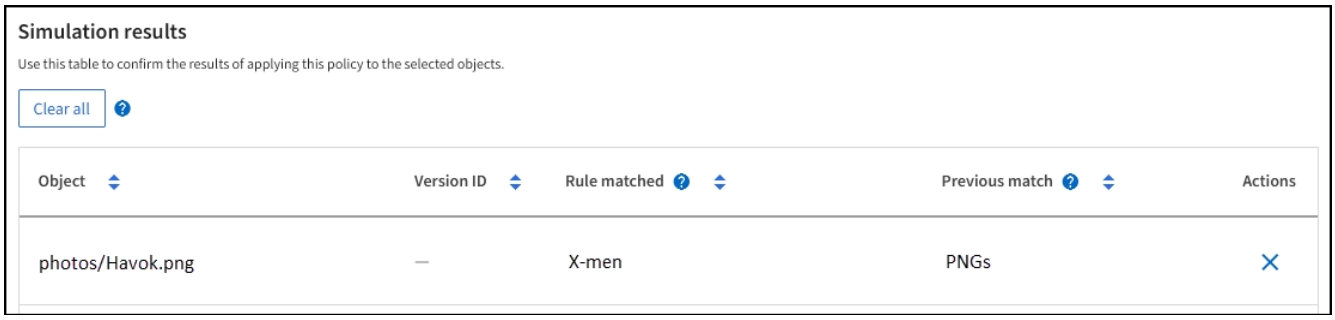
   Aparecen los resultados de Simulation, que muestran la `Havok.png` El objeto coincide con la regla **PNgs**.



   Sin embargo, `Havok.png` Estaba destinado a probar la regla **X-MEN**.

3. Para resolver el problema, vuelva a ordenar las reglas.
   a. Seleccione **Finish** para cerrar la ventana Simulate ILM Policy.
   b. Selecciona **Acciones** > **Editar** para editar la política.
   c. Arrastre la regla **X-men** hasta la parte superior de la lista.
   d. Seleccione **Guardar**.
4. Seleccione **simular**.

   Los objetos probados anteriormente se vuelven a evaluar con la directiva actualizada y se muestran los nuevos resultados de simulación. En el ejemplo, la columna Regla coincidente muestra que la `Havok.png` Ahora Object coincide con la regla de metadatos X-men, según lo esperado. La columna Coincidencia anterior muestra que la regla NGs coincide con el objeto en la simulación anterior.

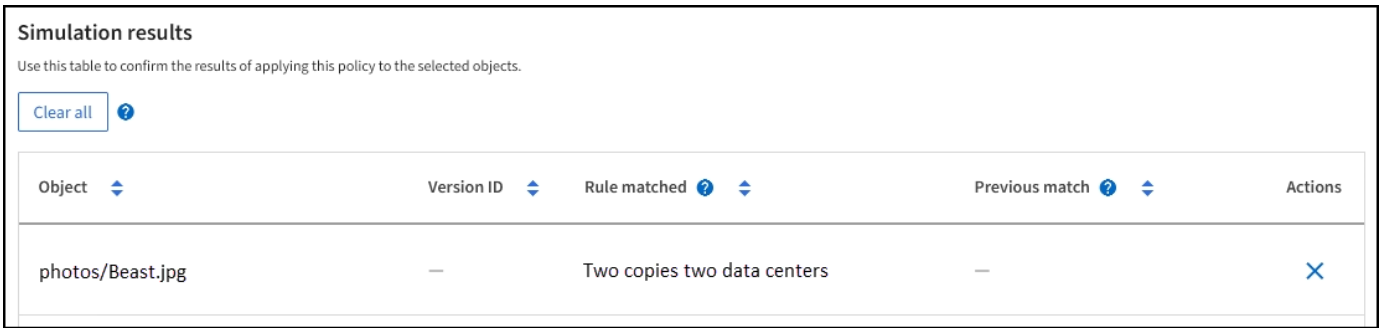


Si permanece en la pestaña Política propuesta, puede volver a simular una política después de realizar cambios sin necesidad de volver a introducir los nombres de los objetos de prueba.

Ejemplo 3: Corrección de una regla al simular una política de ILM propuesta

Este ejemplo muestra cómo simular una política, corregir una regla en la política y continuar con la simulación.

En este ejemplo, se está simulando la política **Demo**. Esta política está destinada a encontrar objetos que tienen `series=x-men` metadatos del usuario. Sin embargo, se produjeron resultados inesperados al simular esta política con la `Beast.jpg` objeto. En lugar de coincidir con la regla de metadatos de X-men, el objeto coincide con la regla predeterminada, dos copias de dos centros de datos.



Cuando un objeto de prueba no coincide con la regla esperada de la directiva, debe examinar cada regla de la directiva y corregir cualquier error.

Pasos

1. Seleccione **Finalizar** para cerrar el diálogo de políticas de simulación. En la pestaña de política propuesta, seleccione **Diagrama de retención**. A continuación, seleccione **Expandir todo** o **Ver detalles** para cada regla según sea necesario.
2. Revise la cuenta de arrendatario de la regla, el tiempo de referencia y los criterios de filtrado.

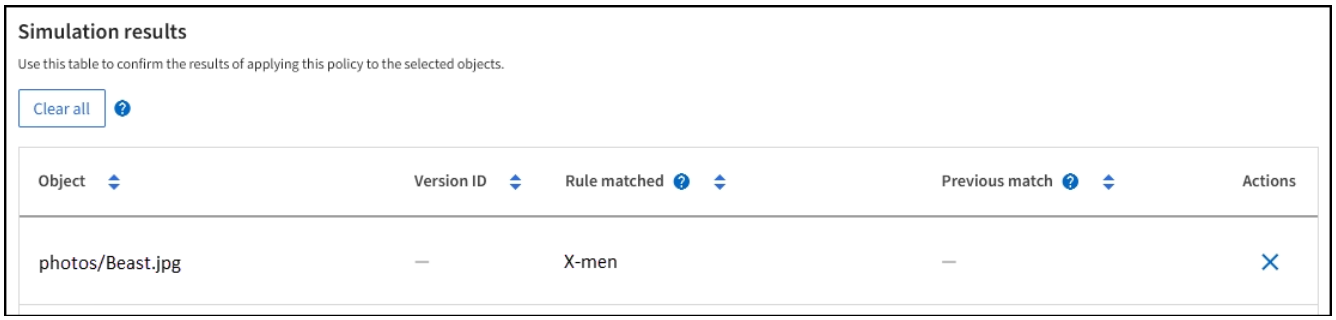
   Como ejemplo, supongamos que los metadatos para la regla X-men se ingresaron como "`x-men01`" en lugar de "`x-men`".

3. Para resolver el error, corrija la regla de la siguiente manera:
   - Si la regla forma parte de la política propuesta, puede clonar la regla o quitar la regla de la política y editarla.
   - Si la regla forma parte de la política activa, debe clonar esa regla. No puede editar ni eliminar una regla de la política activa.

Opción	Pasos
Clone la regla	i. Seleccione **ILM** > **Reglas**. ii. Seleccione la regla incorrecta y seleccione **Clonar**. iii. Introduce un nombre para la nueva regla, cambia la información incorrecta y selecciona **Crear**. iv. Seleccione **ILM** > **Políticas** > **Política propuesta**. v. Selecciona **Acciones** > **Editar**. vi. Seleccione **Seleccionar reglas** y, a continuación, seleccione **Continuar** para aceptar la misma regla predeterminada. vii. En el paso Seleccionar otras reglas, seleccione la casilla de verificación para la nueva regla, desactive la casilla de verificación para la regla original y seleccione **Seleccionar**. viii. Si es necesario, reordene las reglas arrastrando la nueva regla a la ubicación correcta. ix. Seleccione **Guardar**.
Edite la regla	i. Seleccione **ILM** > **Políticas** > **Política propuesta** y elimine la regla que desea editar. ii. Seleccione **ILM** > **Reglas**. iii. Seleccione la regla que desea editar y seleccione **Editar**. O seleccione la casilla de verificación de la regla y seleccione **Acciones** > **Editar**. iv. Cambie la información incorrecta para cada parte del asistente y, a continuación, seleccione **Actualizar**. v. Seleccione **ILM** > **Políticas** > **Política propuesta**. vi. Selecciona **Acciones** > **Editar**. vii. Seleccione **Seleccionar reglas** y, a continuación, seleccione **Continuar** para aceptar la misma regla predeterminada. viii. En el cuadro de diálogo Seleccionar otras reglas, seleccione la casilla de verificación para la regla corregida, seleccione **Seleccionar** y luego seleccione **Guardar**. ix. Arrastre las filas de las reglas no predeterminadas para determinar el orden en el que se evaluarán estas reglas.

4. Vuelva a ejecutar la simulación.

   En este ejemplo, la regla X-men corregida ahora coincide con `Beast.jpg` objeto basado en `series=x-men` los metadatos del usuario, según lo esperado.



Active la política de ILM

Después de añadir reglas de ILM a una política de ILM propuesta, simular la política y confirmar que se comporta como esperaba, está listo para activar la política propuesta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha guardado y simulado la política de ILM propuesta.

> Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable. Revise y simule cuidadosamente la directiva antes de activarla para confirmar que funcionará según lo previsto. + Al activar una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los objetos existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Acerca de esta tarea

Cuando activa una política de ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva directiva activa no surta efecto hasta que todos los nodos de grid estén disponibles para recibir la nueva directiva. En algunos casos, el sistema espera implementar una nueva política activa para garantizar que los objetos de cuadrícula no se eliminen accidentalmente.

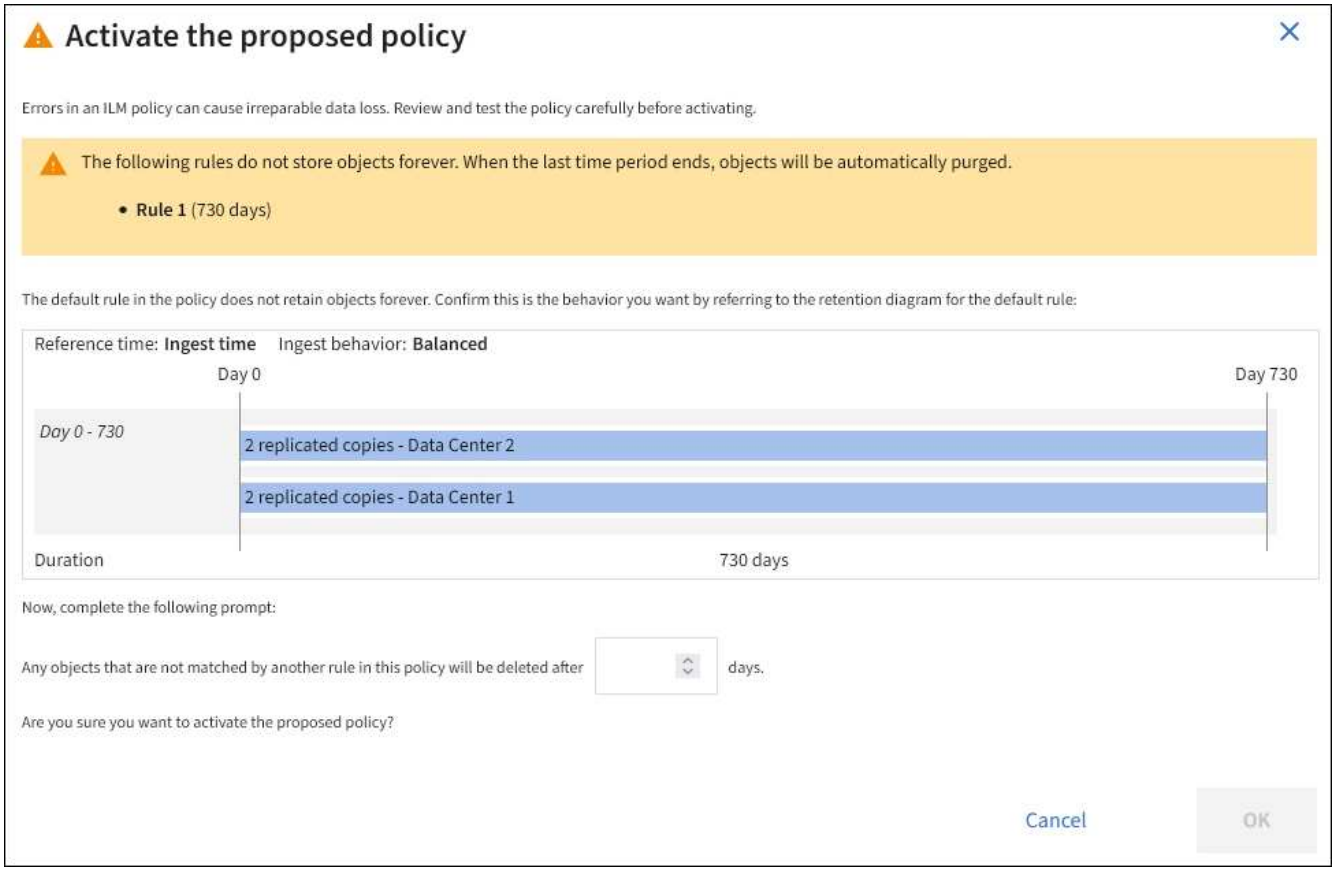
- Si realiza cambios en las políticas que aumentan la redundancia o la durabilidad de los datos, estos cambios se implementan de inmediato. Por ejemplo, si activa una nueva política que incluye una regla de tres copias en lugar de una regla de dos copias, dicha política se implementará de forma inmediata porque aumenta la redundancia de datos.
- Si realiza cambios en las políticas que podrían reducir la redundancia o la durabilidad de los datos, dichos cambios no se implementarán hasta que todos los nodos de grid estén disponibles. Por ejemplo, si activa una nueva política que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva política aparecerá en la pestaña Política activa, pero no surtirá efecto hasta que todos los nodos estén en línea y disponibles.

Pasos

1. Cuando esté listo para activar una política propuesta, seleccione **Políticas de ILM** > **Política propuesta** y, a continuación, seleccione **Activar**.

   Aparecerá un mensaje de advertencia en el que se le pedirá que confirme que desea activar la directiva propuesta.

Aparece un mensaje de advertencia si la regla por defecto no retiene los objetos para siempre. En este ejemplo, el diagrama de retención muestra que la regla predeterminada eliminará objetos después de 730 días (2 años). Debe escribir **730** en el cuadro de texto para reconocer que cualquier objeto que no coincida con otra regla de la política se eliminará de StorageGRID después de 730 días.



2. Seleccione **OK**.

Resultado

Cuando se activa una nueva política de ILM:

- La política se muestra en la pestaña Active policy. La entrada Fecha de inicio indica la fecha y la hora en que se activó la política.
- La política activa anteriormente aparece en la pestaña Historial de políticas. Las entradas Fecha de inicio y Fecha de finalización indican cuándo se activó la política y cuándo ya no estaba en vigor.

Información relacionada

"Ejemplo 6: Cambiar una política de ILM"

Comprobar una política de ILM con la búsqueda de metadatos de objetos

Después de activar una política de ILM, debe procesar objetos de prueba representativos en el sistema StorageGRID. A continuación, debe realizar una búsqueda de metadatos de objetos para confirmar que las copias se están creando como intencionadas y se encuentran en las ubicaciones correctas.

Antes de empezar

- Tiene un identificador de objeto, que puede ser uno de los siguientes:
  - **UUID**: Identificador único universal del objeto. Introduzca el UUID en toda la mayúscula.
  - **CBID**: Identificador único del objeto dentro de StorageGRID. Es posible obtener el CBID de un objeto del registro de auditoría. Introduzca el CBID en todas las mayúsculas.
  - **Bloque de S3 y clave de objeto**: Cuando un objeto se ingiere a través de la interfaz S3, la aplicación cliente utiliza una combinación de bucket y clave de objeto para almacenar e identificar el objeto. Si el bloque de S3 tiene versiones y desea buscar una versión específica de un objeto S3 mediante el bloque y la clave de objeto, tendrá el **ID de versión**.
  - **Nombre de objeto y contenedor Swift**: Cuando un objeto se ingiere a través de la interfaz Swift, la aplicación cliente utiliza una combinación de nombre de objeto y contenedor para almacenar e identificar el objeto.

Pasos

1. Procese el objeto.
2. Seleccione **ILM** > **Búsqueda de metadatos de objetos**.
3. Escriba el identificador del objeto en el campo **Identificador**. Es posible introducir un UUID, CBID, bucket/object-key de S3 o nombre de objeto/contenedor de Swift.
4. De manera opcional, introduzca un ID de versión para el objeto (solo S3).

5. Seleccione **Buscar**.

   Se muestran los resultados de la búsqueda de metadatos de los objetos. Esta página incluye los siguientes tipos de información:

   - Metadatos del sistema, incluidos el ID de objeto (UUID), el nombre del objeto, el nombre del contenedor, el ID o el nombre de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y 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, una lista de segmentos de objetos que incluyen identificadores de segmentos y tamaños de datos. Para objetos con más de 100 segmentos, sólo se

muestran los primeros 100 segmentos.

- Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen los metadatos internos del sistema que no se garantiza que continúen del lanzamiento al lanzamiento.

  En el ejemplo siguiente se muestran los resultados de búsqueda de metadatos de objetos para un objeto de prueba S3 almacenado como dos copias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. Confirme que el objeto se almacena en la ubicación o las ubicaciones correctas y que es el tipo de copia correcto.

> Si la opción Auditoría está activada, también puede supervisar el registro de auditoría del mensaje ORLM Object Rules met. El mensaje de auditoría ORLM puede proporcionarle más información sobre el estado del proceso de evaluación de ILM, pero no puede proporcionar información sobre la corrección de la ubicación de los datos de objetos ni la integridad de la política de ILM. Debe evaluar esto usted mismo. Para obtener más información, consulte "Revisar los registros de auditoría".

Información relacionada

- "USE LA API DE REST DE S3"
- "Use la API DE REST de Swift"

Funciona con políticas de ILM y reglas de ILM

A medida que cambian sus requisitos de almacenamiento, es posible que deba aplicar otra normativa o modificar las reglas de ILM asociadas a la política. Puede ver las métricas de ILM para determinar el rendimiento del sistema.

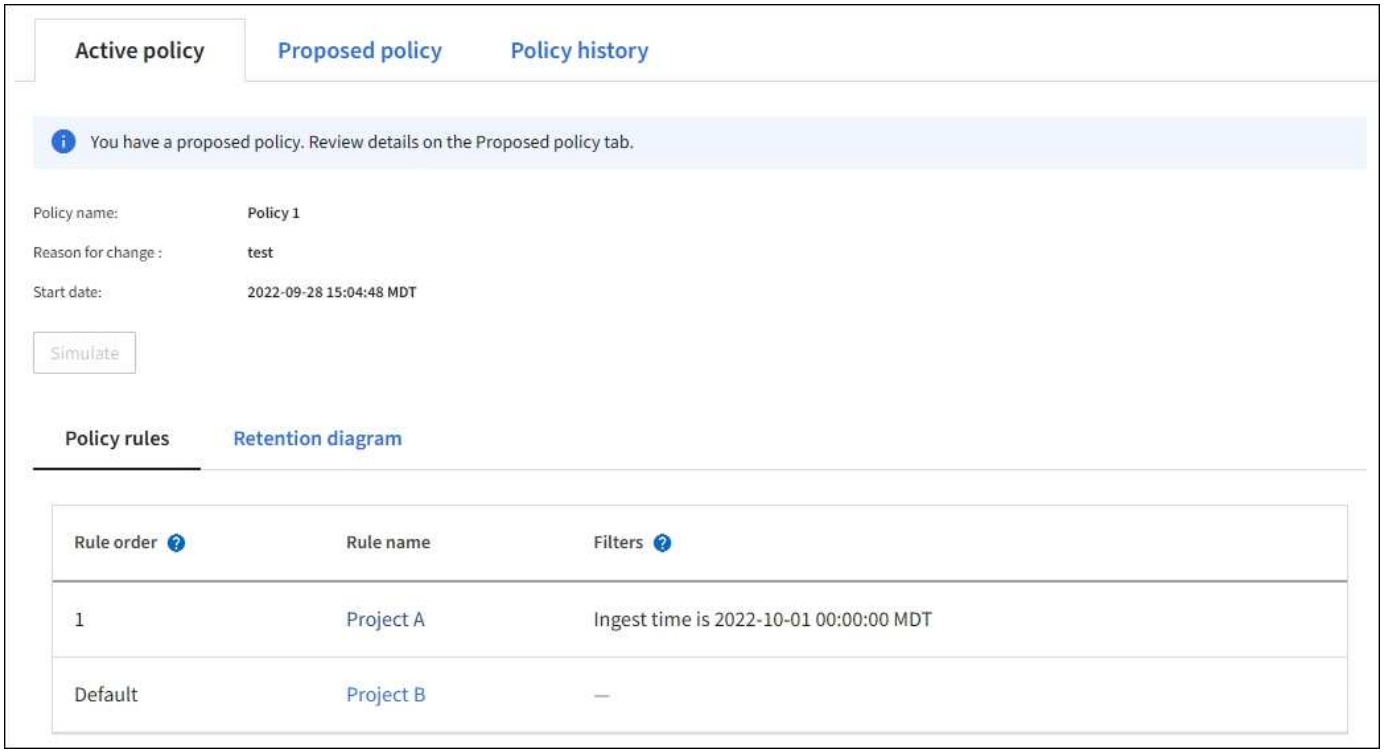
Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Vea las políticas de ILM

Para ver políticas de ILM activas, propuestas e históricas:

1. Seleccione **ILM** > **políticas**.
2. Según sea necesario, seleccione **Política activa**, **Política propuesta** o **Historial de políticas** para ver los detalles de cada una. En cada pestaña, puede seleccionar **Reglas de política** y **Diagrama de retención**.



Clonar una política histórica de ILM

Para clonar una política de ILM histórica:

1. Selecciona **ILM** > **Políticas** > **Historial de políticas**.
2. Elimine la política propuesta si existe.

3. Seleccione el botón de radio para la política que desea clonar y luego seleccione **Clonar política histórica**.
4. Complete los detalles requeridos siguiendo las instrucciones de "Cree la política de ILM propuesta".

> Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Elimine la política de ILM propuesta

Para eliminar la política propuesta:

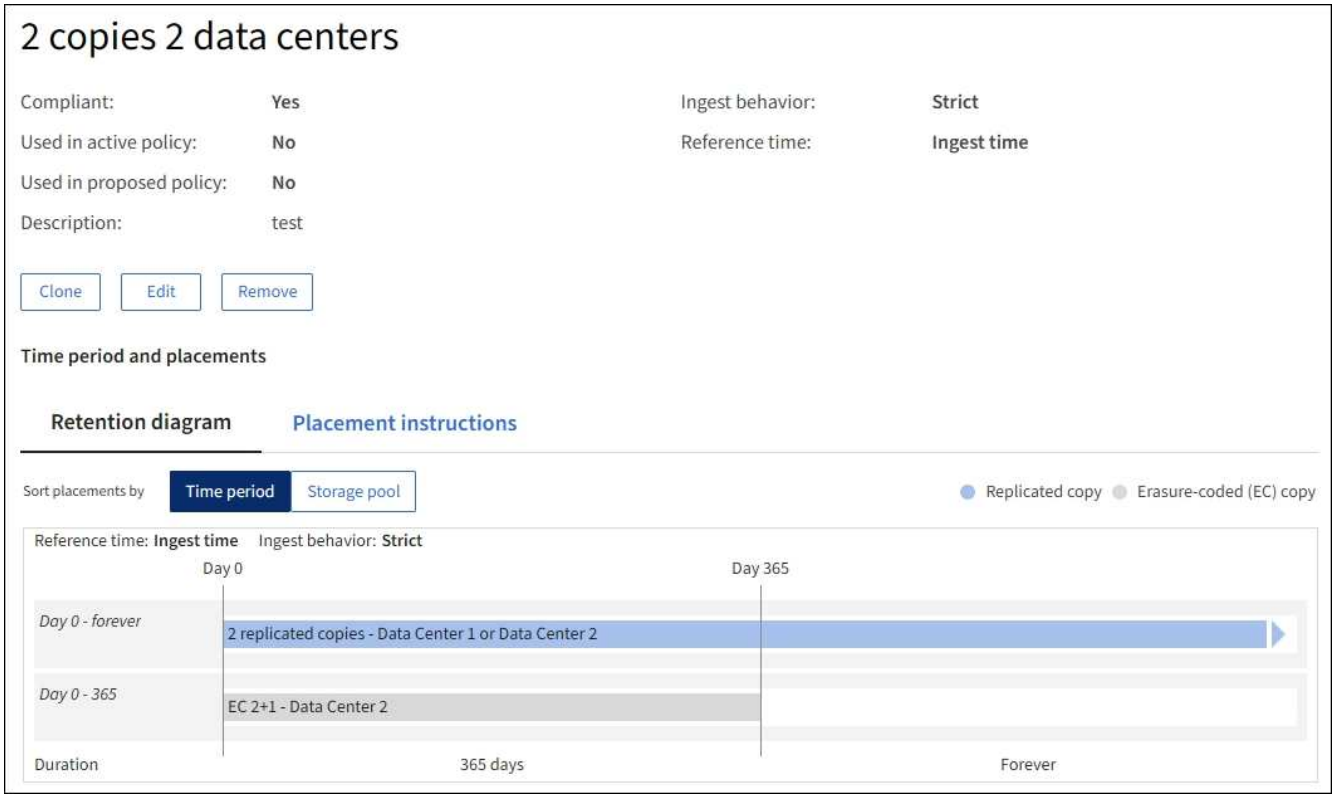
1. Seleccione **ILM** > **Políticas** > **Política propuesta**.
2. Seleccione **acciones** > **Quitar**.

Se eliminan la política propuesta y la pestaña de política propuesta.

Vea los detalles de las reglas de ILM

Para ver los detalles de una regla de ILM, incluido el diagrama de retención y las instrucciones de colocación de la regla:

1. Seleccione **ILM** > **Reglas**.
2. Seleccione la regla cuyos detalles desea ver. Ejemplo:



Además, puede utilizar la página de detalles para clonar, editar o eliminar una regla.

Clonar una regla de ILM

No puede editar una regla si se está utilizando en la política de ILM propuesta o la política de ILM activa. En su lugar, puede clonar una regla y hacer los cambios necesarios en la copia clonada. A continuación, si es necesario, puede eliminar la regla original de la directiva propuesta y sustituirla por la versión modificada. No puede clonar una regla de gestión de la vida útil de la información si se creó con StorageGRID versión 10,2 o anterior.

Antes de añadir una regla clonada a la política de ILM activa, tenga en cuenta que un cambio en las instrucciones de ubicación de un objeto puede provocar un aumento de la carga en el sistema.

Pasos

1. Seleccione **ILM** > **Reglas**.
2. Seleccione la casilla de verificación para la regla que desea clonar y luego seleccione **Clonar**. Como alternativa, seleccione el nombre de la regla y, a continuación, seleccione **Clonar** en la página de detalles de la regla.
3. Actualice la regla clonada siguiendo los pasos para Editar una regla de ILM y.. "Usar filtros avanzados en reglas de ILM".

   Al clonar una regla de ILM, debe introducir un nombre nuevo.

Editar una regla de ILM

Es posible que deba editar una regla de ILM para cambiar un filtro o una instrucción de ubicación.

No puede editar una regla si se está utilizando en la política de ILM activa o en la política de ILM propuesta. En su lugar, puede clonar estas reglas y hacer los cambios necesarios en la copia clonada. Tampoco puede editar la regla proporcionada por el sistema, hacer 2 copias.

> Antes de agregar una regla editada a la política de ILM activa, tenga en cuenta que un cambio en las instrucciones de ubicación de un objeto puede provocar un aumento de la carga en el sistema.

Pasos

1. Seleccione **ILM** > **Reglas**.
2. Confirme que la regla que desea editar no se utiliza en la política de ILM activa ni en la política de ILM propuesta.
3. Si la regla que desea editar no está en uso, seleccione la casilla de verificación de la regla y seleccione * Acciones * > * Editar **. Alternativamente, seleccione el nombre de la regla y luego seleccione *Editar** en la página de detalles de la regla.
4. Complete las páginas del asistente Edit ILM Rule. Según sea necesario, siga los pasos de "Creación de una regla de ILM" y.. "Usar filtros avanzados en reglas de ILM".

   Al editar una regla de ILM, no es posible cambiar su nombre.

> Si edita una regla que se utiliza en una política histórica, la aparece un icono para la regla cuando se visualiza la política, lo que indica que la regla se ha convertido en una regla histórica.

Quite una regla de ILM

Para que la lista de reglas de ILM actuales sea gestionable, elimine las reglas de ILM que probablemente no use.

Pasos

Para quitar una regla de ILM utilizada actualmente en la política activa o en la política propuesta:

1. Clone la política activa o edite la política propuesta.
2. Quite la regla de ILM de la política.
3. Guarde, simule y active la nueva directiva para asegurarse de que los objetos están protegidos como se espera.

Para eliminar una regla de ILM que no se está utilizando actualmente:

1. Seleccione **ILM** > **Reglas**.
2. Confirme que la regla que desea eliminar no se utiliza en la política activa ni en la política propuesta.
3. Si la regla que desea eliminar no está en uso, seleccione la regla y seleccione * Eliminar *. Puede seleccionar varias reglas y eliminarlas todas al mismo tiempo.
4. Seleccione **Sí** para confirmar que desea eliminar la regla de ILM.

   Se elimina la regla de ILM.

> Si elimina una regla que se utiliza en una política histórica, el aparece un icono para la regla cuando se visualiza la política, lo que indica que la regla se ha convertido en una regla histórica.

Ver las métricas de ILM

Se pueden ver métricas para ILM, como el número de objetos de la cola y la tasa de evaluación. Puede supervisar estas métricas para determinar el rendimiento del sistema. Una cola grande o una tasa de evaluación puede indicar que el sistema no es capaz de mantener el ritmo de la tasa de consumo, la carga de las aplicaciones cliente es excesiva o que existe alguna condición anormal.

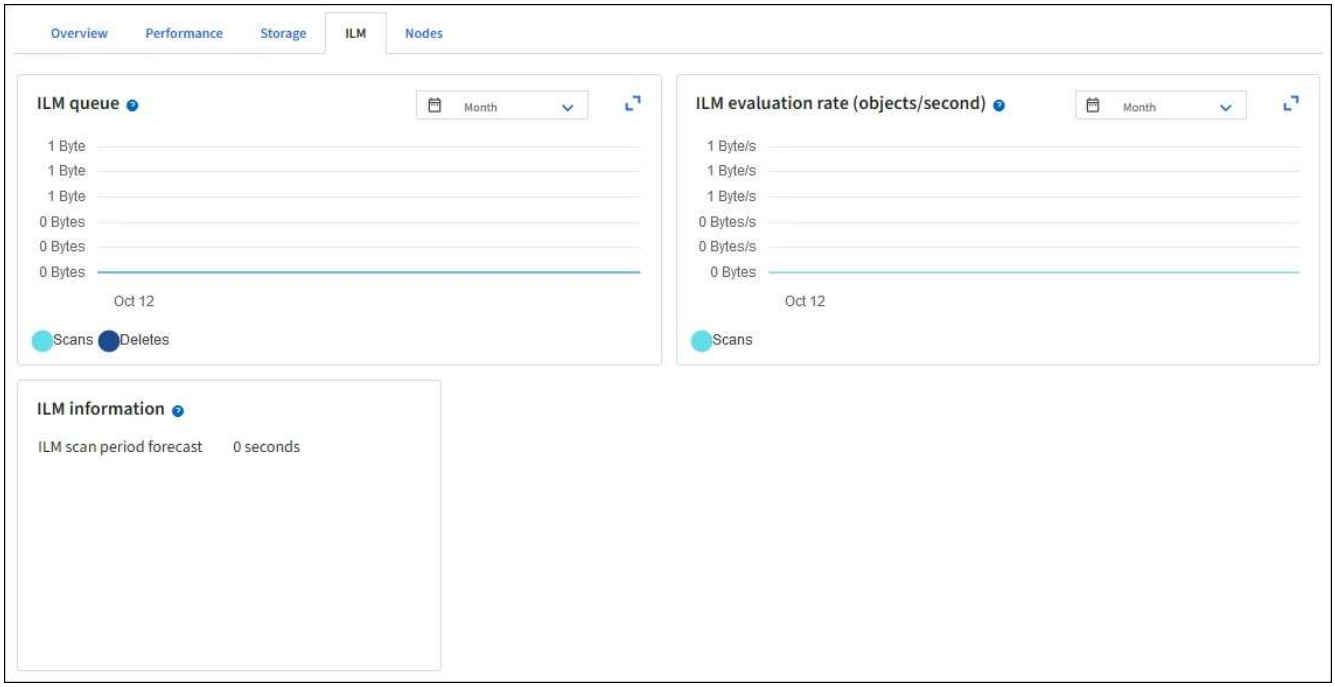
Pasos

1. Selecciona **Dashboard** > **ILM**.

> Como la consola se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervise las métricas en la pestaña ILM.

   Puede seleccionar el signo de interrogación Para ver una descripción de los elementos en la pestaña ILM.



Utilice el bloqueo de objetos de S3

Gestione objetos con S3 Object Lock

Como administrador de grid, puede habilitar el bloqueo de objetos de S3 GB en su sistema StorageGRID e implementar una política de gestión del ciclo de vida de la información conforme a la normativa para garantizar que los objetos de bloques de S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo determinado.

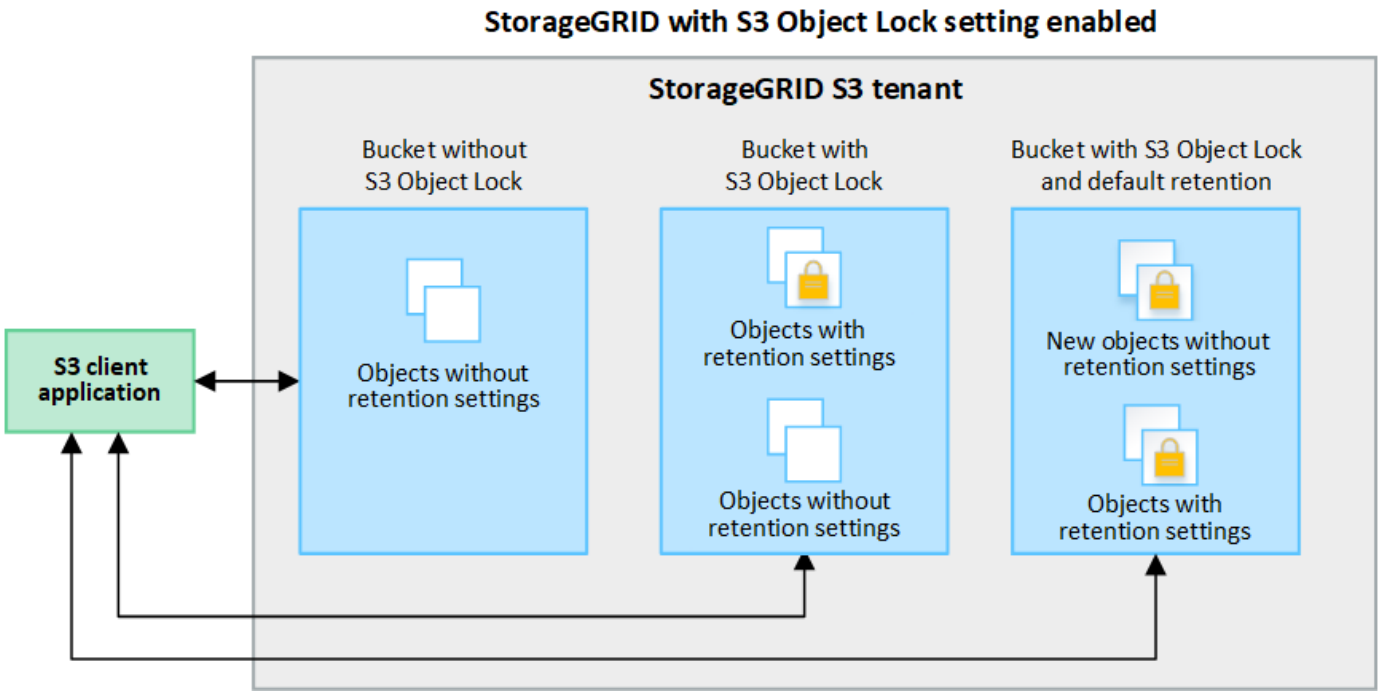
¿Qué es el bloqueo de objetos de S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos equivalente a S3 Object Lock en Amazon simple Storage Service (Amazon S3).

Tal y como se muestra en la figura, cuando se habilita la opción global de bloqueo de objetos de S3 para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear bloques con o sin la función de bloqueo de objetos de S3 habilitada. Si un bucket tiene S3 Object Lock habilitado, se requiere el control de versiones de bucket y se habilita automáticamente.

Si un bucket tiene S3 Object Lock habilitado, las aplicaciones cliente S3 pueden especificar, de manera opcional, la configuración de retención para cualquier versión de objeto guardada en ese bucket.

Además, un bloque que tiene S3 Object Lock habilitado puede tener opcionalmente un modo de retención y un período de retención predeterminados. La configuración predeterminada se aplica solo a los objetos que se agregan al depósito sin su propia configuración de retención.



Modos de retención

La función de bloqueo de objetos StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
  - El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.
  - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
  - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
- En modo de gobierno:
  - Los usuarios con permiso especial pueden utilizar un encabezado de omisión en las solicitudes para modificar ciertos valores de retención.
  - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden utilizar la aplicación cliente S3 para especificar opcionalmente los siguientes valores de retención para cada objeto que se agregue al depósito:

- **Modo de retención**: Ya sea cumplimiento o gobierno.
- **Retain-until-date**: Si la fecha de retención de una versión de objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente. La retención legal es independiente de la retención hasta la fecha.

Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener más información sobre la configuración del objeto, consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".

Valor de retención predeterminado para los depósitos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden especificar opcionalmente los siguientes ajustes predeterminados para el bloque:

- **Modo de retención predeterminado**: Ya sea cumplimiento o gobierno.
- **Período de retención predeterminado**: Cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este depósito, a partir del día en que se agregan.

La configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención. Los objetos de cubo existentes no se ven afectados al agregar o cambiar estos valores predeterminados.

Consulte "Cree un bloque de S3" y.. "Actualizar S3 Retención predeterminada de bloqueo de objetos".

Comparación del bloqueo de objetos de S3 con el cumplimiento de normativas heredado

El bloqueo de objetos de S3 sustituye la función de cumplimiento de normativas que estaba disponible en versiones anteriores de StorageGRID. Debido a que la función de bloqueo de objetos S3 cumple los requisitos de Amazon S3, deja obsoleto la función propia de cumplimiento de StorageGRID, que ahora se conoce como "'Legacy Compliance".

La configuración de cumplimiento global está anticuada. Si ha habilitado esta configuración con una versión anterior de StorageGRID, la configuración Bloqueo de objetos S3 se activa automáticamente. Puede seguir usando StorageGRID para gestionar la configuración de los buckets compatibles existentes; sin embargo, no puede crear nuevos buckets compatibles. Para obtener más información, consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

Si ha utilizado la función de cumplimiento de normativas heredada en una versión anterior de StorageGRID, consulte la siguiente tabla para saber cómo se compara con la función de bloqueo de objetos S3 de StorageGRID.

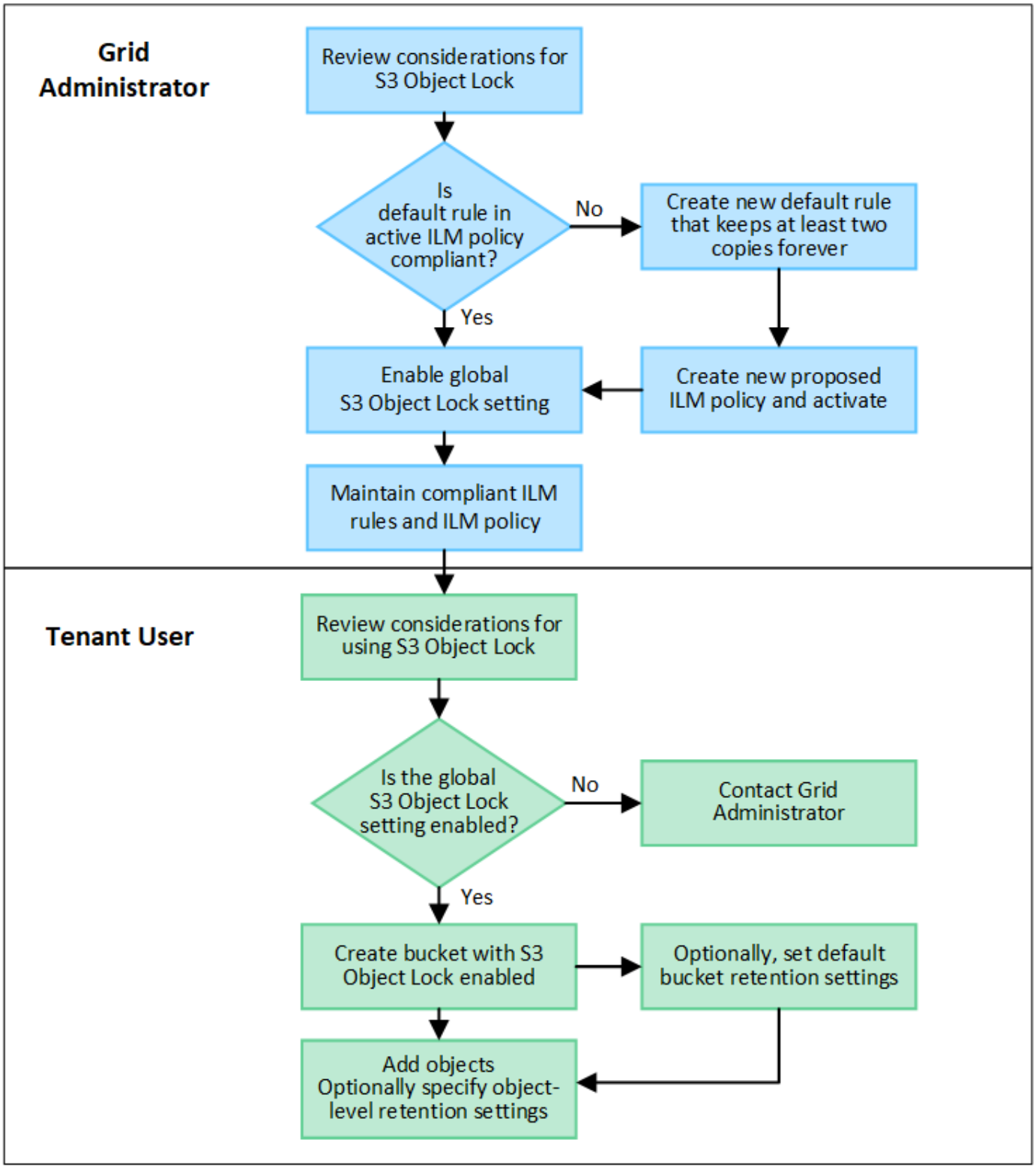
	Bloqueo de objetos de S3	Cumplimiento (heredado)
¿Cómo se habilita la función a nivel global?	En Grid Manager, seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.	Ya no es compatible.
¿Cómo se habilita la función para un bloque?	Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo bloque con el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST de S3.	Ya no es compatible.

	Bloqueo de objetos de S3	Cumplimiento (heredado)
¿Se admite el control de versiones de bloques?	Sí. El versionado de bloques se requiere y se habilita automáticamente si se habilita S3 Object Lock para el bloque.	No
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención hasta la fecha para cada versión de objeto, o pueden establecer un período de retención predeterminado para cada bloque.	Los usuarios deben establecer un período de retención para todo el segmento. El período de retención se aplica a todos los objetos del bloque.
¿Se puede cambiar el período de retención?	• En el modo de cumplimiento de normativas, se puede aumentar la fecha de retención de una versión de objeto, pero nunca disminuir. • En el modo de gobierno, los usuarios con permisos especiales pueden disminuir o incluso eliminar la configuración de retención de un objeto.	El período de retención de un depósito se puede aumentar, pero nunca disminuir.
¿Dónde se controla la conservación legal?	Los usuarios pueden poner una retención legal o levantar una retención legal para cualquier versión de objeto en el cubo.	Se coloca una retención legal en el cubo y afecta a todos los objetos del cucharón.
¿Cuándo se pueden eliminar los objetos?	• En el modo de cumplimiento, se puede suprimir una versión de objeto después de alcanzar la fecha de retención hasta la fecha, asumiendo que el objeto no está bajo conservación legal. • En el modo de gobierno, los usuarios con permisos especiales pueden eliminar un objeto antes de alcanzar su fecha de retención, asumiendo que el objeto no está bajo retención legal.	Un objeto se puede eliminar después de que caduque el período de retención, suponiendo que el segmento no esté en retención legal. Los objetos se pueden eliminar de forma automática o manual.
¿Se admite la configuración del ciclo de vida de bloques?	Sí	No

Flujo de trabajo para bloqueo de objetos de S3

Como administrador de grid, debe coordinar estrechamente con los usuarios inquilinos a fin de asegurarse de que los objetos estén protegidos de forma que cumplan sus requisitos de retención.

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar el bloqueo de objetos de S3. Estos pasos los realiza el administrador de grid y los usuarios inquilinos.



Tareas del administrador de grid

Tal y como se muestra en el diagrama de flujo de trabajo, un administrador de grid debe ejecutar dos tareas de alto nivel para que los usuarios de inquilinos S3 puedan usar el bloqueo de objetos S3:

1. Cree al menos una regla de ILM que cumpla las normativas y convierta esa regla en la regla predeterminada en la política de ILM activa.
2. Habilite el valor global de Object Lock para todo el sistema StorageGRID.

Tareas del usuario inquilino

Una vez habilitada la configuración global de bloqueo de objetos S3, los inquilinos pueden realizar estas tareas:

1. Cree bloques con el bloqueo de objetos de S3 habilitado.
2. Opcionalmente, especifique la configuración de retención predeterminada para el bloque. Cualquier configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención.
3. Agregue objetos a esos bloques y, opcionalmente, especifique los períodos de retención a nivel de objeto y la configuración de retención legal.
4. Según sea necesario, actualice la retención predeterminada del depósito o actualice el período de retención o la configuración de retención legal para un objeto individual.

Requisitos para el bloqueo de objetos de S3

Debe revisar los requisitos para habilitar la configuración global de bloqueo de objetos de S3, los requisitos para crear reglas de ILM y políticas de ILM conformes con la normativa, y las restricciones que StorageGRID coloca en bloques y objetos que usan el bloqueo de objetos S3.

Requisitos para usar el valor global de bloqueo de objetos S3

- Debe habilitar la configuración global de Object Lock mediante el administrador de grid o la API de gestión de grid antes de que cualquier inquilino de S3 pueda crear un bucket con el bloqueo de objetos S3 habilitado.
- Al habilitar el ajuste global de Object Lock, todas las cuentas de inquilinos S3 pueden crear bloques con el bloqueo de objetos S3 habilitado.
- Después de habilitar la configuración global S3 Object Lock, no puede desactivar la configuración.
- No puede activar el bloqueo de objetos S3 global a menos que la regla predeterminada de la política de ILM activa sea *compliant* (es decir, la regla predeterminada debe cumplir con los requisitos de los depósitos con bloqueo de objetos S3 activado).
- Cuando se habilita la configuración de bloqueo de objetos S3 global, no se puede crear una nueva política de ILM propuesta ni activar una política de ILM propuesta existente a menos que la regla predeterminada de la política sea compatible. Una vez habilitada la configuración global S3 Object Lock, las reglas de ILM y las páginas de políticas de ILM indican qué reglas de ILM cumplen.

Requisitos para las reglas de ILM que cumplen con las normativas

Si desea habilitar la configuración global de bloqueo de objetos S3, debe asegurarse de que la regla predeterminada de la política de ILM activa sea compatible. Una regla conforme a las normativas satisface los requisitos de ambos bloques con el bloqueo de objetos S3 habilitado y de cualquier bloque existente con el

cumplimiento de normativas heredado habilitado:

- Debe crear al menos dos copias de objetos replicados o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante todo el tiempo que dure cada línea en las instrucciones de colocación.
- Las copias de objetos no se pueden guardar en un pool de almacenamiento en la nube.
- Las copias de objetos no se pueden guardar en los nodos de archivado.
- Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando **tiempo de ingesta** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación deberá ser «'para siempre».

Requisitos para políticas de ILM activas y propuestas

Cuando se habilita la configuración global de bloqueo de objetos S3, las políticas de ILM activas y propuestas pueden incluir reglas tanto conformes a la normativa como no.

- La regla predeterminada de la política de ILM activa o propuesta debe ser conforme.
- Las reglas no compatibles solo se aplican a objetos de los depósitos que no tienen activado el bloqueo de objetos S3 o que no tienen activada la función de cumplimiento de normativas heredada.
- Las reglas que cumplen las normativas se pueden aplicar a los objetos de cualquier bloque; no es necesario habilitar el bloqueo de objetos S3 o la conformidad heredada para el bloque.

Una política de ILM compatible puede incluir estas tres reglas:

1. Se trata de una regla que crea copias de los objetos con código de borrado en un bloque específico con el bloqueo de objetos S3 habilitado. Las copias EC se almacenan en nodos de almacenamiento del día 0 al permanente.
2. Una regla no compatible que crea dos copias de objetos replicadas en los nodos de almacenamiento durante un año y, a continuación, mueve una copia de objetos a los nodos de archivado y almacena esa copia para siempre. Esta regla solo se aplica a los depósitos que no tienen activado el bloqueo de objetos S3 o el cumplimiento de normativas heredado porque almacena una sola copia de objeto para siempre y utiliza nodos de archivado.
3. Una regla predeterminada que cumple con las normativas crea dos copias de objetos replicados en los nodos de almacenamiento del día 0 al permanente. Esta regla se aplica a cualquier objeto de cualquier segmento que no haya sido filtrado por las dos primeras reglas.

Requisitos para bloques con bloqueo de objetos de S3 habilitado

- Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede usar el administrador de inquilinos, la API de gestión de inquilinos o la API REST de S3 para crear bloques con el bloqueo de objetos S3 habilitado.
- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No puede activar el bloqueo de objetos S3 para un depósito existente.
- Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque. No puede desactivar el bloqueo de objetos de S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención y un período de retención predeterminados para cada bloque mediante el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST S3. La configuración de retención predeterminada del depósito se aplica solo a los nuevos objetos

agregados al depósito que no tienen su propia configuración de retención. Puede anular esta configuración predeterminada especificando un modo de retención y Retain-until-date para cada versión del objeto cuando se cargue.

- Se admite la configuración de ciclo de vida de bloques para los bloques con S3 Object Lock habilitado.
- La replicación de CloudMirror no es compatible para bloques con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en bloques con S3 Object Lock habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el bloque, o bien puede especificar la configuración de retención para cada versión de objeto. La configuración de retención a nivel de objeto se puede especificar mediante la aplicación cliente S3 o la API DE REST S3.
- La configuración de retención se aplica a versiones individuales de objetos. Una versión de objeto puede tener una configuración de retención hasta fecha y una retención legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta fecha o de retención legal para un objeto, sólo se protege la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en bloques con S3 Object Lock habilitado

Cada objeto que se guarda en un depósito con S3 Object Lock habilitado pasa por las siguientes etapas:

1. **Procesamiento de objetos**

   Cuando se agrega una versión de objeto al depósito que tiene S3 Object Lock habilitado, la configuración de retención se aplica de la siguiente manera:

   - Si se especifica la configuración de retención para el objeto, se aplica la configuración de nivel de objeto. Se ignoran todos los valores predeterminados de los depósitos.
   - Si no se especifica ninguna configuración de retención para el objeto, se aplica la configuración de bloque predeterminada, si existe.
   - Si no se especifica ninguna configuración de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

   Si se aplica una configuración de retención, tanto el objeto como cualquier metadatos definidos por el usuario S3 se protegen.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. El número y el tipo exactos de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas conformes a la normativa de la política de ILM activa. Si se puede eliminar un objeto protegido antes de alcanzar su fecha de retención hasta la fecha, depende de su modo de retención.

   - Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Información relacionada

- "Cree un bloque de S3"
- "Actualizar S3 Retención predeterminada de bloqueo de objetos"
- "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

- "Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3"

Habilite el bloqueo de objetos de S3 globalmente

Si una cuenta de inquilino de S3 tiene que cumplir con los requisitos de normativa al guardar datos de objetos, debe habilitar el bloqueo de objetos de S3 para todo el sistema StorageGRID. Al habilitar el ajuste global de bloqueo de objetos de S3, cualquier usuario inquilino de S3 puede crear y gestionar bloques y objetos con S3 Object Lock.

Antes de empezar

- Tiene el permiso acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ha revisado el flujo de trabajo de bloqueo de objetos de S3 y comprende las consideraciones.
- Ha confirmado que la regla predeterminada de la política de ILM activa cumple con las normativas. Consulte "Cree una regla de ILM predeterminada" para obtener más detalles.

Acerca de esta tarea

Un administrador de grid debe habilitar la configuración global de bloqueo de objetos S3 para permitir a los usuarios inquilinos crear nuevos bloques con el bloqueo de objetos S3 habilitado. Una vez habilitada esta configuración, no se puede desactivar.

> La configuración de cumplimiento global está anticuada. Si ha habilitado esta configuración con una versión anterior de StorageGRID, la configuración Bloqueo de objetos S3 se activa automáticamente. Puede seguir usando StorageGRID para gestionar la configuración de los buckets compatibles existentes; sin embargo, no puede crear nuevos buckets compatibles. Para obtener más información, consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.

   Se muestra la página S3 Object Lock Settings.

2. Seleccione **Activar el bloqueo de objetos S3**.
3. Seleccione **aplicar**.

   Aparece un cuadro de diálogo de confirmación que le recuerda que no puede desactivar el bloqueo de objetos S3 después de que esté habilitado.

4. Si está seguro de que desea activar de forma permanente el bloqueo de objetos S3 para todo el sistema, seleccione **Aceptar**.

   Al seleccionar **Aceptar**:

   - Si la regla predeterminada de la política de ILM activa es compatible, S3 Object Lock ahora está habilitado para toda la cuadrícula y no se puede deshabilitar.
   - Si la regla predeterminada no es compatible, aparece un error. Debe crear y activar una nueva política de ILM que incluya una regla de cumplimiento como regla predeterminada. Seleccione **OK**. A continuación, cree una nueva política propuesta, simule y actívela. Consulte "Cree una política de ILM" si desea obtener instrucciones.

Después de terminar

Después de habilitar la configuración global S3 Object Lock, es posible que desee hacerlo "Cree una nueva política de ILM". Una vez activada la configuración, la política de ILM puede incluir de manera opcional una regla predeterminada que cumpla las normativas y una regla predeterminada que no sea compatible. Por ejemplo, es posible que desee utilizar una regla no compatible que no tenga filtros para objetos en depósitos que no tengan S3 Object Lock activado.

Resuelva los errores de coherencia al actualizar la configuración de bloqueo de objetos de S3 o cumplimiento heredado

Si un sitio de centro de datos o varios nodos de almacenamiento de un sitio no están disponibles, es posible que deba ayudar a los usuarios inquilinos S3 a aplicar los cambios en la configuración del bloqueo de objetos S3 o del cumplimiento heredado.

Los usuarios inquilinos que tienen bloques con S3 Object Lock (o Legacy Compliance) habilitado pueden cambiar ciertas opciones. Por ejemplo, es posible que un usuario arrendatario que utilice el bloqueo de objetos S3 deba poner una versión de objeto en retención legal.

Cuando un usuario tenant actualiza la configuración de un bloque de S3 o una versión de objeto, StorageGRID intenta actualizar inmediatamente los metadatos del objeto o el bloque en el grid. Si el sistema no puede actualizar los metadatos porque no hay disponibles un sitio de centro de datos o varios nodos de almacenamiento, devuelve un error:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Para resolver este error, siga estos pasos:

1. Se debe intentar que todos los nodos o sitios de almacenamiento estén disponibles de nuevo Lo antes posible..
2. Si no puede dejar suficientes nodos de almacenamiento en cada sitio disponible, póngase en contacto con el soporte técnico, que puede ayudarle a recuperar nodos y asegurarse de que los cambios se apliquen de manera coherente en la cuadrícula.
3. Una vez resuelto el problema subyacente, recuerde al usuario inquilino que vuelva a intentar cambiar sus cambios de configuración.

Información relacionada

- "Usar una cuenta de inquilino"
- "USE LA API DE REST DE S3"
- "Recuperación y mantenimiento"

Ejemplo de reglas y políticas de ILM

Ejemplo 1: Reglas de ILM y políticas para el almacenamiento de objetos

Es posible usar las siguientes reglas y políticas de ejemplo como punto de inicio al definir una política de ILM para cumplir con los requisitos de retención y protección de objetos.

Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

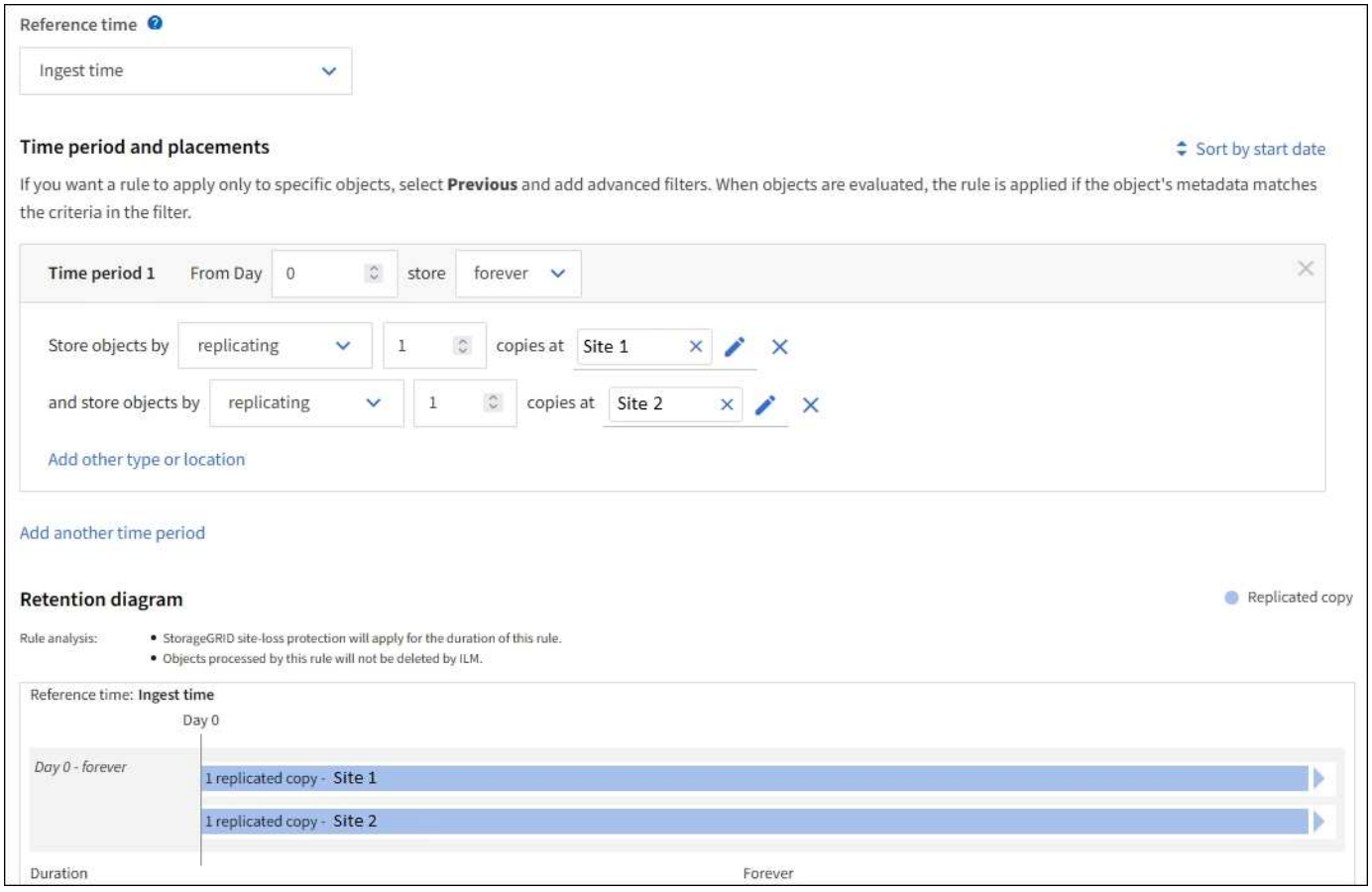
Regla ILM 1 Por ejemplo 1: Copiar datos de objetos en dos sitios

Este ejemplo de regla ILM copia datos de objetos en pools de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Pools de almacenamiento in situ	Dos pools de almacenamiento, cada uno de los cuales contiene sitios diferentes, denominados Sitio 1 y Sitio 2.
Nombre de regla	Dos copias Dos sitios
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	En el día 0 hasta siempre, conserve una copia replicada en el sitio 1 y una copia replicada en el sitio 2.

La sección de análisis de reglas del diagrama de retención indica lo siguiente:

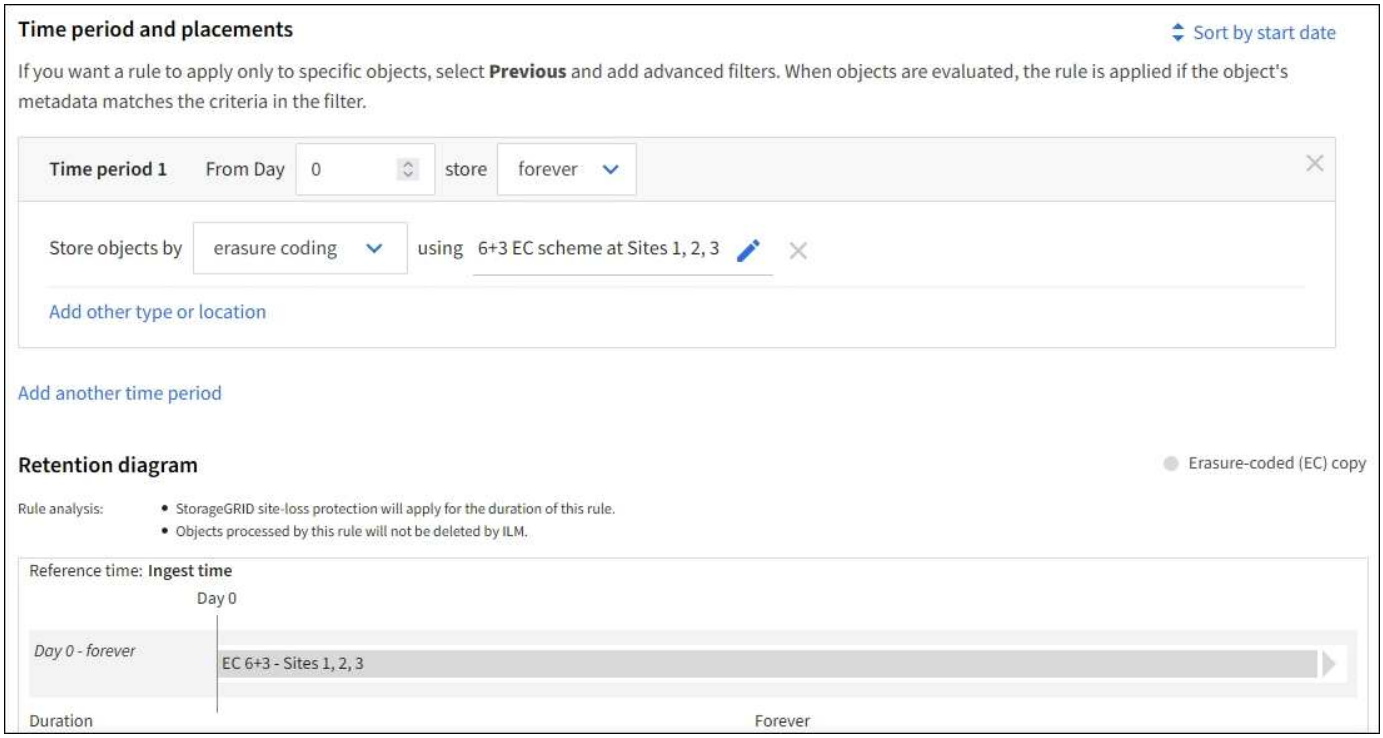
- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- ILM no eliminará los objetos procesados por esta regla.



Regla de ILM 2 Por ejemplo 1: Perfil de código de borrado con coincidencia de bloques

En esta regla de ILM de ejemplo se utiliza un perfil de código de borrado y un bloque de S3 para determinar dónde y durante cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Pool de almacenamiento con múltiples sitios	• Un pool de almacenamiento en tres sitios (sitios 1, 2, 3) • Utilice un esquema de codificación de borrado de 6+3
Nombre de regla	S3 registros financieros del bloque
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	Para los objetos del bloque de S3 denominados registros financieros, cree una copia con código de borrado en el pool especificado por el perfil de código de borrado. Guarde esta copia para siempre.



Política de ILM, por ejemplo 1

En la práctica, la mayoría de las políticas de ILM son sencillas, a pesar de que el sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas.

Una política de ILM típica para un grid de varios sitios podría incluir reglas de ILM como las siguientes:

- Durante la ingesta, almacene todos los objetos que pertenecen al bloque de S3 denominado `finance-records` en un pool de almacenamiento que contiene tres sitios. Use el código de borrado 6+3.
- Si un objeto no coincide con la primera regla de ILM, utilice la regla de ILM predeterminada de la política, dos copias dos centros de datos, para almacenar una copia de ese objeto en el sitio 1 y una copia en el

sitio 2.

Información relacionada

- "Cree una política de ILM: Información general"
- "Cree una política de ILM propuesta"

Ejemplo 2: Reglas de ILM y política para el filtrado de tamaño de objetos de EC

Puede usar las siguientes reglas y políticas de ejemplo como puntos de inicio para definir una política de ILM que filtra por tamaño de objeto para cumplir los requisitos de EC recomendados.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Regla de ILM 1 por ejemplo 2: Utilice EC para objetos de más de 1 MB

Este ejemplo codifica los objetos de borrado de regla ILM que tienen más de 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Definición de regla	Valor de ejemplo
Nombre de regla	Objetos sólo EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para Tamaño de objeto	Tamaño de objeto superior a 1 MB
Ubicaciones	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones

Regla de ILM 2 por ejemplo 2: Dos copias replicadas

Esta regla de ILM de ejemplo crea dos copias replicadas y no filtra por el tamaño del objeto. Esta regla es la regla predeterminada para la directiva. Dado que la primera regla filtra todos los objetos mayores de 1 MB, esta regla sólo se aplica a objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de regla	Dos copias replicadas
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para Tamaño de objeto	Ninguno
Ubicaciones	En el día 0 hasta siempre, conserve una copia replicada en el sitio 1 y una copia replicada en el sitio 2.

Política de ILM, por ejemplo 2: Usar EC para objetos de más de 1 MB

Este ejemplo de política de ILM incluye dos reglas ILM:

- La primera regla de borrado codifica todos los objetos que sean mayores de 1 MB.
- La segunda regla de ILM (predeterminada) crea dos copias replicadas. Dado que los objetos mayores de 1 MB se han filtrado mediante la regla 1, la regla 2 sólo se aplica a objetos de 1 MB o menos.

Ejemplo 3: Reglas de ILM y política para mejorar la protección de los archivos de imagen

Puede utilizar las siguientes reglas y políticas de ejemplo a fin de garantizar que las imágenes mayores de 1 MB estén codificadas para el borrado y que haya dos copias de imágenes más pequeñas.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

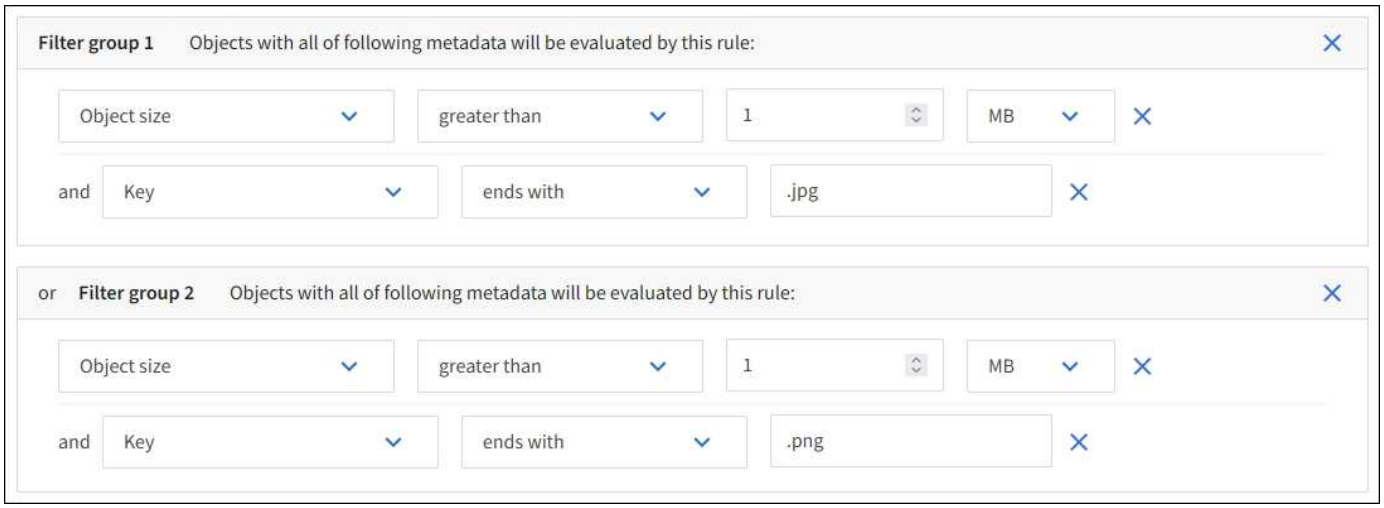
Regla ILM 1 por ejemplo 3: Utilice EC para archivos de imagen superiores a 1 MB

En esta regla de ILM de ejemplo se utiliza un filtrado avanzado para borrar el código de todos los archivos de imagen superiores a 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Definición de regla	Valor de ejemplo
Nombre de regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para Tamaño de objeto	Tamaño de objeto superior a 1 MB

Definición de regla	Valor de ejemplo
Filtros avanzados para Clave	• Termina en .jpg • Termina en .png
Ubicaciones	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones



Debido a que esta regla se configura como la primera regla de la directiva, la instrucción de colocación de codificación de borrado solo se aplica a los archivos .jpg y .png que sean mayores de 1 MB.

Regla ILM 2 por ejemplo 3: Cree 2 copias replicadas para todos los archivos de imagen restantes

En este ejemplo, la regla ILM utiliza un filtrado avanzado para especificar que se repliquen los archivos de imagen más pequeños. Dado que la primera regla de la directiva ya coincide con los archivos de imagen superiores a 1 MB, esta regla se aplica a los archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de regla	2 copias para archivos de imagen
Tiempo de referencia	Tiempo de ingesta
Filtros avanzados para Clave	• Termina en .jpg • Termina en .png
Ubicaciones	Cree 2 copias replicadas en dos pools de almacenamiento

Política de ILM, por ejemplo 3: Mejor protección para los archivos de imagen

Este ejemplo de política de ILM incluye tres reglas:

- La primera regla de borrado codifica todos los archivos de imagen mayores de 1 MB.
- La segunda regla crea dos copias de cualquier archivo de imagen restante (es decir, imágenes de 1 MB o menos).

- La regla predeterminada se aplica a todos los objetos restantes (es decir, cualquier archivo que no sea de imagen).

Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3

Si tiene un bucket de S3 con el control de versiones habilitado, puede administrar las versiones de objetos no corrientes incluyendo reglas en su política de ILM que utilicen «`hora no corriente » como tiempo de referencia.

> Si especifica un tiempo de retención limitado para los objetos, esos objetos se suprimirán permanentemente después de alcanzar el período de tiempo. Asegúrese de comprender cuánto tiempo se retendrán los objetos.

Como se muestra en este ejemplo, puede controlar la cantidad de almacenamiento que utilizan los objetos con versiones utilizando instrucciones de colocación diferentes para las versiones de objetos no actuales.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

> Para realizar la simulación de política de ILM en una versión no actual de un objeto, debe conocer el UUID o CBID de la versión del objeto. Para encontrar el UUID y CBID, utilice "búsqueda de metadatos de objetos" mientras el objeto sigue siendo actual.

Información relacionada

- "Cómo se eliminan los objetos"

Regla 1 de ILM, por ejemplo 4: Guarde tres copias durante 10 años

Esta regla de ILM de ejemplo almacena una copia de cada objeto en tres sitios durante 10 años.

Esta regla se aplica a todos los objetos, con o sin versiones.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Tres pools de almacenamiento, cada uno compuesto por diferentes centros de datos, denominados Sitio 1, Sitio 2 y Sitio 3.
Nombre de regla	Tres copias diez años
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	El día 0, conserve tres copias replicadas durante 10 años (3.652 días), una en el sitio 1, una en el sitio 2 y otra en el sitio 3. Al final de 10 años, elimine todas las copias del objeto.

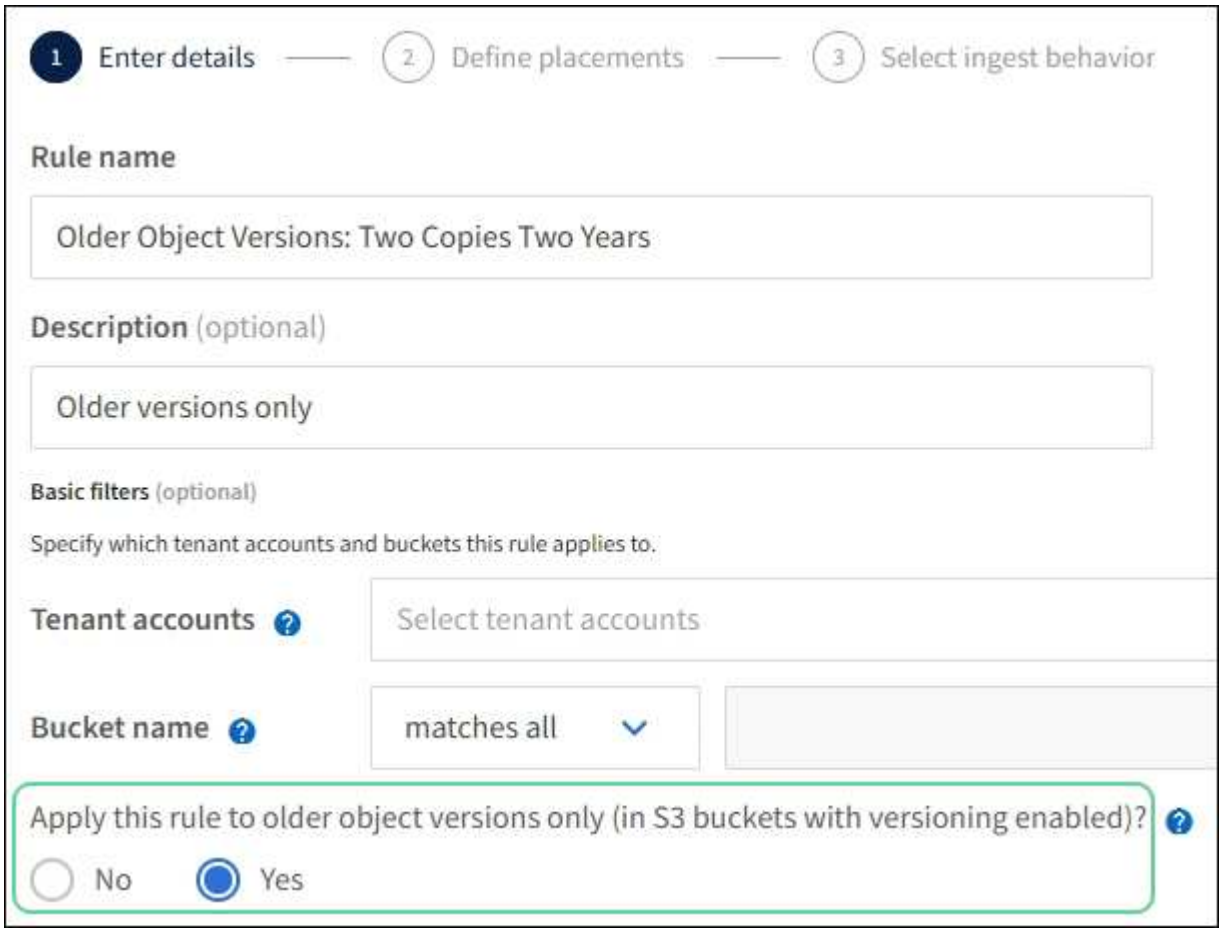
Regla de ILM 2 por ejemplo 4: Guarde dos copias de las versiones no corrientes durante 2 años

Esta regla de ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto con versiones

de S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debe crear otra regla para filtrar las versiones no actuales.

Para crear una regla que utilice "tiempo no corriente" como tiempo de referencia, seleccione **Sí** para la pregunta, "`Aplicar esta regla solo a versiones de objetos anteriores (en cubos S3 con control de versiones activado)?` En el paso 1 (introduzca detalles) del asistente Create an ILM Rule. Cuando selecciona **Sí**, *Tiempo no corriente* se selecciona automáticamente para el tiempo de referencia y no puede seleccionar un tiempo de referencia diferente.



En este ejemplo, sólo se almacenan dos copias de las versiones no corrientes, y esas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos pools de almacenamiento, cada uno en diferentes centros de datos, Sitio 1 y Sitio 2.
Nombre de regla	Versiones no corrientes: Dos copias dos años

Definición de regla	Valor de ejemplo
Tiempo de referencia	Hora no corriente Seleccionado automáticamente cuando selecciona **Sí** para la pregunta, “`Aplicar esta regla solo a versiones de objetos anteriores (en cubos S3 con control de versiones activado)?” En el asistente Create an ILM Rule.
Ubicaciones	El día 0 relativo a la hora no corriente (es decir, a partir del día en que la versión del objeto se convierte en la versión no actual), mantenga dos copias replicadas de las versiones del objeto no corriente durante 2 años (730 días), una en el sitio 1 y otra en el sitio 2. Al final de 2 años, elimine las versiones no actuales.

Política de ILM, por ejemplo 4: Objetos con versiones de S3

Si desea administrar versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilizan '`tiempo no corriente " como tiempo de referencia deben aparecer en la política de ILM antes de las reglas que se aplican a la versión del objeto actual.

Una política de ILM para objetos con versiones de S3 puede incluir reglas de ILM como las siguientes:

- Mantenga las versiones antiguas (no actuales) de cada objeto durante 2 años, a partir del día en que la versión se volvió no actual.

> Las reglas de “tiempo no corriente” deben aparecer en la política antes de las reglas que se aplican a la versión de objeto actual. De lo contrario, las versiones del objeto no corriente nunca se coincidirán con la regla "hora no corriente".

- Al ingerir, cree tres copias replicadas y almacene una copia en cada uno de tres sitios. Guarde copias de la versión actual del objeto durante 10 años.

Al simular la directiva de ejemplo, se esperaría que los objetos de prueba se evaluaran de la siguiente manera:

- Cualquier versión de objeto no actual se haría coincidir con la primera regla. Si una versión de objeto no actual tiene más de 2 años, ILM lo elimina de forma permanente (todas las copias de la versión no actual se eliminan de la cuadrícula).

> Para simular versiones de objeto no actuales, debe utilizar el UUID o CBID de esa versión. Mientras el objeto sigue siendo actual, puede utilizar "búsqueda de metadatos de objetos" Para encontrar su UUID y CBID.

- La versión actual del objeto coincidiría con la segunda regla. Cuando la versión del objeto actual se ha almacenado durante 10 años, el proceso de ILM agrega un marcador de eliminación como la versión actual del objeto y convierte la versión del objeto anterior en “no corriente”. La próxima vez que se produzca una evaluación de ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en el sitio 3 se purga y las dos copias en el sitio 1 y el sitio 2 se almacenan durante 2 años más.

Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto

Puede usar un filtro de ubicación y el comportamiento de ingesta estricto de una regla

para evitar que los objetos se guarden en una ubicación de centro de datos en particular.

En este ejemplo, un inquilino con sede en París no quiere almacenar algunos objetos fuera de la UE debido a preocupaciones regulatorias. Otros objetos, incluidos todos los objetos de otras cuentas de inquilino, pueden almacenarse en el centro de datos de París o en el centro de datos de EE. UU.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Información relacionada

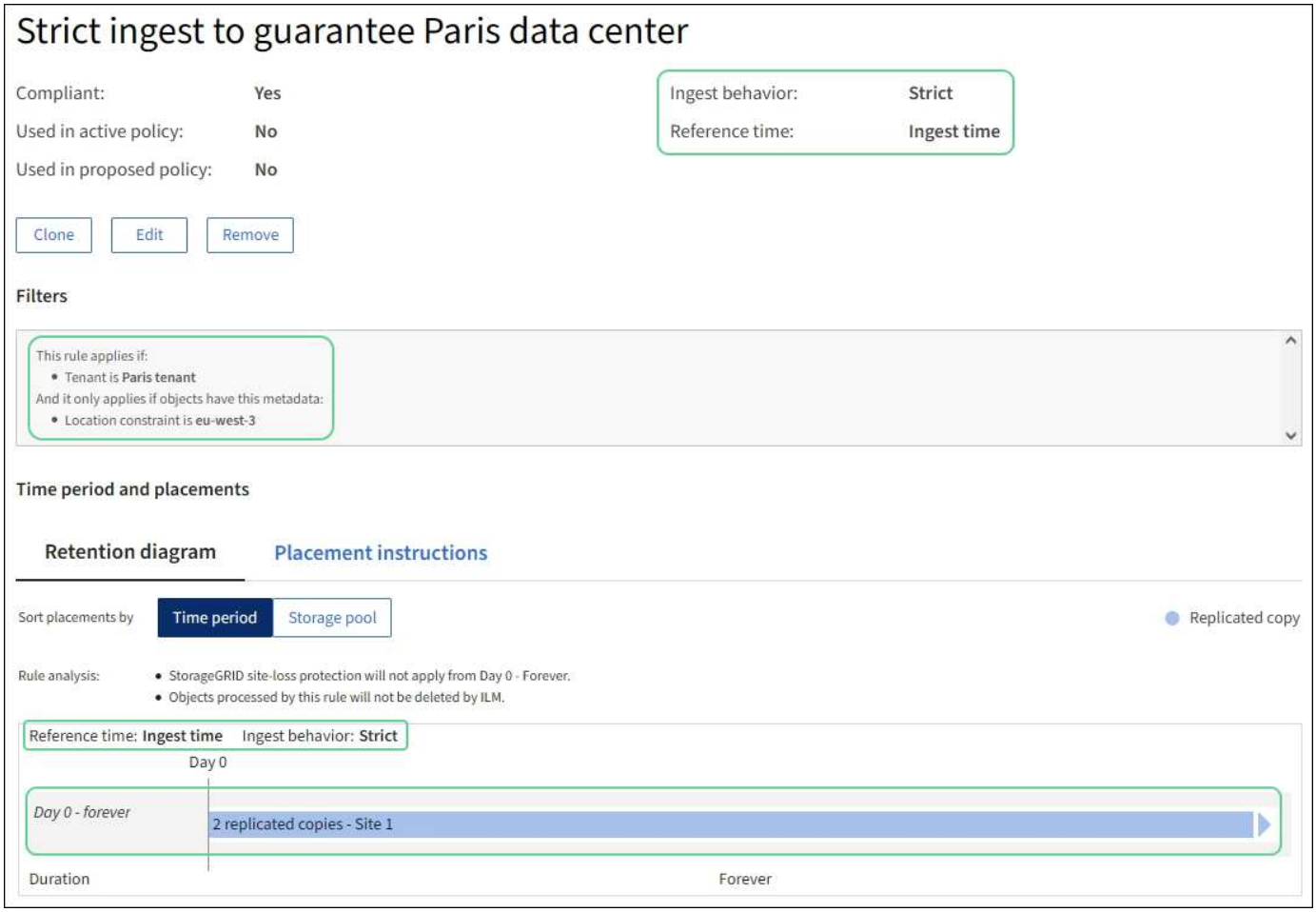
- "Opciones de procesamiento"
- "Create ILM rule: Seleccione el comportamiento de ingesta"

Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

Esta regla de ILM de ejemplo usa el comportamiento de ingesta estricto para garantizar que los objetos que ha ahorrado un inquilino basado en París en cubos S3 con la región establecida en la región eu-West-3 (París) nunca se almacenen en el centro de datos de EE. UU.

Esta regla se aplica a objetos que pertenecen al arrendatario de París y que tienen la región de cubo S3 establecida en eu-West-3 (París).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Inquilino de París
Filtro avanzado	La restricción de ubicación es igual a eu-west-3
Pools de almacenamiento	Sitio 1 (París)
Nombre de regla	Ingesta estricta para garantizar el centro de datos París
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	El día 0, mantenga dos copias replicadas para siempre en el sitio 1 (París)
Comportamiento de ingesta	Estricto. Utilice siempre las colocaciones de esta regla durante el procesamiento. La ingesta falla si no es posible almacenar dos copias del objeto en el centro de datos de París.



Regla 2 de ILM, por ejemplo 5: Ingesta equilibrada de otros objetos

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta equilibrada para proporcionar una eficiencia de ILM óptima para cualquier objeto que no sea coincidente con la primera regla. Se almacenarán dos copias de todos los objetos compatibles con esta regla: Una en el centro de datos estadounidense y una en el centro de datos de París. Si la regla no se puede cumplir inmediatamente, las copias provisionales se almacenan en cualquier ubicación disponible.

Esta regla se aplica a objetos que pertenecen a cualquier arrendatario y a cualquier región.

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtro avanzado	*No especificado*
Pools de almacenamiento	Sitio 1 (París) y Sitio 2 (EE.UU.)
Nombre de regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingesta

Definición de regla	Valor de ejemplo
Ubicaciones	Desde el día 0, mantenga dos copias replicadas para siempre en dos centros de datos
Comportamiento de ingesta	Equilibrado. Los objetos que coinciden con esta regla se colocan de acuerdo con las instrucciones de colocación de la regla, si es posible. De lo contrario, las copias provisionales se realizan en cualquier lugar disponible.

Política de ILM, por ejemplo 5: Combinar comportamientos de consumo

La política de ILM de ejemplo incluye dos reglas que tienen comportamientos de consumo diferentes.

Una política de ILM que usa dos comportamientos de consumo diferentes puede incluir reglas de ILM como las siguientes:

- Almacene objetos que pertenecen al inquilino de París y que tienen la región de cubo de S3 establecida en eu-West-3 (París) solo en el centro de datos de París. No se procese correctamente si el centro de datos de París no está disponible.
- Almacenar todos los demás objetos (incluidos los que pertenecen al inquilino de París, pero que tienen una región de bloques diferente) tanto en el centro de datos de EE. UU. Como en el de París. Realice copias provisionales en cualquier ubicación disponible si la instrucción de colocación no se puede satisfacer.

Al simular la directiva de ejemplo, espera que los objetos de prueba se evalúen de la siguiente forma:

- Cualquier objeto que pertenezca al inquilino de París y que tenga la región de bloque de S3 establecida en eu-West-3 se ajusta a la primera regla y se almacena en el centro de datos de París. Como la primera regla usa un procesamiento estricto, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los nodos de almacenamiento del centro de datos de París no están disponibles, la ingesta falla.
- Todos los demás objetos coinciden con la segunda regla, incluidos los objetos que pertenecen al arrendatario de París y que no tienen la región del cubo S3 establecida en eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, como la segunda regla utiliza procesamiento equilibrado, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Ejemplo 6: Cambiar una política de ILM

Si es necesario cambiar su protección de datos o añadir nuevos sitios, puede crear y activar una nueva política de ILM.

Antes de cambiar una política, debe comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente al rendimiento general de un sistema StorageGRID.

En este ejemplo, se ha agregado un nuevo sitio StorageGRID en una ampliación y se debe implementar una nueva política de gestión del ciclo de vida de la información activa para almacenar los datos en el nuevo sitio. Para implementar una nueva política activa, primero cree una política propuesta por cualquiera de los dos "clonación de una política existente *or* comenzando desde cero". Después, debes hacerlo "simular" y después "activar" la nueva política.

Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Cómo el cambio de una política de ILM afecta al rendimiento

Al activar una nueva política de ILM, el rendimiento de su sistema StorageGRID puede verse afectado temporalmente, especialmente si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se muevan a nuevas ubicaciones.

Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Para garantizar que una nueva política de ILM no afecte a la ubicación de los objetos existentes replicados y codificados de borrado, puede hacerlo "Cree una regla de ILM con un filtro de tiempo de ingesta". Por ejemplo, **tiempo de ingesta *es el o posterior <date and time>***, de modo que la nueva regla se aplica solo a los objetos ingeridos en o después de la fecha y hora especificadas.

Entre los tipos de cambios en la política de ILM que pueden afectar temporalmente el rendimiento de la StorageGRID se encuentran los siguientes:

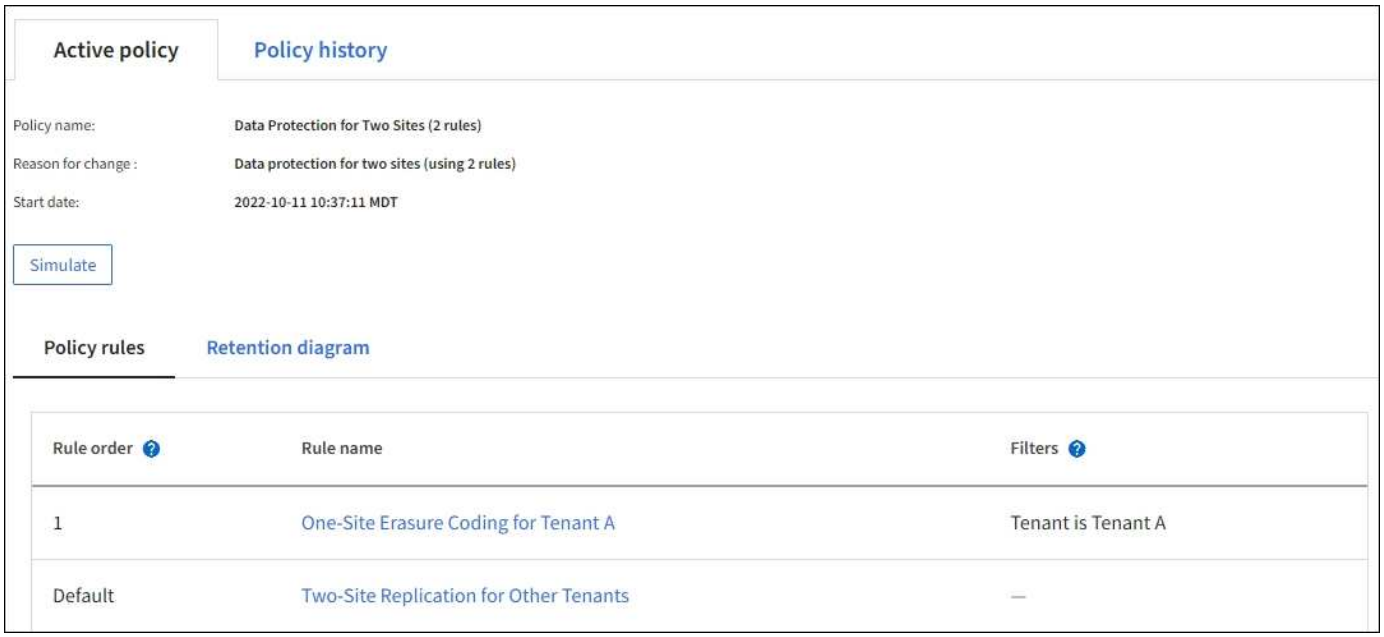
- Aplicar un perfil de código de borrado diferente a los objetos existentes con código de borrado.

  StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos de código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover un gran número de objetos hacia o desde un pool de almacenamiento en cloud, o desde un sitio remoto.

Política de ILM activa, por ejemplo 6: Protección de datos en dos sitios

En este ejemplo, la activa política de ILM se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas de ILM.



En esta política de ILM, los objetos del inquilino A están protegidos con codificación de borrado 2+1 en un único sitio, mientras que los objetos que pertenecen al resto de usuarios se protegen en dos sitios mediante replicación de copia.

> La primera regla de este ejemplo utiliza un filtro avanzado para garantizar que la codificación de borrado no se utilice para objetos pequeños. Cualquiera de los objetos del inquilino A que sean menores de 1 MB estará protegido por la regla predeterminada, que utiliza replicación.

Regla 1: Codificación de borrado de un sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de regla	Codificación de borrado de un sitio para el inquilino A
Cuenta de inquilino	Inquilinoa
Pool de almacenamiento	Sitio 1
Ubicaciones	Código de borrado 2+1 en el Sitio 1 desde el día 0 hasta siempre

Regla 2: Replicación de dos sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de dos sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1 y sitio 2

Definición de regla	Valor de ejemplo
Ubicaciones	Dos copias replicadas desde el día 0 hasta siempre: Una copia en el sitio 1 y una copia en el sitio 2.

Propuesta de política de ILM, por ejemplo 6: Protección de datos en tres sitios

En este ejemplo, la política de ILM se está reemplazando por una nueva política para un sistema StorageGRID de tres sitios.

Después de realizar una expansión para agregar el nuevo sitio, el administrador de grid creó dos nuevos pools de almacenamiento: Un pool de almacenamiento para el sitio 3 y un pool de almacenamiento que contiene los tres sitios (no el mismo que el pool de almacenamiento predeterminado de todos los nodos de almacenamiento). Posteriormente, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM propuesta, diseñada para proteger datos en los tres sitios.

Cuando se activa esta nueva política de ILM, los objetos que pertenecen al inquilino A se protegerán mediante codificación de borrado 2+1 en tres sitios, mientras que los objetos que pertenecen a otros clientes (y objetos más pequeños que pertenecen al inquilino A) se protegerán en tres sitios usando replicación de 3 copias.

Regla 1: Codificación de borrado a tres ubicaciones para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de regla	Codificación de borrado de tres sitios para el inquilino A
Cuenta de inquilino	Inquilinoa
Pool de almacenamiento	Todos los sitios 3 (incluye el sitio 1, el sitio 2 y el sitio 3)
Ubicaciones	Código de borrado 2+1 en todos los sitios 3 desde el día 0 hasta siempre

Regla 2: Replicación de tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1, Sitio 2 y Sitio 3
Ubicaciones	Tres copias replicadas desde el día 0 hasta siempre: Una copia en el sitio 1, una copia en el sitio 2 y una copia en el sitio 3.

Activar la política de ILM propuesta por ejemplo 6

Al activar una nueva política de ILM propuesta, es posible que los objetos existentes se muevan a nuevas

ubicaciones o que se puedan crear copias de objetos nuevas para los objetos existentes, según las instrucciones de colocación de cualquier regla nueva o actualizada.

> Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable. Revise y simule cuidadosamente la directiva antes de activarla para confirmar que funcionará según lo previsto.

> Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Lo que ocurre al cambiar las instrucciones de codificación de borrado

En la política de ILM actualmente activa en este ejemplo, los objetos que pertenecen al inquilino A se protegen con el código de borrado 2+1 en el sitio 1. En la nueva política de ILM propuesta, los objetos pertenecientes al inquilino A se protegerán con el código de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Los objetos nuevos procesados por el inquilino A se dividen en dos fragmentos de datos y se añade un fragmento de paridad. Entonces, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen al inquilino A se reevalúan durante el proceso de análisis de ILM en curso. Dado que las instrucciones de colocación de ILM usan un nuevo perfil de código de borrado, se crean y distribuyen fragmentos con código de borrado totalmente nuevos en los tres sitios.

> Los fragmentos 2+1 existentes en el Sitio 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

Qué ocurre cuando cambian las instrucciones de replicación

En la política de ILM actualmente activa en este ejemplo, los objetos que pertenecen a otros inquilinos se protegen usando dos copias replicadas en los pools de almacenamiento de los sitios 1 y 2. En la nueva política de ILM propuesta, los objetos que pertenezcan a otros clientes se protegerán usando tres copias replicadas en pools de almacenamiento de los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Cuando cualquier inquilino que no sea el inquilino A procesa un objeto nuevo, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Como las copias de objetos existentes en el Sitio 1 y el Sitio 2 siguen satisfaciendo los requisitos de replicación de la nueva regla de ILM, StorageGRID solo tiene que crear una nueva copia del objeto para el sitio 3.

Impacto en el rendimiento de la activación de esta política

Si se activa la política de ILM propuesta en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles superiores a los normales de recursos de grid para

crear nuevos fragmentos con código de borrado para los objetos existentes del inquilino A y nuevas copias replicadas en el sitio 3 para los objetos existentes de otros inquilinos.

Como resultado del cambio en la política de ILM, es posible que las solicitudes de lectura y escritura del cliente experimenten temporalmente más latencias normales. Las latencias volverán a los niveles normales una vez que se implementen por completo las instrucciones de colocación en el grid.

Para evitar problemas de recursos al activar una nueva política de ILM, puede utilizar el filtro avanzado de tiempo de procesamiento en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de procesamiento en mayor o igual que el tiempo aproximado en el que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.

> Si necesita ralentizar o aumentar la velocidad a la que se procesan los objetos después de un cambio de la política de ILM, póngase en contacto con el soporte técnico.

Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3

Puede usar el bloque de S3, las reglas de ILM y la política de ILM en este ejemplo como un punto de partida para definir una política de ILM para cumplir con los requisitos de retención y protección de objetos para los objetos en bloques con el bloqueo de objetos S3 habilitado.

> Si ha utilizado la función de cumplimiento de normativas anterior en versiones de StorageGRID anteriores, también puede utilizar este ejemplo para ayudar a gestionar los bloques existentes que tengan habilitada la función de cumplimiento de normativas heredadas.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Información relacionada

- "Gestione objetos con S3 Object Lock"
- "Cree una política de ILM"

Ejemplo de bloque y objetos para S3 Object Lock

En este ejemplo, una cuenta de inquilino de S3 llamada Bank of ABC ha utilizado el administrador de inquilinos para crear un bloque con el bloqueo de objetos S3 habilitado para almacenar registros bancarios críticos.

Definición de bloque	Valor de ejemplo
Nombre de cuenta de inquilino	Banco de ABC
Nombre del bloque	registros bancarios
Región de bloque	us-east-1 (predeterminado)

Cada objeto y versión de objeto que se agrega al bloque de registros bancarios utilizará los siguientes valores para `retain-until-date` y.. `legal hold` configuración.

Configuración para cada objeto	Valor de ejemplo
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 de diciembre de 2030) Cada versión de objeto tiene su propia `retain-until-date` ajuste. Este ajuste se puede aumentar, pero no disminuir.
`legal hold`	`"OFF"` (No en vigor) Se puede colocar o levantar una retención legal en cualquier versión del objeto en cualquier momento durante el período de retención. Si un objeto está sujeto a una conservación legal, dicho objeto no se puede eliminar ni siquiera si el `retain-until-date` se ha alcanzado.

Regla de ILM 1 para S3 Object Lock Ejemplo: Perfil de codificación de borrado con coincidencia de bloques

Esta regla de ILM de ejemplo se aplica solo a la cuenta de inquilino de S3 llamada Bank of ABC. Coincide con cualquier objeto de `bank-records` Bucket y, a continuación, utiliza código de borrado para almacenar el objeto en los nodos de almacenamiento en tres sitios de centros de datos mediante un perfil de código de borrado 6+3. Esta regla satisface los requisitos de los buckets con S3 Object Lock activado: Se mantiene una copia en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando el tiempo de ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla compatible: Objetos EC en el depósito de registros bancarios - Banco de ABC
Cuenta de inquilino	Banco de ABC
Nombre del bloque	`bank-records`
Filtro avanzado	Tamaño de objeto (MB) mayor que 1 **Nota:** este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menores.

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 almacenar para siempre
Perfil de código de borrado	• Cree una copia codificada con borrado en los nodos de almacenamiento en tres centros de datos • Utiliza un esquema de codificación de borrado de 6+3

Ejemplo de regla ILM 2 para bloqueo de objetos S3: Regla no conforme a las normativas

Esta regla de ILM de ejemplo almacena inicialmente dos copias de objetos replicadas en nodos de almacenamiento. Después de un año, se almacena una copia en un pool de almacenamiento en cloud para siempre. Como esta regla utiliza un pool de almacenamiento en cloud, no es compatible y no se aplica a los objetos en bloques con el bloqueo de objetos S3 habilitado.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla no conforme a las normativas: Use Cloud Storage Pool
Cuentas de inquilino	No especificado
Nombre del bloque	No se especifica, pero solo se aplica a los depósitos que no tienen S3 Object Lock (o la función de cumplimiento de normativas heredada) activada.
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	• El día 0, conserve dos copias replicadas en los nodos de almacenamiento en el centro de datos 1 y en el centro de datos 2 durante 365 días • Después de 1 año, mantenga siempre una copia replicada en un pool de almacenamiento en cloud

Ejemplo de regla ILM 3 para bloqueo de objetos S3: Regla predeterminada

Esta regla de ILM de ejemplo copia los datos de objetos en dos pools de almacenamiento en dos centros de datos. Esta regla de cumplimiento está diseñada para ser la regla predeterminada de la política de ILM. No incluye ningún filtro, no utiliza el tiempo de referencia no corriente y satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado: Se mantienen dos copias de objetos en los nodos de almacenamiento del día 0 al permanente, utilizando procesamiento como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla de conformidad predeterminada: Dos copias Dos centros de datos
Cuenta de inquilino	No especificado
Nombre del bloque	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	De día 0 a siempre, conserve dos copias replicadas (una en los nodos de almacenamiento en el centro de datos 1 y otra en los nodos de almacenamiento en el centro de datos 2).

Ejemplo de política de ILM conforme a la normativa para el bloqueo de objetos S3

Para crear una política de ILM que proteja de manera efectiva todos los objetos del sistema, incluidos los que están en bloques con el bloqueo de objetos S3 habilitado, debe seleccionar reglas de ILM que cumplan con los requisitos de almacenamiento para todos los objetos. A continuación, debe simular y activar la directiva propuesta.

Añada reglas a la política

En este ejemplo, la política de ILM incluye tres reglas de ILM, en el siguiente orden:

1. Regla de conformidad que utiliza la codificación de borrado para proteger objetos de más de 1 MB en un bloque específico con el bloqueo de objetos S3 habilitado. Los objetos se almacenan en nodos de almacenamiento del día 0 al permanente.
2. Una regla no conforme a las normativas que crea dos copias de objetos replicados en los nodos de almacenamiento durante un año y, a continuación, mueve una copia de objetos a un Cloud Storage Pool de forma permanente. Esta regla no se aplica a bloques con el bloqueo de objetos S3 habilitado porque utiliza un pool de almacenamiento en cloud.
3. La regla de cumplimiento predeterminada que crea dos copias de objetos replicados en los nodos de almacenamiento desde el día 0 hasta siempre.

Simular la política propuesta

Después de añadir reglas a la política propuesta, elegir una regla de cumplimiento predeterminada y organizar las demás reglas, debe simular la política probando objetos desde el bloque con el bloqueo de objetos S3 habilitado y desde otros bloques. Por ejemplo, al simular la directiva de ejemplo, debería esperar que los objetos de prueba se evaluaran de la siguiente manera:

- La primera regla sólo coincidirán con los objetos de prueba que son superiores a 1 MB en los registros bancarios de bloque para el inquilino Banco de ABC.
- La segunda regla coincidirán con todos los objetos de todos los segmentos no compatibles para todas las demás cuentas de arrendatario.
- La regla predeterminada coincidirán con estos objetos:
  - Objetos de 1 MB o menos en los registros bancarios del bloque para el inquilino del Banco de ABC.
  - Objetos de cualquier otro bloque que tenga habilitado el bloqueo de objetos S3 para todas las demás cuentas de inquilino.

Activar la política

Cuando esté completamente satisfecho de que la nueva política protege los datos del objeto según lo esperado, puede activarlo.

Endurecimiento del sistema

Refuerzo del sistema: Descripción general

El endurecimiento del sistema es el proceso de eliminar tantos riesgos de seguridad como sea posible a través de un sistema StorageGRID.

Este documento proporciona una descripción general de las directrices generales específicas de StorageGRID. Estas directrices complementan las mejores prácticas estándar del sector para el endurecimiento del sistema. Por ejemplo, estas directrices asumen que utiliza contraseñas seguras para StorageGRID, utiliza HTTPS en lugar de HTTP y habilite la autenticación basada en certificados cuando esté disponible.

Al instalar y configurar StorageGRID, puede usar estas directrices para ayudarle a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad del sistema de información.

StorageGRID sigue el "Política de gestión de vulnerabilidades de NetApp". Las vulnerabilidades notificadas se verifican y se tratan de acuerdo con el proceso de respuesta a incidentes de seguridad del producto.

Consideraciones generales sobre el refuerzo de los sistemas StorageGRID

Al reforzar un sistema StorageGRID, debe tener en cuenta lo siguiente:

- ¿Cuál de las tres redes StorageGRID que ha implementado? Todos los sistemas StorageGRID deben utilizar la red de cuadrícula, pero también puede utilizar la red de administración, la red de cliente o ambas. Cada red tiene diferentes consideraciones de seguridad.
- El tipo de plataformas que utiliza para los nodos individuales del sistema StorageGRID. Los nodos StorageGRID se pueden implementar en máquinas virtuales de VMware, en un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma tiene su propio conjunto de mejores prácticas de optimización.
- Qué confianza tienen las cuentas de inquilino. Si es un proveedor de servicios con cuentas de inquilino que no son de confianza, tendrá problemas de seguridad diferentes a si solo utiliza clientes internos de confianza.
- Los requisitos y convenciones de seguridad que siguen su organización. Es posible que deba cumplir requisitos normativos o corporativos específicos.

Directrices de refuerzo para las actualizaciones de software

Debe mantener su sistema StorageGRID y los servicios relacionados actualizados para defender los ataques.

Actualice al software StorageGRID

Siempre que sea posible, debe actualizar el software StorageGRID a la versión principal más reciente o a la versión principal anterior. Mantener la StorageGRID actualizada ayuda a reducir la cantidad de tiempo que las vulnerabilidades conocidas están activas y reduce el área general de la superficie de ataque. Además, las versiones más recientes de StorageGRID a menudo contienen funciones de refuerzo de la seguridad que no se incluyen en versiones anteriores.

Consulte la "Herramienta de matriz de interoperabilidad de NetApp" (IMT) Para determinar qué versión del software StorageGRID debería utilizar. Cuando se necesita una corrección, NetApp prioriza la creación de

actualizaciones para las versiones más recientes. Es posible que algunos parches no sean compatibles con versiones anteriores.

- Para descargar las versiones y correcciones urgentes de StorageGRID más recientes, vaya a. "Descargas de NetApp: StorageGRID".
- Para actualizar el software StorageGRID, consulte "instrucciones de actualización".
- Para aplicar una revisión, consulte "Procedimiento de revisión de StorageGRID".

Actualizaciones a servicios externos

Los servicios externos pueden tener vulnerabilidades que afectan indirectamente a StorageGRID. Debe asegurarse de que los servicios de los que depende StorageGRID se mantengan actualizados. Estos servicios incluyen LDAP, KMS (servidor KMIP o KMS), DNS y NTP.

Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

Actualizaciones a hipervisores

Si los nodos de StorageGRID se ejecutan en VMware u otro hipervisor, debe asegurarse de que el software y el firmware del hipervisor estén actualizados.

Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

Actualizaciones a nodos Linux

Si los nodos de StorageGRID utilizan plataformas host Linux, debe asegurarse de que las actualizaciones de seguridad y del kernel se apliquen al sistema operativo host. Además, debe aplicar actualizaciones de firmware al hardware vulnerable cuando estas actualizaciones estén disponibles.

Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

Directrices de refuerzo para redes de StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Para obtener información detallada sobre las redes StorageGRID, consulte "Tipos de red StorageGRID".

Directrices para la red Grid

Debe configurar una red de red para todo el tráfico interno de StorageGRID. Todos los nodos de grid se encuentran en Grid Network, por lo que deben poder hablar con el resto de nodos.

Al configurar Grid Network, siga estas directrices:

- Asegúrese de que la red está protegida de clientes que no son de confianza, como los que están en Internet abierto.
- Cuando sea posible, utilice la red de red exclusiva para el tráfico interno. Tanto la red de administración como la red de cliente tienen restricciones de firewall adicionales que bloquean el tráfico externo a los

servicios internos. Se admite el uso de Grid Network para el tráfico de clientes externos, pero este uso ofrece menos capas de protección.

- Si la implementación de StorageGRID abarca varios centros de datos, utilice una red privada virtual (VPN) o equivalente en la red de Grid para proporcionar protección adicional para el tráfico interno.
- Algunos procedimientos de mantenimiento requieren un acceso de shell seguro (SSH) en el puerto 22 entre el nodo de administrador principal y todos los demás nodos de grid. Use un firewall externo para restringir el acceso SSH a clientes de confianza.

Directrices para la red administrativa

La red de administración suele utilizarse para tareas administrativas (empleados de confianza que utilizan Grid Manager o SSH) y para comunicarse con otros servicios de confianza como LDAP, DNS, NTP o KMS (o servidor KMIP). Sin embargo, StorageGRID no exige este uso interno.

Si utiliza la red de administración, siga estas directrices:

- Bloquee todos los puertos de tráfico internos en la red administrativa. Consulte "lista de puertos internos".
- Si los clientes que no son de confianza pueden acceder a la red de administración, bloquee el acceso a StorageGRID en la red de administración con un firewall externo.

Directrices para la red de clientes

La red de cliente suele utilizarse para los inquilinos y para comunicarse con servicios externos, como el servicio de replicación de CloudMirror o otro servicio de la plataforma. Sin embargo, StorageGRID no exige este uso interno.

Si está utilizando la red cliente, siga estas directrices:

- Bloquee todos los puertos de tráfico internos de la red cliente. Consulte "lista de puertos internos".
- Acepte tráfico de cliente entrante sólo en puntos finales configurados explícitamente. Consulte la información acerca de "gestión de controles de firewall".

Directrices de refuerzo para nodos de StorageGRID

Los nodos StorageGRID se pueden implementar en máquinas virtuales de VMware, en un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma y cada tipo de nodo tiene su propio conjunto de prácticas recomendadas de endurecimiento.

Configuración del firewall

Como parte del proceso de endurecimiento del sistema, debe revisar las configuraciones de firewall externo y modificarlas para que el tráfico se acepte solo de las direcciones IP y en los puertos de los que se necesite estrictamente.

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad del grid al permitirle controlar el acceso de red al nodo. Usted debe "gestionar los controles internos del firewall" para evitar el acceso a la red en todos los puertos, excepto los necesarios para su implementación de grid específica. Los cambios de configuración que realice en la página de control del firewall se despliegan en cada nodo.

Específicamente, puede gestionar estas áreas:

- **Direcciones privilegiadas**: Puede permitir que las direcciones IP o subredes seleccionadas accedan a los puertos que están cerrados por la configuración en la pestaña Administrar acceso externo.
- **Administrar el acceso externo**: Puede cerrar los puertos que están abiertos por defecto, o reabrir los puertos previamente cerrados.
- **Red cliente no confiable**: Puede especificar si un nodo confía en el tráfico entrante de la red cliente, así como en los puertos adicionales que desea abrir cuando la red cliente no confiable está configurada.

Aunque este firewall interno proporciona una capa adicional de protección contra algunas amenazas comunes, no elimina la necesidad de un firewall externo.

Para obtener una lista de todos los puertos internos y externos utilizados por StorageGRID, consulte "Referencia de puerto de red".

Desactive los servicios no utilizados

Para todos los nodos StorageGRID, debe deshabilitar o bloquear el acceso a los servicios que no se utilizan. Por ejemplo, si no está planeando configurar el acceso de cliente a los recursos compartidos de auditoría para NFS, bloquee o deshabilite el acceso a estos servicios.

Virtualización, contenedores y hardware compartido

Para todos los nodos de StorageGRID, evite ejecutar StorageGRID en el mismo hardware físico que el software que no es de confianza. No asuma que las protecciones del hipervisor evitarán que el malware acceda a los datos protegidos por StorageGRID si el StorageGRID y el malware existen en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre aprovechan vulnerabilidades críticas en los procesadores modernos y permiten a los programas robar datos en memoria en el mismo equipo.

Proteja los nodos durante la instalación

No permita que usuarios que no sean de confianza accedan a los nodos StorageGRID a través de la red cuando se van a instalar los nodos. Los nodos no son totalmente seguros hasta que se han unido a la cuadrícula.

Directrices para los nodos de administrador

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Cuando inicia sesión en el administrador de grid o en el administrador de inquilinos, se conecta a un nodo de administración.

Siga estas directrices para proteger los nodos de administrador en el sistema StorageGRID:

- Proteja todos los nodos de administrador de clientes que no son de confianza, como los que están en Internet abierto. Asegúrese de que ningún cliente que no sea de confianza puede acceder a un nodo de administración en la red de grid, la red de administración o la red de cliente.
- Los grupos StorageGRID controlan el acceso a las funciones de administrador de grid y administrador de inquilinos. Otorgue a cada grupo de usuarios los permisos mínimos necesarios para su función y utilice el modo de acceso de sólo lectura para evitar que los usuarios cambien la configuración.
- Cuando se utilizan extremos de equilibrador de carga de StorageGRID, use nodos de puerta de enlace en lugar de nodos de administrador para el tráfico de cliente que no es de confianza.
- Si tiene inquilinos que no son de confianza, no permita que tengan acceso directo al administrador de inquilinos o a la API de gestión de inquilinos. En su lugar, para que los inquilinos que no son de confianza utilicen un portal de inquilinos o un sistema de gestión de inquilinos externo, que interactúa con la API de

gestión de inquilinos.

- Opcionalmente, use un proxy de administrador para obtener un mayor control sobre la comunicación de AutoSupport de los nodos de administración al soporte de NetApp. Consulte los pasos para "Creación de un proxy de administración".
- Opcionalmente, utilice los puertos restringidos 8443 y 9443 para separar las comunicaciones de Grid Manager y de arrendatario Manager. Bloquee el puerto compartido 443 y limite las solicitudes de inquilinos al puerto 9443 para obtener una protección adicional.
- De manera opcional, utilice nodos de administrador separados para los administradores de grid y los usuarios inquilinos.

Para obtener más información, consulte las instrucciones de "Administración de StorageGRID".

Directrices para nodos de almacenamiento

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Siga estas directrices para proteger los nodos de almacenamiento en el sistema StorageGRID.

- No permita que los clientes que no son de confianza se conecten directamente con los nodos de almacenamiento. Utilice un punto final de equilibrio de carga servido por un nodo de gateway o un equilibrador de carga de terceros.
- No habilite los servicios de salida para inquilinos que no son de confianza. Por ejemplo, al crear la cuenta para un inquilino que no sea de confianza, no permita que el inquilino utilice su propia fuente de identidad y no permita el uso de servicios de plataforma. Consulte los pasos para "crear una cuenta de inquilino".
- Utilice un equilibrador de carga de terceros para el tráfico de clientes que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques.
- Opcionalmente, utilice un proxy de almacenamiento para obtener más control sobre los pools de almacenamiento en cloud y la comunicación de servicios de plataforma de los nodos de almacenamiento a los servicios externos. Consulte los pasos para "Creación de un proxy de almacenamiento".
- Opcionalmente, conéctese a servicios externos mediante la red cliente. A continuación, seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall** > **Redes de clientes sin confianza** e indique que la red cliente del nodo de almacenamiento no es de confianza. El nodo de almacenamiento ya no acepta tráfico entrante en la red cliente, pero sigue permitiendo solicitudes salientes para los servicios de plataforma.

Directrices para los nodos de puerta de enlace

Los nodos de puerta de enlace proporcionan una interfaz opcional de equilibrio de carga que las aplicaciones cliente pueden utilizar para conectarse a StorageGRID. Siga estas directrices para proteger cualquier nodo de puerta de enlace en el sistema StorageGRID:

- Configurar y utilizar puntos finales del equilibrador de carga. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".
- Utilice un equilibrador de carga de terceros entre el cliente y los nodos de puerta de enlace o de almacenamiento para buscar tráfico de cliente que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques. Si utiliza un equilibrador de carga de terceros, se puede configurar opcionalmente el tráfico de red para que pase por un extremo de equilibrador de carga interno o se envíe directamente a nodos de almacenamiento.
- Si utiliza puntos finales de equilibrador de carga, haga que los clientes se conecten a través de la red de cliente de forma opcional. A continuación, seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall** > **Redes de clientes sin confianza** e indique que la red cliente del nodo de gateway no es de confianza. El nodo Gateway sólo acepta tráfico entrante en los puertos configurados explícitamente como

extremos equilibradores de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware StorageGRID están especialmente diseñados para su uso en un sistema StorageGRID. Algunos dispositivos se pueden usar como nodos de almacenamiento. Otros dispositivos se pueden usar como nodos de administrador o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o poner en marcha grids totalmente diseñados para todos los dispositivos.

Siga estas directrices para proteger cualquier nodo de dispositivo de hardware en el sistema StorageGRID:

- Si el dispositivo utiliza System Manager de SANtricity para la gestión de la controladora de almacenamiento, evite que los clientes que no son de confianza accedan a System Manager de SANtricity a través de la red.
- Si el dispositivo tiene un controlador de administración de placa base (BMC), tenga en cuenta que el puerto de administración del BMC permite un acceso bajo al hardware. Conecte el puerto de gestión de BMC sólo a una red de gestión interna segura y de confianza. Si no existe dicha red disponible, deje el puerto de administración del BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión al BMC.
- Si el dispositivo admite la administración remota del hardware de la controladora a través de Ethernet mediante el estándar de interfaz de gestión de plataforma inteligente (IPMI), bloquee el tráfico que no sea de confianza en el puerto 623.

> Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contienen un BMC mediante el extremo privado de la API de gestión, PUT /private/bmc.

- Si la controladora de almacenamiento del dispositivo incluye unidades FDE o FIPS y la función Drive Security está habilitada, use SANtricity para configurar las claves de seguridad de unidades. Consulte "Configuración del administrador del sistema de SANtricity (SG6000 y SG5700)".
- Para dispositivos sin unidades FDE o FIPS, habilite el cifrado de nodos con un servidor de gestión de claves (KMS). Consulte "Opcional: Habilite el cifrado de nodos".

Directrices de refuerzo para TLS y SSH

Debe reemplazar los certificados predeterminados creados durante la instalación y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de refuerzo para los certificados

Debe sustituir los certificados predeterminados creados durante la instalación por sus propios certificados personalizados.

Para muchas organizaciones, el certificado digital autofirmado para el acceso web StorageGRID no cumple con sus políticas de seguridad de la información. En los sistemas de producción, debe instalar un certificado digital firmado por CA para utilizarlo en la autenticación de StorageGRID.

Específicamente, debe utilizar certificados de servidor personalizados en lugar de los siguientes certificados predeterminados:

- **Certificado de interfaz de administración**: Se utiliza para asegurar el acceso a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de administración de inquilinos.

- **Certificado API S3 y Swift**: Se utiliza para garantizar el acceso seguro a los nodos de almacenamiento y los nodos de puerta de enlace, que las aplicaciones cliente S3 y Swift utilizan para cargar y descargar datos de objetos.

Consulte "Gestionar certificados de seguridad" para obtener detalles e instrucciones.

> StorageGRID gestiona los certificados utilizados para los extremos del equilibrador de carga por separado. Para configurar los certificados del equilibrador de carga, consulte "Configurar puntos finales del equilibrador de carga".

Cuando utilice certificados de servidor personalizados, siga estas directrices:

- Los certificados deben tener un *`subjectAltName`* Que coincida con las entradas de DNS para StorageGRID. Para obtener más información, consulte la sección 4.2.1.6, "Nombre alternativo de la expulsión" en "RFC 5280: Certificado PKIX y perfil CRL".
- Cuando sea posible, evite el uso de certificados comodín. Una excepción a esta directriz es el certificado para un punto final de estilo alojado virtual S3, que requiere el uso de un comodín si los nombres de depósito no se conocen por adelantado.
- Cuando debe utilizar comodines en los certificados, debe tomar medidas adicionales para reducir los riesgos. Utilice un patrón comodín como `*.s3.example.com`, y no utilice el `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con acceso S3 de estilo de ruta como, por ejemplo `dc1-s1.s3.example.com/mybucket`.
- Establezca los tiempos de caducidad del certificado como cortos (por ejemplo, 2 meses) y utilice la API de gestión de grid para automatizar la rotación del certificado. Esto es especialmente importante para los certificados con caracteres comodín.

Además, los clientes deben usar una comprobación estricta del nombre de host al comunicarse con StorageGRID.

Directrices de endurecimiento para las políticas TLS y SSH

Es posible seleccionar una política de seguridad para determinar qué protocolos y cifrados se usan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras a servicios StorageGRID internos.

La directiva de seguridad controla cómo TLS y SSH cifran los datos en movimiento. Como práctica recomendada, debe desactivar las opciones de cifrado que no son necesarias para la compatibilidad de aplicaciones. Utilice la directiva Modern predeterminada, a menos que el sistema deba cumplir con Common Criteria o que necesite utilizar otros cifrados.

Consulte "Gestione la política TLS y SSH" para obtener detalles e instrucciones.

Otras directrices de endurecimiento

Además de seguir las directrices de refuerzo para redes y nodos de StorageGRID, debe seguir las directrices de refuerzo para otras áreas del sistema StorageGRID.

Registros y mensajes de auditoría

Proteja siempre los registros de StorageGRID y los resultados de mensajes de auditoría de forma segura. Los registros y mensajes de auditoría de StorageGRID proporcionan información de gran valor desde el punto de vista del soporte y la disponibilidad del sistema. Además, la información y los detalles que contienen los

registros de StorageGRID y el resultado de un mensaje de auditoría suelen ser confidenciales.

Configure StorageGRID para que envíe eventos de seguridad a un servidor de syslog externo. Si utiliza la exportación de syslog, seleccione TLS y RELP/TLS para los protocolos de transporte.

Consulte "Referencia de archivos de registro" Para obtener más información acerca de los registros de StorageGRID. Consulte "Auditar mensajes" Para obtener más información acerca de los mensajes de auditoría de StorageGRID.

AutoSupport de NetApp

La función AutoSupport de StorageGRID permite supervisar de manera proactiva el estado del sistema y enviar automáticamente mensajes y detalles al soporte técnico de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera predeterminada, los mensajes de AutoSupport en el soporte técnico de NetApp se habilitan cuando StorageGRID se configura por primera vez.

Es posible deshabilitar la función AutoSupport. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y resolución de problemas en caso de que se produzca un problema en su sistema StorageGRID.

AutoSupport admite HTTPS, HTTP y SMTP para los protocolos de transporte. Debido a la naturaleza confidencial de los mensajes de AutoSupport, NetApp recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport a los servicios de soporte de NetApp.

Uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un depósito de S3 si desea que las aplicaciones web de otros dominios puedan acceder a ese depósito y a los objetos de ese depósito. En general, no active CORS a menos que sea necesario. Si se requiere CORS, restringirlo a orígenes de confianza.

Consulte los pasos para "Configuración del uso compartido de recursos de origen cruzado (CORS)".

Dispositivos de seguridad externos

Una solución completa de consolidación debe abordar los mecanismos de seguridad fuera de StorageGRID. El uso de dispositivos de infraestructura adicionales para filtrar y limitar el acceso a StorageGRID es una forma efectiva de establecer y mantener una política de seguridad estricta. Estos dispositivos de seguridad externos incluyen firewalls, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda un equilibrador de carga de terceros para el tráfico de clientes que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques.

Mitigación de ransomware

Ayuda a proteger los datos de objetos frente a ataques de ransomware siguiendo las recomendaciones de "Defensa contra ransomware con StorageGRID".

Configure StorageGRID para FabricPool

Configure StorageGRID para FabricPool: Información general

Si utiliza el software ONTAP de NetApp, puede utilizar FabricPool de NetApp para organizar en niveles los datos inactivos en un sistema de almacenamiento de objetos de StorageGRID de NetApp.

Utilice estas instrucciones para:

- Conozca las consideraciones y las prácticas recomendadas para configurar StorageGRID para una carga de trabajo FabricPool.
- Aprenda a configurar un sistema de almacenamiento de objetos StorageGRID para su uso con FabricPool.
- Aprenda a proporcionar los valores necesarios a ONTAP al añadir StorageGRID como nivel de cloud de FabricPool.

Inicio rápido para configurar StorageGRID para FabricPool

Planificación de la configuración

- Decidir qué política de organización en niveles de volúmenes de FabricPool utilizará para organizar los datos de ONTAP inactivos en StorageGRID.
- Planificar e instalar un sistema StorageGRID para satisfacer sus necesidades de rendimiento y capacidad de almacenamiento.
- Familiarícese con el software del sistema StorageGRID, incluido el "Administrador de grid" y la "Administrador de inquilinos".
- Consulte las prácticas recomendadas de FabricPool para "Grupos DE ALTA disponibilidad", "balanceo de carga", "ILM", y. "más".
- Revise estos recursos adicionales, que ofrecen detalles sobre el uso y la configuración de ONTAP y FabricPool:

  "TR-4598: Prácticas recomendadas de FabricPool en ONTAP"

  "ONTAP 9: Información general de gestión de niveles de FabricPool con System Manager"

Realizar tareas de requisitos previos

Obtenga el "Información necesaria para adjuntar StorageGRID como nivel de nube", incluyendo:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Opcionalmente, configure "federación de identidades" y.. "inicio de sesión único".

Configure los ajustes de StorageGRID

Utilice StorageGRID para obtener los valores que ONTAP necesita para conectarse a la cuadrícula.

Con el "Asistente de configuración de FabricPool" es la forma recomendada y la más rápida de configurar todos los elementos, pero también puede configurar cada entidad manualmente, si es necesario.

4 **Configure ONTAP y DNS**

Utilice ONTAP para "añada un nivel de cloud" Que utiliza los valores de StorageGRID. A continuación, "Configurar entradas DNS" Para asociar direcciones IP a cualquier nombre de dominio que desee utilizar.

5 **Supervisar y gestionar**

Cuando el sistema esté activo, lleve a cabo tareas continuas en ONTAP y StorageGRID para gestionar y supervisar la organización en niveles de los datos de FabricPool a lo largo del tiempo.

¿Qué es FabricPool?

FabricPool es una solución de almacenamiento híbrido de ONTAP que utiliza un agregado flash de alto rendimiento como nivel de rendimiento y un almacén de objetos como nivel del cloud. El uso de agregados habilitados para FabricPool le ayuda a reducir el coste del almacenamiento sin comprometer el rendimiento, la eficiencia o la protección.

FabricPool asocia un nivel de cloud (un almacén de objetos externo, como StorageGRID) con un nivel local (un agregado de almacenamiento de ONTAP) para crear una colección de discos compuesta. A continuación, los volúmenes del FabricPool pueden aprovechar la organización en niveles porque mantienen los datos activos (calientes) en un almacenamiento de alto rendimiento (el nivel local) y organizan en niveles los datos inactivos (fríos) en el almacén de objetos externo (el nivel de cloud).

No se necesitan cambios de arquitectura y puede continuar gestionando sus datos y entorno de aplicaciones desde el sistema de almacenamiento de ONTAP central.

¿Qué es StorageGRID?

StorageGRID de NetApp es una arquitectura de almacenamiento que gestiona los datos como objetos, frente a otras arquitecturas de almacenamiento, como almacenamiento de archivos o bloques. Los objetos se mantienen dentro de un único contenedor (como un depósito) y no se anidan como archivos dentro de un directorio dentro de otros directorios. Aunque el almacenamiento de objetos por lo general proporciona un rendimiento menor que el almacenamiento de archivos o bloques, es mucho más escalable. Los bloques de StorageGRID pueden alojar petabytes de datos y miles de millones de objetos.

¿Por qué usar StorageGRID como nivel de cloud de FabricPool?

FabricPool puede organizar en niveles los datos de ONTAP en diversos proveedores de almacenamiento de objetos, incluidos StorageGRID. A diferencia de los clouds públicos que podrían establecer un número máximo de operaciones de entrada/salida por segundo (IOPS) admitidas a nivel de bloque o contenedor, el rendimiento de StorageGRID se escala con el número de nodos de un sistema. Usar StorageGRID como nivel de cloud de FabricPool le permite mantener sus datos fríos en su propio cloud privado para obtener el máximo rendimiento y un control total sobre sus datos.

Además, no hace falta una licencia de FabricPool cuando utiliza StorageGRID como nivel de cloud.

Información necesaria para adjuntar StorageGRID como nivel de cloud

Para poder asociar StorageGRID como nivel de nube para FabricPool, debe realizar

pasos de configuración en StorageGRID y obtener determinados valores para utilizarlos en ONTAP.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y cómo los utiliza ONTAP y el servidor DNS.

Valor	Donde se configura el valor	Donde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del equilibrador de carga	System Manager de ONTAP > Agregar nivel de cloud
Certificado SSL	StorageGRID > Punto final del equilibrador de carga	System Manager de ONTAP > Agregar nivel de cloud
Nombre del servidor (FQDN)	StorageGRID > Punto final del equilibrador de carga	Entrada DNS
ID de clave de acceso y clave de acceso secreta	StorageGRID > inquilino y bloque	System Manager de ONTAP > Agregar nivel de cloud
Nombre de cubo/contenedor	StorageGRID > inquilino y bloque	System Manager de ONTAP > Agregar nivel de cloud

¿Cómo obtengo estos valores?

Dependiendo de sus requisitos, puede hacer cualquiera de los siguientes pasos para obtener la información que necesita:

- Utilice la "Asistente de configuración de FabricPool". El asistente de configuración de FabricPool ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera un archivo que puede utilizar para configurar System Manager de ONTAP. El asistente le guiará por los pasos necesarios y le ayudará a garantizar que la configuración cumple las prácticas recomendadas de StorageGRID y FabricPool.
- Configure cada elemento manualmente. A continuación, introduzca los valores en ONTAP System Manager o en la CLI de ONTAP. Siga estos pasos:
  a. "Configure un grupo de alta disponibilidad para FabricPool".
  b. "Cree un extremo de equilibrador de carga para FabricPool".
  c. "Cree una cuenta de inquilino para FabricPool".
  d. Inicie sesión en la cuenta de inquilino, y. "cree el bloque y las claves de acceso para el usuario raíz".
  e. Crear una regla de ILM para los datos de FabricPool y añadirla a su política de ILM activa. Consulte "Configurar ILM para los datos de FabricPool".
  f. Opcionalmente, "Cree una política de clasificación del tráfico para FabricPool".

Use el asistente de configuración de FabricPool

Use el asistente de configuración de FabricPool: Consideraciones y requisitos

Puede usar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de cloud de FabricPool. Después de completar el asistente de configuración, puede introducir los detalles necesarios en ONTAP System Manager.

Cuándo utilizar el asistente de configuración de FabricPool

El asistente de configuración de FabricPool lo guiará a través de cada paso de configuración de StorageGRID para su uso con FabricPool y configurará automáticamente ciertas entidades para usted, como ILM y las políticas de clasificación de tráfico. Como parte de completar el asistente, descargará un archivo que podrá utilizar para introducir valores en ONTAP System Manager. Utilice el asistente para configurar su sistema con mayor rapidez y asegurarse de que su configuración cumple las prácticas recomendadas de StorageGRID y FabricPool.

Suponiendo que dispone de permiso de acceso de raíz, puede completar el asistente de configuración de FabricPool cuando comience a utilizar el Administrador de grid de StorageGRID, o bien puede acceder al asistente y completarlo en cualquier momento posterior. En función de los requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y, a continuación, utilizar el asistente para ensamblar los valores que ONTAP necesita en un único archivo.

Use el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

Antes de utilizar el asistente

Confirme que ha completado estos pasos de requisitos previos.

Revise las prácticas recomendadas

- Usted tiene una comprensión general de "Información necesaria para adjuntar StorageGRID como nivel de nube".
- Ha revisado las prácticas recomendadas de FabricPool para:
  - "Grupos de alta disponibilidad"
  - "Balanceo de carga"
  - "Reglas y políticas de ILM"

Obtenga direcciones IP y configure interfaces VLAN

Si va a configurar un grupo de alta disponibilidad, sabrá a qué nodos se conectará ONTAP y a qué red StorageGRID se usará. También sabe qué valores introducir para la subred CIDR, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de FabricPool, ya habrá configurado la interfaz de VLAN. Consulte "Configure las interfaces VLAN".

Configurar la federación de identidades y SSO

Si tiene pensado utilizar la federación de identidades o el inicio de sesión único (SSO) para el sistema StorageGRID, tiene activadas estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará ONTAP. Consulte "Usar la federación de identidades" y.. "Configurar el inicio de sesión único".

Obtener y configurar nombres de dominio

- Sabe qué nombre de dominio completo (FQDN) debe utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree con el asistente. Consulte "Configure el servidor DNS".
- Si tiene pensado utilizar S3 solicitudes virtuales de estilo hospedado, tiene "Nombres de dominio de punto final S3 configurados". ONTAP utiliza URL de estilo de ruta de forma predeterminada, pero se recomienda el uso de solicitudes virtuales de estilo hospedado.

Revisión de los requisitos del equilibrio de carga y del certificado de seguridad

Si tiene pensado utilizar el equilibrador de carga StorageGRID, ha revisado el general "consideraciones que tener en cuenta al equilibrio de carga". Tiene los certificados que cargará o los valores necesarios para generar un certificado.

Si planea utilizar un punto final de equilibrio de carga externo (de terceros), tiene el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Confirmar la configuración del pool de almacenamiento ILM

Si actualizó a StorageGRID 11,7 desde una versión anterior de StorageGRID, configuró el pool de almacenamiento que usará. En general, debe crear un pool de almacenamiento para cada sitio de StorageGRID que utilizará para almacenar los datos de ONTAP.

> Este requisito previo no se aplica a las nuevas instalaciones de StorageGRID 11,7. Cuando se instala StorageGRID 11,7 en un nuevo grid, se crean automáticamente pools de almacenamiento para cada sitio.

Relación entre ONTAP y el nivel de cloud de StorageGRID

El asistente de FabricPool lo guiará por el proceso de creación de un único nivel de cloud de StorageGRID que incluye un inquilino de StorageGRID, un conjunto de claves de acceso y un bloque de StorageGRID. Puede asociar este nivel de cloud de StorageGRID a uno o más niveles locales de ONTAP.

La práctica recomendada general es asociar un solo nivel cloud a varios niveles locales en un clúster. Sin embargo, según sus requisitos, es posible que desee utilizar más de un bloque o incluso más de un inquilino StorageGRID para los niveles locales en un único clúster. El uso de diferentes bloques e inquilinos permite aislar el acceso a los datos y los datos entre las capas locales de ONTAP, pero resulta más complejo de configurar y gestionar.

NetApp no recomienda vincular un único nivel de cloud a niveles locales en varios clústeres.

> Para conocer las prácticas recomendadas para usar StorageGRID con NetApp MetroCluster™ y FabricPool Mirror, consulte "TR-4598: Prácticas recomendadas de FabricPool en ONTAP".

Opcional: Use un bloque diferente para cada nivel local

Para utilizar más de un bloque para los niveles locales de un clúster de ONTAP, añada más de un nivel de cloud de StorageGRID en ONTAP. Cada nivel de cloud comparte el mismo grupo de alta disponibilidad, extremo de balanceador de carga, inquilino y claves de acceso, pero utiliza un contenedor diferente (bloque de StorageGRID). Siga estos pasos generales:

1. En Grid Manager de StorageGRID, complete el asistente de configuración de FabricPool para el primer nivel de cloud.
2. En ONTAP System Manager, añada un nivel de cloud y utilice el archivo que ha descargado desde StorageGRID para proporcionar los valores necesarios.
3. En el Administrador de inquilinos de StorageGRID, inicie sesión en el inquilino que creó el asistente y cree un segundo bloque.
4. Vuelva a completar el asistente FabricPool. Seleccione el grupo de alta disponibilidad existente, el extremo del equilibrador de carga y el inquilino. A continuación, seleccione el nuevo bloque que creó manualmente. Cree una regla de ILM nueva para el nuevo bloque y active una política de ILM para incluir esa regla.
5. En ONTAP, añada un segundo nivel de cloud, pero proporcione el nuevo nombre del bloque.

Opcional: Use un inquilino y un depósito diferentes para cada nivel local

Para usar más de un inquilino y conjuntos diferentes de claves de acceso para los niveles locales de un clúster de ONTAP, añada más de un nivel de cloud de StorageGRID en ONTAP. Cada nivel de cloud comparte el mismo grupo de alta disponibilidad, extremo de balanceador de carga, pero utiliza un inquilino, claves de acceso y contenedor (bloque de StorageGRID) diferentes. Siga estos pasos generales:

1. En Grid Manager de StorageGRID, complete el asistente de configuración de FabricPool para el primer nivel de cloud.
2. En ONTAP System Manager, añada un nivel de cloud y utilice el archivo que ha descargado desde StorageGRID para proporcionar los valores necesarios.
3. Vuelva a completar el asistente FabricPool. Seleccione el grupo de alta disponibilidad existente y el extremo del equilibrador de carga. Cree un inquilino y un bloque nuevos. Cree una regla de ILM nueva para el nuevo bloque y active una política de ILM para incluir esa regla.
4. En ONTAP, añada un segundo nivel de cloud pero proporcione la nueva clave de acceso, la clave secreta y el nombre del bloque.

Acceda al asistente de configuración de FabricPool y complete este

Puede usar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de cloud de FabricPool.

Antes de empezar

- Ha revisado el "consideraciones y requisitos" Para utilizar el asistente de configuración de FabricPool.

> Si desea configurar StorageGRID para utilizarlo con cualquier otra aplicación cliente S3, vaya a. "Utilice el asistente de configuración de S3".

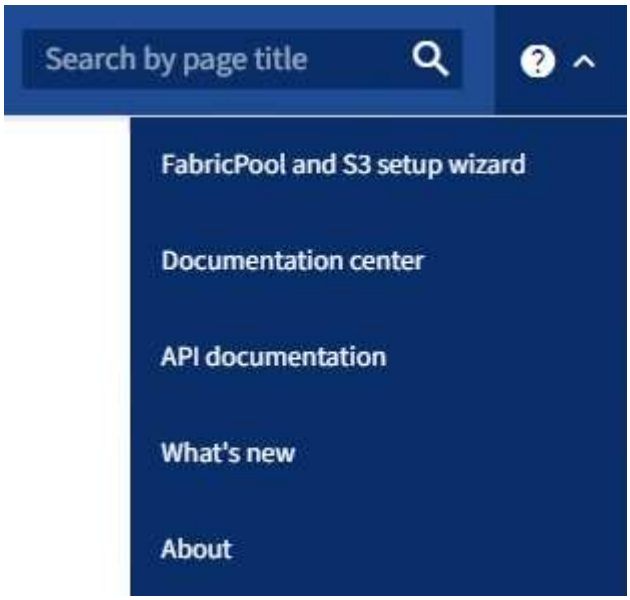
- Tiene el permiso acceso raíz.

Acceda al asistente

Puede completar el asistente de configuración de FabricPool cuando empiece a usar el Administrador de grid de StorageGRID, o bien puede acceder al asistente y completarlo en cualquier momento posterior.

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Si el banner del asistente de configuración **FabricPool y S3** aparece en el panel de control, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el icono de ayuda en la barra de encabezado del Administrador de cuadrículas y seleccione **FabricPool y el asistente de configuración S3**.



3. En la sección FabricPool de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

   Paso 1 de 9: Aparece CONFIGURAR GRUPO HA.

Paso 1 de 9: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contienen el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela, nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener disponibles las conexiones de datos FabricPool. Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si falla la interfaz activa en el grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool

Para obtener más detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad" y.. "Mejores prácticas para grupos de alta disponibilidad".

Pasos

1. Si va a utilizar un equilibrador de carga externo, no es necesario crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a. Paso 2 de 9: Configurar punto final de equilibrio de carga.
2. Para usar el balanceador de carga de StorageGRID, cree un grupo de alta disponibilidad nuevo o use un grupo de alta disponibilidad existente.

Crear grupo de alta disponibilidad

a. Para crear un nuevo grupo HA, selecciona **Crear grupo HA**.

b. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

d. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

e. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en CIDR notation—Una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para volver al asistente de configuración de FabricPool.

g. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Use el grupo de alta disponibilidad existente

a. Para usar un grupo HA existente, seleccione el nombre del grupo HA en la lista desplegable **Select an HA group**.

b. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Paso 2 de 9: Configurar punto final de equilibrio de carga

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Puede usar el servicio de equilibrador de carga de StorageGRID, que existe en todos los nodos de administración y puerta de enlace, o puede conectarse a un equilibrador de carga externo (de terceros). Se recomienda utilizar el equilibrador de carga de StorageGRID.

Para obtener detalles sobre esta tarea, consulte la sección general "consideraciones que tener en cuenta al equilibrio de carga" y la "Prácticas recomendadas para el equilibrio de carga para FabricPool".

Pasos

1. Seleccione o cree un extremo de equilibrador de carga de StorageGRID o utilice un equilibrador de carga externo.

Crear punto final

a. Seleccione **Crear punto final**.

b. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que estos puertos están reservados en los nodos de Admin. **Nota:** Los puertos utilizados por otros servicios de red no están permitidos. Consulte"Referencia de puerto de red".
Tipo de cliente	Debe ser **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

c. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final—utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Opción	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.

Opción	Descripción
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

d. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. **Permitir a todos los inquilinos** es casi siempre la opción apropiada para el punto final del equilibrador de carga utilizado para FabricPool. Debe seleccionar esta opción si está utilizando el asistente de configuración de FabricPool para un sistema de StorageGRID nuevo y todavía no ha creado ninguna cuenta de inquilino.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

e. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener detalles sobre lo que se debe introducir.
Usar certificado StorageGRID S3 y Swift	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados API S3 y Swift" para obtener más detalles.

f. Seleccione **Finalizar** para volver al asistente de configuración de FabricPool.

g. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilizar punto final de equilibrio de carga existente

a. Seleccione el nombre de un punto final existente de la lista desplegable **Select a load balancer endpoint**.

b. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Utilizar equilibrador de carga externo

a. Complete los siguientes campos para el equilibrador de carga externo.

Campo	Descripción
FQDN	Nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	Número de puerto que FabricPool utilizará para conectar al equilibrador de carga externo.
Certificado	Copie el certificado del servidor para el equilibrador de carga externo y péguelo en este campo.

b. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Paso 3 de 9: Inquilino y cubo

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, bloques, objetos y un conjunto específico de funcionalidades. Debe crear un inquilino de StorageGRID antes de poder crear el bloque que utilizará FabricPool.

Un bucket es un contenedor que se usa para almacenar los objetos y los metadatos de objetos de un inquilino. Aunque es posible que algunos inquilinos tengan muchos buckets, el asistente le permite crear o seleccionar solo un inquilino y un bucket a la vez. Puede utilizar el Gestor de inquilinos más adelante para agregar los depósitos adicionales que necesite.

Puede crear un inquilino y un bloque nuevos para uso de FabricPool, o puede seleccionar un inquilino y un bloque existentes. Si crea un inquilino nuevo, el sistema crea automáticamente el ID de clave de acceso y la clave de acceso secreta para el usuario raíz del inquilino.

Para obtener más detalles sobre esta tarea, consulte "Cree una cuenta de inquilino para FabricPool" y.. "Cree un bloque de S3 y obtenga una clave de acceso".

Pasos

Cree un nuevo arrendatario y un bloque o seleccione un arrendatario existente.

Inquilino y bloque nuevos

1. Para crear un nuevo inquilino y depósito, introduzca un **Nombre del inquilino**. Por ejemplo: `FabricPool tenant`.
2. Defina el acceso raíz para la cuenta de inquilino en función de si utiliza el sistema StorageGRID "federación de identidades", "Inicio de sesión único (SSO)", o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

3. Para **Nombre del cubo**, ingrese el nombre del cubo que FabricPool usará para almacenar datos de ONTAP. Por ejemplo: `fabricpool-bucket`.

   No puede cambiar el nombre del bloque después de crear el bloque.

4. Seleccione la **Región** para este cubo.

   Utilice la región predeterminada (us-east-1) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del bloque.

5. Seleccione **Crear y continuar** para crear el inquilino y el depósito y para ir al paso de datos de descarga

Seleccione tenant and bucket

La cuenta de inquilino existente debe tener al menos un depósito que no tenga el control de versiones activado. No puede seleccionar una cuenta de arrendatario existente si no existe ningún depósito para ese arrendatario.

1. Seleccione el arrendatario existente de la lista desplegable **Nombre del arrendatario**.
2. Seleccione el cubo existente de la lista desplegable **Nombre del cubo**.

   FabricPool no admite el control de versiones de objetos, por lo que no se muestran los bloques que tienen el control de versiones activado.

   No seleccione un depósito que tenga S3 Object Lock habilitado para su uso con FabricPool.

3. Seleccione **Continuar** para ir al paso de datos de descarga.

Paso 4 de 9: Descargar la configuración de ONTAP

Durante este paso, debe descargar un archivo que puede usar para introducir valores en ONTAP System Manager.

Pasos

1. Si lo desea, seleccione el icono de copia ( ) Para copiar el ID de clave de acceso y la clave de acceso secreta en el portapapeles.

   Estos valores están incluidos en el archivo de descarga, pero es posible que desee guardarlos por separado.

2. Selecciona **Descargar configuración de ONTAP** para descargar un archivo de texto que contenga los valores que has introducido hasta ahora.

   La `ONTAP_FabricPool_settings_bucketname.txt` En el archivo se incluye la información que necesita configurar StorageGRID como sistema de almacenamiento de objetos para un nivel de cloud de FabricPool, lo que incluye:

   - Detalles de conexión del balanceador de carga, incluido el nombre del servidor (FQDN), el puerto y el certificado
   - Nombre del bloque
   - El ID de clave de acceso y la clave de acceso secreta para el usuario raíz de la cuenta de inquilino

3. Guarde las claves copiadas y el archivo descargado en una ubicación segura.

   No cierre esta página hasta que haya copiado ambas claves de acceso, descargado la configuración de ONTAP o ambas. Las teclas no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura, ya que se puede utilizar para obtener datos de su sistema StorageGRID.

4. Seleccione la casilla de verificación para confirmar que ha descargado o copiado el ID de clave de acceso y la clave de acceso secreta.
5. Seleccione **Continuar** para ir al paso del pool de almacenamiento ILM.

Paso 5 de 9: Seleccione un pool de almacenamiento

Un pool de almacenamiento es un grupo de nodos de almacenamiento. Cuando se selecciona un pool de almacenamiento, se determina qué nodos StorageGRID utilizará para almacenar los datos organizados en niveles de ONTAP.

Para obtener más información sobre este paso, consulte "Cree un pool de almacenamiento".

Pasos

1. En la lista desplegable **Sitio**, selecciona el sitio StorageGRID que deseas usar para los datos organizados en niveles desde ONTAP.
2. En la lista desplegable **Pool de almacenamiento**, seleccione el grupo de almacenamiento para ese sitio.

   El pool de almacenamiento para un sitio incluye todos los nodos de almacenamiento en ese sitio.

3. Seleccione **Continuar** para ir al paso de la regla ILM.

Paso 6 de 9: Revise la regla de gestión de la vida útil de la información para FabricPool

Las reglas de gestión de la vida útil de la información controlan la ubicación, la duración y el comportamiento de procesamiento de todos los objetos del sistema StorageGRID.

El asistente de configuración de FabricPool crea automáticamente la regla de ILM recomendada para su uso en FabricPool. Esta regla se aplica sólo al bloque especificado. Utiliza código de borrado 2+1 en un único sitio para almacenar los datos organizados en niveles de ONTAP.

Para obtener más información sobre este paso, consulte "Cree la regla de ILM" y.. "Prácticas recomendadas para usar ILM con datos de FabricPool".

Pasos

1. Revise los detalles de la regla.

Campo	Descripción
Nombre de regla	Se genera automáticamente y no se puede cambiar
Descripción	Se genera automáticamente y no se puede cambiar
Filtro	El nombre del cubo Esta regla sólo se aplica a los objetos guardados en el depósito especificado.
Tiempo de referencia	Tiempo de ingesta La instrucción de colocación comienza cuando los objetos se guardan inicialmente en el depósito.
Instrucción de colocación	Use el código de borrado 2+1 desde el día 0 hasta siempre

2. Ordena el diagrama de retención por **periodo de tiempo** y **Grupo de almacenamiento** para confirmar la instrucción de colocación.
   - El **período de tiempo** para la regla es **Día 0 - Para siempre**. **Día 0** significa que la regla se aplica cuando los datos se almacenan en niveles desde ONTAP. **Forever** significa que StorageGRID ILM no eliminará los datos que se han organizado en niveles desde ONTAP.
   - El **Pool de almacenamiento** para la regla es el pool de almacenamiento seleccionado. **EC 2+1** significa que los datos se almacenarán utilizando la codificación de borrado 2+1. Cada objeto se guardará como dos fragmentos de datos y un fragmento de paridad. Los tres fragmentos para cada objeto se guardarán en nodos de almacenamiento diferentes en un único sitio.
3. Seleccione **Crear y continuar** para crear esta regla y para ir al paso de la política de ILM.

Paso 7 de 9: Revisar y activar la política de ILM

Una vez que el asistente de configuración de FabricPool crea la regla de ILM para su uso en FabricPool, crea una política de ILM propuesta. Debe revisar cuidadosamente esta política antes de activarla.

Para obtener más información sobre este paso, consulte "Cree una política de ILM" y.. "Prácticas

recomendadas para usar ILM con datos de FabricPool".

> Al activar una nueva política de ILM, StorageGRID utiliza esa política para gestionar la ubicación, la duración y la protección de datos de todos los objetos del grid, incluidos los objetos existentes y los objetos recién procesados. En algunos casos, la activación de una nueva política puede provocar que los objetos existentes se muevan a nuevas ubicaciones.

> Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool. Establezca el período de retención en **Forever** para asegurarse de que los objetos FabricPool no sean eliminados por StorageGRID ILM.

Pasos

1. Opcionalmente, actualice el **Policy name** generado por el sistema. De forma predeterminada, el sistema agrega «`+ FabricPool » al nombre de su política activa o propuesta, pero puede proporcionar su propio nombre.
2. Revise la lista de reglas en la política propuesta.
   - Si el grid no tiene una política de ILM propuesta, el asistente crea una política propuesta clonando su política activa y agregando la nueva regla a la parte superior.
   - Si el grid ya tiene una política de ILM propuesta y esa política utiliza las mismas reglas y el mismo orden que la política de ILM activa, el asistente añade la nueva regla a la parte superior de la política propuesta.
   - Si la política propuesta contiene reglas diferentes o un orden diferente al de la política activa, aparecerá un mensaje. Debe añadir manualmente la nueva regla de FabricPool a la política de ILM. Siga estos pasos, en función de si desea comenzar desde la política activa o la política propuesta.

Política desde la que empezar	Pasos
Política activa	i. Seleccione **ILM** > **Policies** en el menú de la izquierda en Grid Manager. ii. Seleccione la pestaña Política propuesta. iii. Selecciona **Acciones** > **Eliminar** para eliminar la política propuesta existente. iv. Vuelva al asistente de configuración de FabricPool. Ahora el asistente puede clonar su política activa para crear una nueva política propuesta. La nueva regla FabricPool se añadirá a la parte superior.
Política propuesta	i. Seleccione **ILM** > **Policies** en el menú de la izquierda en Grid Manager. ii. Seleccione la pestaña Política propuesta. iii. Selecciona **Acciones** > **Editar** para editar la política propuesta existente. iv. Agregue la nueva regla FabricPool a la parte superior. v. Active la política actualizada. vi. Vaya a la clasificación de tráfico paso.

Consulte "Cree la política de ILM propuesta" si necesita instrucciones más detalladas.

3. Revise el orden de las reglas en la nueva política.

   Puesto que la regla FabricPool es la primera regla, los objetos del depósito de FabricPool se colocan antes de que se evalúen las demás reglas de la política. Los objetos de cualquier otro depósito se colocan por reglas posteriores de la política.

4. Revise el diagrama de retención para saber cómo se retendrán los diferentes objetos.
   a. Seleccione **Expandir todo** para ver un diagrama de retención para cada regla en la política propuesta.
   b. Seleccione **Período de tiempo** y **Grupo de almacenamiento** para revisar el diagrama de retención. Confirme que cualquier regla que se aplique al depósito o inquilino de FabricPool retenga objetos **para siempre**.
5. Cuando haya revisado la política propuesta, seleccione **Activar y continuar** para activar la política y vaya al paso de clasificación de tráfico.

> Los errores en una política de ILM pueden provocar una pérdida de datos irreparable. Revise la política detenidamente antes de activarla.

Paso 8 de 9: Crear política de clasificación de tráfico

Como opción, el asistente de configuración de FabricPool puede crear una política de clasificación del tráfico que puede utilizar para supervisar la carga de trabajo de FabricPool. La política creada por el sistema utiliza una regla de coincidencia para identificar todo el tráfico de red relacionado con el bloque que ha creado. Esta política supervisa únicamente el tráfico; no limita el tráfico de FabricPool ni de otros clientes.

Para obtener más información sobre este paso, consulte "Cree una directiva de clasificación del tráfico para FabricPool".

Pasos

1. Revise la política.
2. Si desea crear esta política de clasificación de tráfico, seleccione **Crear y continuar**.

   Tan pronto como FabricPool empiece a organizar los datos en niveles en StorageGRID, puede ir a la página Directivas de clasificación del tráfico para ver las métricas del tráfico de red para esta directiva. Posteriormente, también puede agregar reglas para limitar otras cargas de trabajo y asegurarse de que la carga de trabajo de la FabricPool tenga la mayor parte del ancho de banda.

3. De lo contrario, selecciona **Omitir este paso**.

Paso 9 de 9: Resumen de la revisión

El resumen proporciona detalles sobre los elementos configurados, incluidos el nombre del equilibrador de carga, el inquilino y el bloque, la política de clasificación de tráfico y la política de ILM activa.

Pasos

1. Revise el resumen.
2. Seleccione **Finalizar**.

Siguientes pasos

Después de completar el asistente FabricPool, realice estos pasos adicionales.

Pasos

1. Vaya a. "Configure System Manager de ONTAP" Para introducir los valores guardados y completar el lado ONTAP de la conexión. Debe añadir StorageGRID como nivel de cloud, adjuntar el nivel de cloud a un nivel local para crear una FabricPool y establecer las políticas de organización en niveles de los volúmenes.
2. Vaya a. "Configure el servidor DNS" Y asegúrese de que el DNS incluye un registro para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilizará.
3. Vaya a. "Otras prácticas recomendadas para StorageGRID y FabricPool" Para conocer las mejores prácticas para los registros de auditoría de StorageGRID y otras opciones de configuración global.

Configure StorageGRID manualmente

Crear un grupo de alta disponibilidad para FabricPool

Al configurar StorageGRID para su uso con FabricPool, puede opcionalmente crear uno o varios grupos de alta disponibilidad (ha). Un grupo de alta disponibilidad es una colección de nodos que contiene cada uno de ellos el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela, nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener disponibles las conexiones de datos FabricPool. Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si falla la interfaz activa en el grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Para obtener más detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha revisado el "prácticas recomendadas para grupos de alta disponibilidad".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Si planea utilizar una VLAN, ha creado la interfaz VLAN. Consulte "Configure las interfaces VLAN".

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.
3. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

4. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

5. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

   Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

   La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

   Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

6. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en CIDR notation—Una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

7. Seleccione **Crear grupo ha** y, a continuación, seleccione **Finalizar**.

Cree un extremo de equilibrador de carga para FabricPool

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Al configurar StorageGRID para su uso con FabricPool, debe configurar un extremo de equilibrador de carga y cargar o generar un certificado de extremo de equilibrador de carga, que se utiliza para proteger la conexión entre ONTAP y StorageGRID.

Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.
- Ha revisado el general "consideraciones que tener en cuenta al equilibrio de carga" así como la "Prácticas recomendadas para el equilibrio de carga para FabricPool".

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Seleccione **Crear**.
3. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway. Estos puertos están reservados en los nodos de administrador. **Nota:** Los puertos utilizados por otros servicios de red no están permitidos. Consulte"Referencia de puerto de red". Proporcionará este número a ONTAP cuando adjunte StorageGRID como nivel de cloud de FabricPool.
Tipo de cliente	Seleccione **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

4. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final—utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Opción	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

5. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. **Permitir a todos los inquilinos** es casi siempre la opción apropiada para el punto final del equilibrador de carga utilizado para FabricPool. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de arrendatario.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

6. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener detalles sobre lo que se debe introducir.
Usar certificado StorageGRID S3 y Swift	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados API S3 y Swift" para obtener más detalles.

7. Seleccione **Crear**.

> Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Cree una cuenta de inquilino para FabricPool

Debe crear una cuenta de inquilino en el Gestor de grid para uso de FabricPool.

Las cuentas de inquilino permiten a las aplicaciones cliente almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, bloques y objetos.

Para obtener más detalles sobre esta tarea, consulte "Cree una cuenta de inquilino". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso específicos.

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear**.
3. Para los pasos Enter details, introduzca la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.
Descripción (opcional)	Descripción para ayudar a identificar al inquilino.
Tipo de cliente	Debe ser **S3** para FabricPool.

Campo	Descripción
Cuota de almacenamiento (opcional)	Deje este campo en blanco para FabricPool.

4. Para el paso Seleccionar permisos:
   a. No seleccione **Permitir servicios de plataforma**.

      Normalmente, los inquilinos de FabricPool no necesitan usar servicios de plataforma, como la replicación de CloudMirror.

   b. Opcionalmente, selecciona **Usar fuente de identidad propia**.
   c. No seleccione **Permitir selección S3**.

      Los inquilinos de FabricPool no suelen utilizar S3 Select.

   d. Opcionalmente, seleccione **Usar conexión de federación de grid** para permitir que el inquilino utilice a. "conexión de federación de grid" para el clon de cuentas y la replicación entre grid. A continuación, seleccione la conexión de federación de cuadrícula que desea utilizar.
5. Para el paso Definir acceso root, especifique qué usuario tendrá el permiso de acceso root inicial para la cuenta de tenant, en función de si utiliza el sistema StorageGRID "federación de identidades", "Inicio de sesión único (SSO)", o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

6. Seleccione **Crear arrendatario**.

Cree un cubo S3 y obtenga claves de acceso

Antes de usar StorageGRID con una carga de trabajo de FabricPool, debe crear un bucket de S3 para sus datos de FabricPool. También debe obtener una clave de acceso y una clave de acceso secreta para la cuenta de inquilino que utilizará para FabricPool.

Para obtener más detalles sobre esta tarea, consulte "Crear bloque de S3" y.. "Cree sus propias claves de acceso S3". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Creó una cuenta de inquilino para uso de FabricPool.
- Tiene acceso raíz a la cuenta de inquilino.

Pasos

1. Inicie sesión en el Administrador de inquilinos.

   Puede realizar una de las siguientes acciones:

   - En la página Cuentas de arrendatarios de Grid Manager, seleccione el enlace **Iniciar sesión** para el arrendatario e introduzca sus credenciales.
   - Introduzca la URL para la cuenta de inquilino en un navegador web e introduzca sus credenciales.

2. Cree un bloque de S3 para datos de FabricPool.

   Debe crear un bloque único para cada clúster de ONTAP que vaya a utilizar.

   a. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
   b. Seleccione **Crear cucharón**.
   c. Introduzca el nombre del bucket de StorageGRID que desee usar con FabricPool. Por ejemplo: `fabricpool-bucket`.

      No puede cambiar el nombre del bloque después de crear el bloque.

   d. Seleccione la región para este segmento.

      De forma predeterminada, todos los bloques se crean en la `us-east-1` región.

   e. Seleccione **continuar**.
   f. Seleccione **Crear cucharón**.

      No seleccione **Activar control de versiones de objetos** para el depósito de FabricPool. Del mismo modo, no edite un depósito de FabricPool para usar **disponible** o un nivel de consistencia no predeterminado. El nivel de consistencia del cucharón recomendado para los depósitos de FabricPool es **Leer después de-nuevo-escribir**, que es la configuración predeterminada para un nuevo cucharón.

3. Cree una clave de acceso y una clave de acceso secreta.

   a. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.
   b. Seleccione **Crear clave**.
   c. Seleccione **Crear clave de acceso**.
   d. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de clave de acceso y la clave de acceso secreta.

      Estos valores se introducirán en ONTAP cuando configure StorageGRID como un nivel de cloud de FabricPool.

Si genera una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, introduzca las nuevas claves en ONTAP antes de eliminar los valores anteriores de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.

Configurar ILM para los datos de FabricPool

Puede usar esta política de ejemplo sencillo como punto de inicio para sus propias reglas y política de ILM.

Este ejemplo asume que está diseñando las reglas del ILM y una política de ILM para un sistema StorageGRID que tiene cuatro nodos de almacenamiento en un único centro de datos en Denver, Colorado. Los datos de FabricPool en este ejemplo utilizan un bloque llamado `fabricpool-bucket`.

Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas. Para obtener más información, consulte "Gestión de objetos con ILM".

Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool. Establezca el período de retención en **Forever** para asegurarse de que los objetos FabricPool no sean eliminados por StorageGRID ILM.

Antes de empezar

- Ha revisado el "Prácticas recomendadas para usar ILM con datos de FabricPool".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso de acceso de ILM o raíz.
- Si actualizó a StorageGRID 11,7 desde una versión anterior de StorageGRID, configuró el pool de almacenamiento que usará. En general, debe crear un pool de almacenamiento para cada sitio de StorageGRID.

Este requisito previo no se aplica a las nuevas instalaciones de StorageGRID 11,7. Cuando se instala StorageGRID 11,7 en un nuevo grid, se crean automáticamente pools de almacenamiento para cada sitio.

Pasos

1. Cree una regla de ILM que se aplique solo a los datos de `fabricpool-bucket`. En este ejemplo, se crean copias con código de borrado.

Definición de regla	Valor de ejemplo
Nombre de regla	Código de borrado 2 + 1 para datos de FabricPool
Nombre del bloque	`fabricpool-bucket` También puede filtrar en la cuenta de inquilino de FabricPool.

Definición de regla	Valor de ejemplo
Filtros avanzados	Tamaño de objeto superior a 0,2 MB. **Nota:** FabricPool solo escribe objetos de 4 MB, pero debe agregar un filtro de tamaño de objeto porque esta regla utiliza codificación de borrado.
Tiempo de referencia	Tiempo de ingesta
Período de tiempo y colocaciones	Desde la tienda del día 0 para siempre Almacene objetos mediante la codificación de borrado usando el esquema EC 2+1 en Denver y conserve esos objetos en StorageGRID para siempre. Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool.
Comportamiento de ingesta	Equilibrado

2. Cree una regla de ILM predeterminada que creará dos copias replicadas de todos los objetos que no coincidan con la primera regla. No seleccione un filtro básico (cuenta de inquilino o nombre de depósito) ni ningún filtro avanzado.

Definición de regla	Valor de ejemplo
Nombre de regla	Dos copias replicadas
Nombre del bloque	*none*
Filtros avanzados	*none*
Tiempo de referencia	Tiempo de ingesta
Período de tiempo y colocaciones	Desde la tienda del día 0 para siempre Almacene objetos replicando 2 copias en Denver.
Comportamiento de ingesta	Equilibrado

3. Cree una política de ILM propuesta y seleccione las dos reglas. Como la regla de replicación no utiliza ningún filtro, puede ser la regla predeterminada (última) de la directiva.
4. Ingesta de objetos de prueba en el grid.
5. Simule la directiva con los objetos de prueba para verificar el comportamiento.
6. Activar la política.

Cuando se activa esta política, StorageGRID coloca los datos de objetos de la siguiente manera:

- Los datos se organizan en niveles desde FabricPool en `fabricpool-bucket` se codificará mediante el esquema de codificación de borrado 2+1. Se colocarán dos fragmentos de datos y un fragmento de paridad en tres nodos de almacenamiento diferentes.
- Se replicarán todos los objetos de todos los demás bloques. Se crearán dos copias y se colocarán en dos nodos de almacenamiento diferentes.
- Las copias se mantendrán en StorageGRID para siempre. Gestión de la vida útil de la información de StorageGRID no eliminará estos objetos.

Cree una directiva de clasificación del tráfico para FabricPool

Opcionalmente, puede diseñar una normativa de clasificación del tráfico StorageGRID para optimizar la calidad del servicio para la carga de trabajo de FabricPool.

Para obtener más detalles sobre esta tarea, consulte "Administrar directivas de clasificación de tráfico". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el permiso acceso raíz.

Acerca de esta tarea

Las prácticas recomendadas para crear una política de clasificación del tráfico para FabricPool dependen de la carga de trabajo de la siguiente manera:

- Si planea organizar en niveles los datos de la carga de trabajo principal de FabricPool en StorageGRID, debe asegurarse de que la carga de trabajo de FabricPool tenga la mayor parte de ancho de banda. Puede crear una política de clasificación del tráfico para limitar el resto de cargas de trabajo.

  > En general, es más importante priorizar las operaciones de lectura de FabricPool que las operaciones de escritura.

  Por ejemplo, si otros clientes S3 utilizan este sistema StorageGRID, deberá crear una directiva de clasificación del tráfico. Puede limitar el tráfico de red para los demás bloques, inquilinos, subredes IP o puntos finales de equilibrador de carga.

*Por lo general, no debe imponer límites de calidad de servicio a ninguna carga de trabajo de FabricPool; solo debe limitar las demás cargas de trabajo.

- Los límites puestos en otras cargas de trabajo deben tener en cuenta el comportamiento de estas cargas de trabajo. Los límites impuestos también varían en función del tamaño y las funcionalidades de la cuadrícula y del grado de utilización previsto.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Introduzca un nombre y una descripción (opcional) para la política y seleccione **Continuar**.
4. Para el paso Agregar reglas coincidentes, agregue al menos una regla.

a. Seleccione **Añadir regla**

b. En Tipo, seleccione **Punto final de equilibrio de carga** y seleccione el punto final de equilibrio de carga que creó para FabricPool.

   También puede seleccionar la cuenta de inquilino o el bloque de FabricPool.

c. Si desea que esta política de tráfico limite el tráfico para los otros puntos finales, seleccione **Coincidencia inversa**.

5. Opcionalmente, agregue uno o más límites para controlar el tráfico de red que coincide con la regla.

   > StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias del tráfico.

   a. Selecciona **Añadir un límite**.

   b. Seleccione el tipo de tráfico que desea limitar y el límite que desea aplicar.

6. Seleccione **continuar**.

7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

Después de tu acabado

"Ver las métricas de tráfico de red" para verificar que las políticas están aplicando los límites de tráfico que espera.

Configure System Manager de ONTAP

Una vez que haya obtenido la información de StorageGRID necesaria, puede ir a ONTAP para añadir StorageGRID como nivel de cloud.

Antes de empezar

- Si completó el asistente de configuración de FabricPool, tiene el `ONTAP_FabricPool_settings_bucketname.txt` archivo descargado.
- Si configuró StorageGRID manualmente, tiene el nombre de dominio completo (FQDN) que utiliza para StorageGRID o la dirección IP virtual (VIP) para el grupo HA de StorageGRID, el número de puerto para el extremo del equilibrador de carga, el certificado del equilibrador de carga y el certificado del equilibrador de carga. El ID de clave de acceso y la clave secreta para el usuario raíz de la cuenta de inquilino, y el nombre de la ONTAP de bloque que usará en ese inquilino.

Acceda a Administrador del sistema de ONTAP

Estas instrucciones describen cómo usar el Administrador del sistema de ONTAP para añadir StorageGRID como nivel de cloud. Puede completar la misma configuración con la CLI de ONTAP. Para obtener instrucciones, vaya a. "ONTAP 9: Gestión de niveles de FabricPool con la interfaz de línea de comandos".

Pasos

1. Acceda a System Manager para el clúster ONTAP que desea organizar en niveles en StorageGRID.
2. Inicie sesión como administrador para el clúster.
3. Navegue hasta **STORAGE** > **Tiers** > **Add Cloud Tier**.
4. Seleccione **StorageGRID** de la lista de proveedores de almacenes de objetos.

Introduzca los valores de StorageGRID

Consulte "ONTAP 9: Información general de gestión de niveles de FabricPool con System Manager" si quiere más información.

Pasos

1. Complete el formulario Agregar nivel de nube, mediante `ONTAP_FabricPool_settings _bucketname.txt` archivo o los valores obtenidos manualmente.

Campo	Descripción
Nombre	Introduzca un nombre único para este nivel de cloud. Puede aceptar el valor predeterminado.
Estilo de URL	Si usted "Nombres de dominio de punto final S3 configurados", Seleccione **Virtual Hosted-Style URL**. **URL de estilo de ruta** es el valor predeterminado para ONTAP, pero se recomienda usar solicitudes de estilo hospedado virtual para StorageGRID. Debe usar **URL de estilo de ruta** si proporciona una dirección IP en lugar de un nombre de dominio para el campo **Nombre de servidor (FQDN)**.
Nombre del servidor (FQDN)	Introduzca el nombre de dominio completo (FQDN) que utiliza para StorageGRID o la dirección IP virtual (VIP) del grupo de alta disponibilidad de StorageGRID. Por ejemplo: `s3.storagegrid.company.com`. Tenga en cuenta lo siguiente: • La dirección IP o el nombre de dominio que especifique aquí deben coincidir con el certificado que haya cargado o generado para el punto final del equilibrador de carga de StorageGRID. • Si proporciona un nombre de dominio, el registro DNS debe asignar a cada dirección IP que utilizará para conectarse a StorageGRID. Consulte "Configure el servidor DNS".
SSL	Activado (predeterminado).
Certificado de almacén de objetos	Pegue el PEM del certificado que está utilizando para el punto final del equilibrador de carga de StorageGRID, que incluye: `-----BEGIN CERTIFICATE-----` y.. `-----END CERTIFICATE-----`. **Nota:** 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.
Puerto	Introduzca el puerto utilizado por el punto final del equilibrador de carga de StorageGRID. ONTAP utilizará este puerto cuando se conecte a StorageGRID. Por ejemplo, 10433.

Campo	Descripción
Clave de acceso y clave secreta	Introduzca el ID de clave de acceso y la clave de acceso secreta para el usuario raíz de la cuenta de inquilino de StorageGRID. **Consejo**: Si generas una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, introduce las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.
Nombre del contenedor	Introduzca el nombre del bucket de StorageGRID que ha creado para su uso con este nivel de ONTAP.

2. Complete la configuración final de FabricPool en ONTAP.
   a. Adjunte uno o más agregados al nivel de cloud.
   b. Opcionalmente, cree una política de organización en niveles de volúmenes.

Configure el servidor DNS

Después de configurar grupos de alta disponibilidad, puntos finales de equilibrio de carga y nombres de dominio de punto final S3, debe asegurarse de que el DNS incluya las entradas necesarias para StorageGRID. Debe incluir una entrada DNS para cada nombre del certificado de seguridad y para cada dirección IP que pueda utilizar.

Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Entradas DNS para el nombre del servidor StorageGRID

Agregue entradas DNS para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilice. Las direcciones IP que introduzca en el DNS dependen de si va a utilizar un grupo de alta disponibilidad de nodos de equilibrio de carga:

- Si ha configurado un grupo de alta disponibilidad, ONTAP se conectará a las direcciones IP virtuales de dicho grupo de alta disponibilidad.
- Si no está utilizando un grupo de alta disponibilidad, ONTAP puede conectarse al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de cualquier nodo de puerta de enlace o nodo de administración.
- Si el nombre del servidor resuelve más de una dirección IP, ONTAP establece conexiones de cliente con todas las direcciones IP (hasta un máximo de 16 direcciones IP). Las direcciones IP se recogen en un método round-robin cuando se establecen conexiones.

Entradas DNS para solicitudes virtuales de estilo alojado

Si ha definido "Nombres de dominio de punto final S3" Y utilizará solicitudes virtuales de estilo hospedado, agregue entradas DNS para todos los nombres de dominio de punto final S3 necesarios, incluidos los nombres de comodín.

Prácticas recomendadas de StorageGRID para FabricPool

Prácticas recomendadas para grupos de alta disponibilidad

Antes de asociar StorageGRID como nivel de cloud de FabricPool, conozca los grupos de alta disponibilidad de StorageGRID y revise las prácticas recomendadas para usar grupos de alta disponibilidad con FabricPool.

¿Qué es un grupo de alta disponibilidad?

Un grupo de alta disponibilidad es una colección de interfaces de varios nodos de puerta de enlace StorageGRID, nodos de administración o ambos. Un grupo de alta disponibilidad ayuda a mantener la disponibilidad de las conexiones de datos de cliente. Si falla la interfaz activa del grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Cada grupo de alta disponibilidad proporciona acceso de alta disponibilidad a los servicios compartidos en los nodos asociados. Por ejemplo, un grupo de alta disponibilidad que consta de interfaces solo en los nodos de puerta de enlace o en los nodos de administración y de puerta de enlace proporciona un acceso de alta disponibilidad al servicio de equilibrador de carga compartido.

Para obtener más información sobre los grupos de alta disponibilidad, consulte "Gestione grupos de alta disponibilidad".

Usando grupos de alta disponibilidad

Las mejores prácticas para crear un grupo de alta disponibilidad de StorageGRID para FabricPool dependen de la carga de trabajo.

- Si piensa utilizar FabricPool con datos de carga de trabajo principal, debe crear un grupo de alta disponibilidad que incluya al menos dos nodos de equilibrio de carga para evitar la interrupción de la recuperación de datos.
- Si planea utilizar la política de organización en niveles de volúmenes sólo para snapshots de FabricPool o los niveles de rendimiento locales no primarios (por ejemplo, ubicaciones de recuperación ante desastres o destinos de SnapMirror® de NetApp), puede configurar un grupo ha con sólo un nodo.

Estas instrucciones describen cómo configurar un grupo de alta disponibilidad para la alta disponibilidad de Active-Backup (un nodo es activo y uno es backup). Sin embargo, puede que prefiera usar DNS Round Robin o ha activo-activo. Para conocer las ventajas de estas otras configuraciones de alta disponibilidad, consulte "Opciones de configuración para grupos de alta disponibilidad".

Prácticas recomendadas para el equilibrio de carga para FabricPool

Antes de asociar StorageGRID como nivel de cloud de FabricPool, revise las prácticas recomendadas para usar balanceadores de carga con FabricPool.

Para obtener información general sobre el equilibrador de carga StorageGRID y el certificado del equilibrador de carga, consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Prácticas recomendadas para el acceso de inquilinos al extremo del balanceador de carga utilizado para FabricPool

Puede controlar qué inquilinos pueden utilizar un extremo de balanceador de carga específico para acceder a sus bloques. Puede permitir a todos los inquilinos, permitir algunos inquilinos o bloquear algunos inquilinos. Al crear un punto final de equilibrio de carga para el uso de FabricPool, seleccione **Permitir todos los inquilinos**. ONTAP cifra los datos que se almacenan en buckets de StorageGRID, por lo que esta capa de seguridad adicional ofrece poca seguridad adicional.

Prácticas recomendadas para el certificado de seguridad

Cuando se crea un punto final de equilibrio de carga de StorageGRID para uso de FabricPool, se proporciona el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

En la mayoría de los casos, la conexión entre ONTAP y StorageGRID debe utilizar cifrado de seguridad de la capa de transporte (TLS). Pero no es recomendable utilizar FabricPool sin el cifrado TLS. Cuando seleccione el protocolo de red para el punto final del equilibrador de carga StorageGRID, seleccione **HTTPS**. A continuación, proporcione el certificado de seguridad que permitirá la autenticación de ONTAP con StorageGRID.

Para obtener más información acerca del certificado de servidor para un extremo de equilibrio de carga:

- "Gestionar certificados de seguridad"
- "Consideraciones que tener en cuenta al equilibrio de carga"
- "Directrices de refuerzo para certificados de servidor"

Agregar certificado a ONTAP

Al añadir StorageGRID como nivel cloud de FabricPool, debe instalar el mismo certificado en el clúster de ONTAP, incluidos los certificados raíz y todos los certificados de entidad de certificación (CA) subordinados.

Gestionar el vencimiento del certificado

> Si el certificado utilizado para proteger la conexión entre ONTAP y StorageGRID caduca, FabricPool dejará de funcionar temporalmente y ONTAP perderá temporalmente el acceso a los datos almacenados en niveles en StorageGRID.

Para evitar problemas de caducidad de certificados, siga las siguientes prácticas recomendadas:

- Monitoree cuidadosamente cualquier alerta que advierta de fechas de vencimiento de certificados que se acercan, como el **Caducidad del certificado de punto final del equilibrador de carga** y **Caducidad del certificado de servidor global para las alertas S3 y Swift API**.
- Mantenga siempre sincronizadas las versiones de StorageGRID y ONTAP del certificado. Si reemplaza o renueva el certificado utilizado para un extremo de balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por ONTAP para el nivel de cloud.
- Utilice un certificado de CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede usar la API de gestión de grid para automatizar la rotación de certificados. Esto permite sustituir certificados que pronto caducan de forma no disruptiva.
- Si generó un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe sustituir manualmente el certificado tanto en StorageGRID como en ONTAP antes de que caduque el certificado existente. Si ya ha caducado un certificado autofirmado, desactive la validación de certificados en ONTAP para evitar la pérdida de acceso.

  Consulte "Base de conocimientos de NetApp: Cómo configurar un certificado de servidor autofirmado de StorageGRID en una implementación existente de ONTAP FabricPool" si desea obtener instrucciones.

Prácticas recomendadas para usar ILM con datos de FabricPool

Si utiliza FabricPool para organizar los datos en niveles en StorageGRID, debe conocer los requisitos para usar la gestión de la vida útil de la información (ILM) de StorageGRID

con los datos de FabricPool.

> FabricPool no conoce las reglas ni las políticas de ILM de StorageGRID. Se pueden perder datos si la política de ILM de StorageGRID está mal configurada. Para obtener información detallada, consulte "Cree una regla de ILM: Información general" y.. "Cree una política de ILM: Información general".

Directrices para utilizar ILM con FabricPool

Cuando utiliza el asistente de configuración de FabricPool, el asistente crea automáticamente una nueva regla de ILM para cada bloque de S3 que cree, añade esa regla a una política propuesta y le solicita que active la nueva política como parte de la finalización del asistente. La regla creada automáticamente sigue las mejores prácticas recomendadas: Utiliza código de borrado 2+1 en un solo sitio.

Si configura StorageGRID manualmente en lugar de usar el asistente de configuración de FabricPool, revise estas directrices para asegurarse de que las reglas de ILM y la política de ILM sean adecuados para los datos de FabricPool y los requisitos del negocio. Es posible que deba crear nuevas reglas y actualizar la política de ILM activa para cumplir estas directrices.

- Puede utilizar cualquier combinación de reglas de replicación y codificación de borrado para proteger los datos de nivel de cloud.

  La mejor práctica recomendada es utilizar códigos de borrado 2+1 dentro de las instalaciones para una protección de datos rentable. La codificación de borrado utiliza más CPU, pero ofrece mucha menos capacidad de almacenamiento que la replicación. Los esquemas 4+1 y 6+1 utilizan menos capacidad que el esquema 2+1. Sin embargo, los esquemas 4+1 y 6+1 son menos flexibles si necesita agregar nodos de almacenamiento durante la expansión de la cuadrícula. Para obtener más información, consulte "Añada capacidad de almacenamiento para objetos codificados de borrado".

- Cada regla se aplica a los datos FabricPool debe utilizar código de borrado o bien crear al menos dos copias replicadas.

  > Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

- Si lo necesita "Eliminar datos de FabricPool de StorageGRID", Use ONTAP para recuperar todos los datos del volumen FabricPool y promocionarlo al nivel de rendimiento.

  > Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool. Establezca el período de retención en cada regla de gestión de la vida útil de la información en **forever** para asegurarse de que los objetos de FabricPool no se eliminen mediante gestión de la vida útil de la información de StorageGRID.

- No cree reglas que trasladarán los datos de nivel del cloud de FabricPool fuera del bloque a otra ubicación. No se puede usar un Pool de almacenamiento en cloud para mover datos de FabricPool a otro almacén de objetos. De forma similar, no es posible archivar datos FabricPool en cinta utilizando un nodo de archivado.

No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.

- A partir de ONTAP 9.8, puede crear opcionalmente etiquetas de objeto, con el fin de clasificar y ordenar los datos por niveles para simplificar la gestión. Por ejemplo, puede establecer solo etiquetas en los volúmenes de FabricPool conectados a StorageGRID. A continuación, cuando cree reglas de ILM en StorageGRID, puede utilizar el filtro avanzado etiqueta de objeto para seleccionar y colocar estos datos.

Otras prácticas recomendadas para StorageGRID y FabricPool

Al configurar un sistema StorageGRID para utilizarlo con FabricPool, es posible que deba cambiar otras opciones de StorageGRID. Antes de cambiar una configuración global, considere cómo afectará el cambio a otras aplicaciones S3.

Destinos de registro y mensajes de auditoría

Las cargas de trabajo de FabricPool suelen tener una tasa alta de operaciones de lectura, las que pueden generar un alto volumen de mensajes de auditoría.

- Si no necesita un registro de operaciones de lectura de cliente para FabricPool o cualquier otra aplicación S3, vaya opcionalmente a **CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**. Cambie la configuración de **Lecturas de cliente** a **Error** para disminuir el número de mensajes de auditoría registrados en el registro de auditoría. Consulte "Configurar los mensajes de auditoría y los destinos de registro" para obtener más detalles.
- Si tiene un grid grande, utilice varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría, configure un servidor syslog externo y guarde la información de auditoría de forma remota. El uso de un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la integridad de los datos de auditoría. Consulte "Consideraciones sobre el servidor de syslog externo" para obtener más detalles.

Cifrado de objetos

Al configurar StorageGRID, también puede habilitar el "opción global para el cifrado de objetos almacenados" Si se requiere cifrado de datos para otros clientes StorageGRID. Los datos organizados en niveles desde FabricPool a StorageGRID ya están cifrados, por lo que no es necesario habilitar la configuración de StorageGRID. Las claves de cifrado en el cliente son propiedad de ONTAP.

Compresión de objetos

Al configurar StorageGRID, no habilite el "opción global para comprimir objetos almacenados". Los datos que se organizan en niveles de FabricPool a StorageGRID ya están comprimidos. El uso de la opción StorageGRID no reducirá más el tamaño de un objeto.

Nivel de coherencia del cucharón

Para los depósitos FabricPool, el nivel de consistencia del cucharón recomendado es **Leer-después-nuevo-escribir**, que es la configuración predeterminada para un nuevo cucharón. No edite los depósitos de FabricPool para usar **Disponible** o cualquier otro nivel de consistencia.

Organización en niveles de FabricPool

Si un nodo de StorageGRID utiliza almacenamiento asignado desde un sistema ONTAP de NetApp, confirme que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Por ejemplo, si un

nodo StorageGRID se ejecuta en un host VMware, asegúrese de que el volumen que realiza el backup del almacén de datos para el nodo StorageGRID no tenga habilitada una política de organización en niveles de FabricPool. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Eliminar datos de FabricPool de StorageGRID

Si necesita eliminar los datos de FabricPool almacenados actualmente en StorageGRID, deberá usar ONTAP para recuperar todos los datos del volumen de FabricPool y promoverlos al nivel de rendimiento.

Antes de empezar

- Ha revisado las instrucciones y consideraciones de "Promocione los datos al nivel de rendimiento".
- Utiliza ONTAP 9,8 o posterior.
- Está utilizando un "navegador web compatible".
- Pertenece a un grupo de usuarios de StorageGRID de la cuenta de inquilino de FabricPool que tiene el "Gestione todos los bloques o permisos de acceso raíz".

Acerca de esta tarea

En estas instrucciones, se explica cómo mover los datos de StorageGRID a FabricPool. Realice este procedimiento con ONTAP y el Administrador de inquilinos de StorageGRID.

Pasos

1. Desde ONTAP, emita el `volume modify` comando.

   Configurado `tiering-policy` para `none` para detener y establecer una nueva organización en niveles `cloud-retrieval-policy` para `promote` Para devolver todos los datos que anteriormente se organizaban en niveles en StorageGRID.

   Consulte "Promocione todos los datos de un volumen de FabricPool al nivel de rendimiento".

2. Espere a que se complete la operación.

   Puede utilizar el `volume object-store` con el `tiering` opción a. "compruebe el estado del ascenso de nivel de rendimiento".

3. Una vez finalizada la operación de promoción, inicie sesión en el Administrador de inquilinos de StorageGRID para la cuenta de inquilino de FabricPool.
4. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
5. Confirme que el bloque de FabricPool está vacío.
6. Si el cucharón está vacío, "elimine el cucharón".

Después de terminar

Al eliminar el bloque, la organización en niveles desde FabricPool hasta StorageGRID ya no puede continuar. Sin embargo, como el nivel local todavía está conectado a la capa de cloud de StorageGRID, System

Manager de ONTAP devolverá mensajes de error que indican que no se puede acceder al bloque.

Para evitar estos mensajes de error, realice una de las siguientes acciones:

- Utilice FabricPool Mirror para adjuntar un nivel de cloud diferente al agregado.
- Mueva los datos del agregado de FabricPool a un agregado no compatible con FabricPool y, a continuación, elimine el agregado no utilizado.

Consulte "Documentación de ONTAP para FabricPool" si desea obtener instrucciones.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.