Usar una cuenta de inquilino

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Usar una cuenta de inquilino 1
Uso del Administrador de arrendatarios 1
Gestión del acceso al sistema para usuarios de inquilinos 15
Gestión de cuentas de inquilinos de S3 37
Gestión de servicios de plataforma S3 66

Usar una cuenta de inquilino

Aprenda a usar una cuenta de inquilino de StorageGRID.

- "Uso del Administrador de arrendatarios"
- "Gestión del acceso al sistema para usuarios de inquilinos"
- "Gestión de cuentas de inquilinos de S3"
- "Gestión de servicios de plataforma S3"

Uso del Administrador de arrendatarios

El Administrador de inquilinos le permite gestionar todos los aspectos de una cuenta de inquilino de StorageGRID.

Puede usar el Administrador de inquilinos para supervisar el uso del almacenamiento de una cuenta de inquilino y para gestionar los usuarios con federación de identidades o creando grupos y usuarios locales. En las cuentas de inquilinos S3, también se pueden gestionar claves S3, gestionar bloques S3 y configurar servicios de plataforma.

Usar una cuenta de inquilino de StorageGRID

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 sus propios grupos locales o federados, usuarios, bloques S3 o contenedores Swift, y objetos.

Opcionalmente, las cuentas de arrendatarios 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 el sistema StorageGRID se está utilizando dentro de una empresa, el almacenamiento de objetos de la cuadrícula puede estar segregado por los diferentes departamentos de la organización. Por ejemplo, puede haber cuentas de inquilino para el departamento de marketing, el departamento de soporte al cliente, el departamento de recursos humanos, etc.

  > Si utiliza el protocolo cliente S3, también puede utilizar bloques S3 y políticas de bucket para separar objetos entre los departamentos de una empresa. No es necesario crear cuentas de arrendatario independientes. Consulte instrucciones para implementar aplicaciones cliente S3.

- **Caso de uso del proveedor de servicios:** Si un proveedor de servicios utiliza el sistema StorageGRID, el almacenamiento de objetos de la cuadrícula puede estar segregado por las diferentes entidades que arriendan el almacenamiento. Por ejemplo, puede que haya cuentas de inquilino para la empresa A, la empresa B, la empresa C, etc.

Creación de cuentas de inquilino

Las cuentas de inquilino las crea un administrador de grid de StorageGRID mediante Grid Manager. Al crear una cuenta de inquilino, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del arrendatario (el ID de cuenta del arrendatario se asigna automáticamente y no se puede modificar).
- Si la cuenta de inquilino usa S3 o Swift.
- Para las cuentas de inquilino de S3: Si la cuenta de inquilino está permitida para usar los servicios de la plataforma. Si se permite el uso de servicios de plataforma, la cuadrícula debe configurarse para que admita su uso.
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).
- Si está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

Además, los administradores de grid pueden habilitar la configuración de bloqueo de objetos de S3 para el sistema StorageGRID si las cuentas de inquilinos 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.

Configuración de inquilinos de S3

Después de crear una cuenta de inquilino de S3, puede acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) o crear grupos y usuarios locales
- Gestión de claves de acceso de S3
- Creación y gestión de bloques de S3, incluidos los bloques conformes a la normativa
- Uso de servicios de plataforma (si está activado)
- Supervisión del uso de almacenamiento

> Aunque puede crear y gestionar bloques de S3 con el administrador de inquilinos, debe tener claves de acceso de S3 y usar la API REST de S3 para procesar y gestionar objetos.

Configurar inquilinos Swift

Después de crear una cuenta de inquilino de Swift, los usuarios con permiso de acceso raíz pueden acceder al Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de almacenamiento

> Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Información relacionada

"Administre StorageGRID"

"Use S3"

"Use Swift"

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Debe establecer la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Iniciando sesión en el Administrador de arrendatarios

Para acceder al Administrador de inquilinos, introduzca la URL del inquilino en la barra de direcciones de un navegador web compatible.

Lo que necesitará

- Debe tener sus credenciales de inicio de sesión.
- Debe tener una dirección URL para acceder al Administrador de inquilinos, tal y como le ha suministrado el administrador de grid. La dirección URL tendrá el aspecto de uno de estos ejemplos:

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

La URL siempre contiene el nombre de dominio completo (FQDN) o la dirección IP utilizada para acceder a un nodo de administrador, y también puede incluir, de manera opcional, un número de puerto, el ID de cuenta de inquilino de 20 dígitos o ambos.

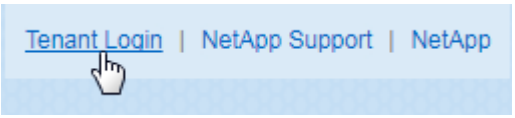
- Si la URL no incluye el ID de cuenta de 20 dígitos del inquilino, debe tener este ID de cuenta.
- Debe utilizar un navegador web compatible.
- Las cookies deben estar habilitadas en su navegador web.
- Debe tener permisos de acceso específicos.

Pasos

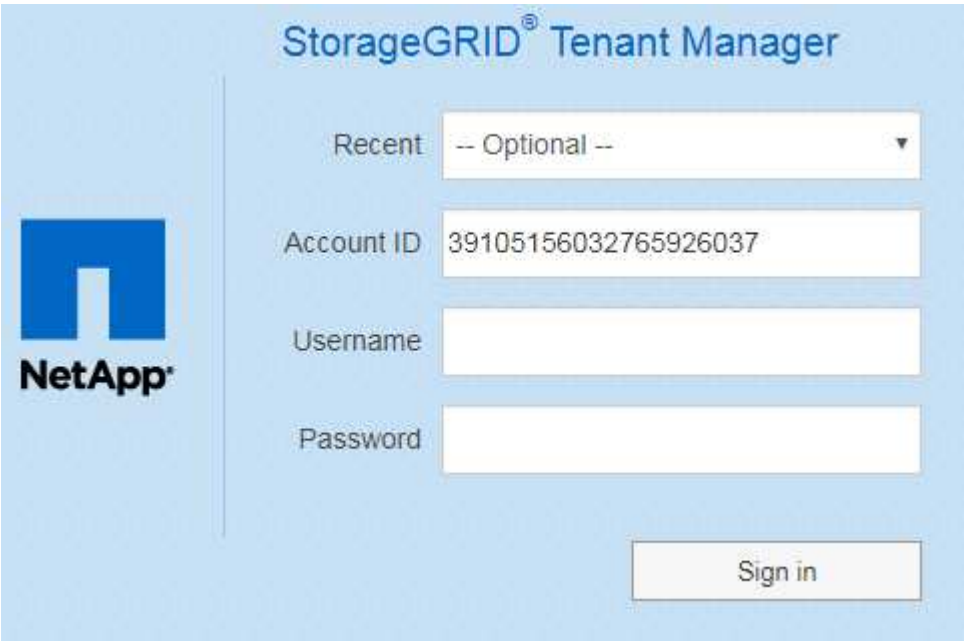
1. Inicie un explorador web compatible.
2. En la barra de dirección del navegador, introduzca la URL para acceder al Administrador de inquilinos.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
4. Inicie sesión en el Administrador de inquilinos.

   La pantalla de inicio de sesión que ve depende de la dirección URL introducida y de si su empresa utiliza el inicio de sesión único (SSO). Verá una de las siguientes pantallas:

   - La página de inicio de sesión de Grid Manager. Haga clic en el enlace **Ingreso de inquilino** de la parte superior derecha.

   - La página de inicio de sesión del administrador de inquilinos. Es posible que el campo **ID de cuenta** ya esté completo, como se muestra a continuación.

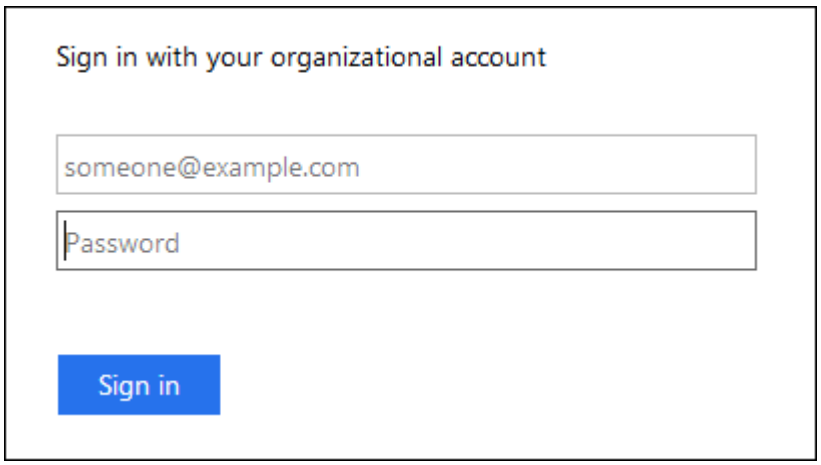
i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.

ii. Introduzca su nombre de usuario y contraseña.

iii. Haga clic en **Iniciar sesión**.

Aparecerá la consola del administrador de inquilinos.

- Si el inicio de sesión único de su organización está habilitado en el grid. Por ejemplo:



Introduzca sus credenciales de SSO estándar y haga clic en **Iniciar sesión**.

- La página de inicio de sesión SSO de inquilino Manager.

i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.

ii. Haga clic en **Iniciar sesión**.

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

Aparecerá la consola del administrador de inquilinos.

5. Si ha recibido una contraseña inicial de otra persona, cambie la contraseña para proteger su cuenta. Seleccione ***username*** > **Change Password**.

Si SSO está habilitado para el sistema StorageGRID, no puede cambiar la contraseña del administrador de inquilinos.

Información relacionada

"Administre StorageGRID"

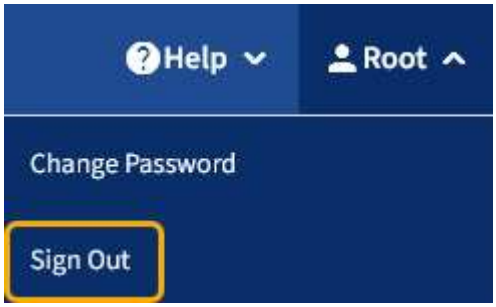
"Requisitos del navegador web"

Cierre de sesión en el Administrador de arrendatarios

Una vez que haya terminado de trabajar con el Administrador de inquilinos, debe cerrar sesión para garantizar que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

Pasos

1. Busque el menú desplegable username en la esquina superior derecha de la interfaz de usuario.



2. Seleccione el nombre de usuario y, a continuación, seleccione **Cerrar sesión**.

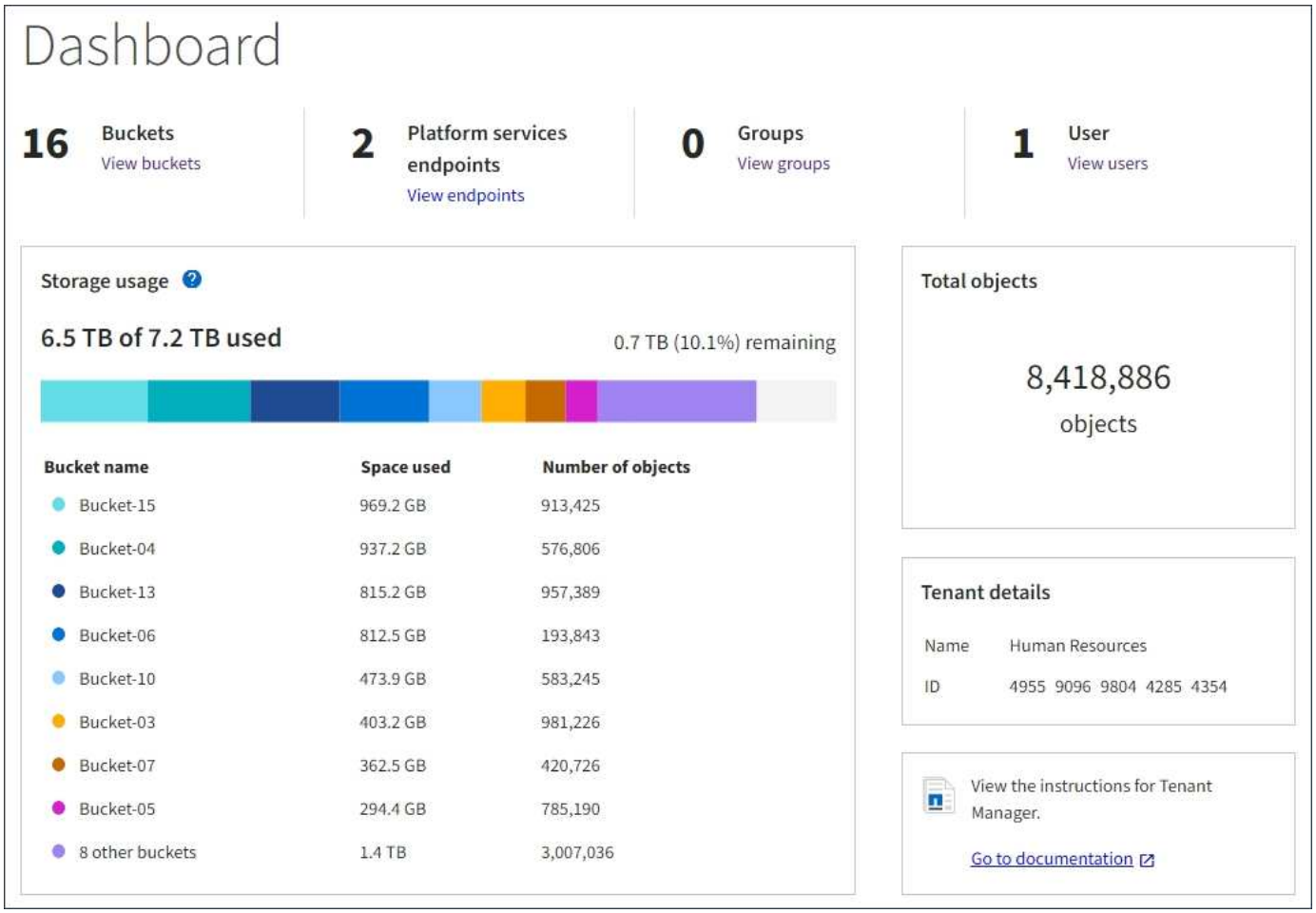
Opción	Descripción
SSO no en uso	Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión del administrador de inquilinos. **Nota:** Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo.
SSO habilitado	Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página Inicio de sesión de StorageGRID. El nombre de la cuenta de arrendatario a la que acaba de acceder aparece como el valor predeterminado en el menú desplegable **Cuentas recientes**, y se muestra el **ID de cuenta** del arrendatario. **Nota:** Si está activado SSO y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Consola del administrador de inquilinos

La consola de tenant Manager proporciona una información general de la configuración de una cuenta de inquilino y la cantidad de espacio utilizado por los objetos en los bloques de inquilino (S3) o contenedores (Swift). Si el cliente tiene una cuota, en Dashboard se muestra cuánto de la cuota se usa y cuánto queda. Si hay algún error relacionado con la cuenta de inquilino, los errores se muestran en la consola.

> Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo.

Cuando se cargan objetos, la consola se parece al siguiente ejemplo:



Resumen de la cuenta de inquilino

La parte superior de la consola contiene la siguiente información:

- El número de bloques o contenedores, grupos y usuarios configurados
- El número de extremos de servicios de plataforma, si se han configurado alguno

Puede seleccionar los enlaces para ver los detalles.

La parte derecha de la consola contiene la siguiente información:

- Número total de objetos para el arrendatario.

  Para una cuenta de S3, si no se han ingerido objetos y tiene el permiso de acceso raíz, se muestran las directrices de introducción en lugar del número total de objetos.

- El nombre de la cuenta de inquilino y su ID.
- Un enlace a la documentación de StorageGRID.

Aprovechamiento del almacenamiento y de la cuota

El panel uso del almacenamiento contiene la siguiente información:

- La cantidad de datos de objeto para el inquilino.

  Este valor indica la cantidad total de datos de objeto cargados y no representa el espacio utilizado para almacenar copias de esos objetos y sus metadatos.

- Si se establece una cuota, la cantidad total de espacio disponible para los datos del objeto y la cantidad y el porcentaje de espacio restante. La cuota limita la cantidad de datos de objetos que se pueden procesar.

  La utilización de cuotas se basa en estimaciones internas y puede superarse en algunos casos. Por ejemplo, StorageGRID comprueba la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas búsquedas si el inquilino ha superado la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha superado la cuota. Si se eliminan objetos, es posible que se impida temporalmente que un arrendatario cargue nuevos objetos hasta que se vuelva a calcular la utilización de cuota. El cálculo de la utilización de cuotas puede tardar 10 minutos o más.

- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes.

  Puede colocar el cursor sobre cualquiera de los segmentos del gráfico para ver el espacio total consumido por ese cucharón o contenedor.

- Para corresponder con el gráfico de barras, una lista de los cubos o contenedores más grandes, incluida la cantidad total de datos de objeto y el número de objetos de cada cucharón o contenedor.

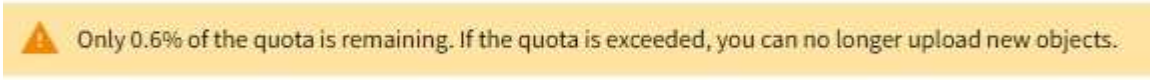
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

Si el inquilino tiene más de nueve cubos o contenedores, el resto de cubos o contenedores se combinan en una sola entrada al final de la lista.

Alertas de uso de cuotas

Si se han habilitado alertas de uso de cuota en Grid Manager, aparecerán en el Gestor de arrendatarios cuando la cuota sea baja o excedida, de la siguiente manera:

Si se ha utilizado un 90% o más de la cuota de un inquilino, se activa la alerta **uso de cuota de inquilino alto**. Para obtener más información, consulte la referencia de alertas en las instrucciones para supervisar y solucionar problemas de StorageGRID.

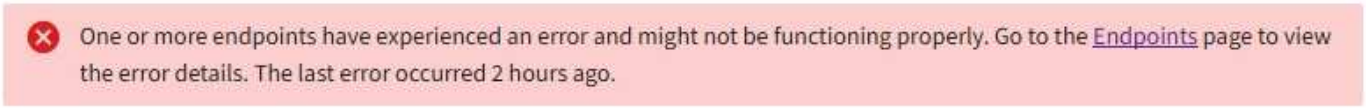


Si supera la cuota, no podrá cargar nuevos objetos.

Para ver detalles adicionales y gestionar reglas y notificaciones para alertas, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.

Errores de punto final

Si ha utilizado Grid Manager para configurar uno o más extremos para utilizarlos con los servicios de la plataforma, el Panel de arrendatarios muestra una alerta si se han producido errores en los últimos siete días.



Para ver detalles sobre un error de punto final, seleccione endpoints para mostrar la página endpoints.

Información relacionada

"Resolución de problemas de errores de extremos de servicios de plataforma"

"Solución de problemas de monitor"

API de gestión de inquilinos

Puede realizar tareas de administración del sistema mediante la API REST de gestión de inquilinos en lugar de la interfaz de usuario de inquilino Manager. Por ejemplo, se recomienda utilizar la API para automatizar operaciones o crear varias entidades, como los usuarios, más rápidamente.

La API de gestión de inquilinos utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores interactuar con la API. La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

Para acceder a la documentación de Swagger para la API de gestión de inquilinos:

Pasos

1. Inicie sesión en el Administrador de inquilinos.
2. Seleccione **Ayuda** > **Documentación de API** en el encabezado Administrador de inquilinos.

Operaciones de API

La API de gestión de inquilinos organiza las operaciones de API disponibles en las siguientes secciones:

- **Cuenta** — Operaciones en la cuenta de arrendatario actual, incluyendo la obtención de información de uso de almacenamiento.
- **Auth** — Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de arrendatarios admite el esquema de autenticación de token Bearer. Para el inicio de sesión de un inquilino, debe proporcionar un nombre de usuario, una contraseña y un ID de cuenta 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 posteriores solicitudes de API ("autorización: Token del portador").

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

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

- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API de Gestión de

arrendatarios. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.

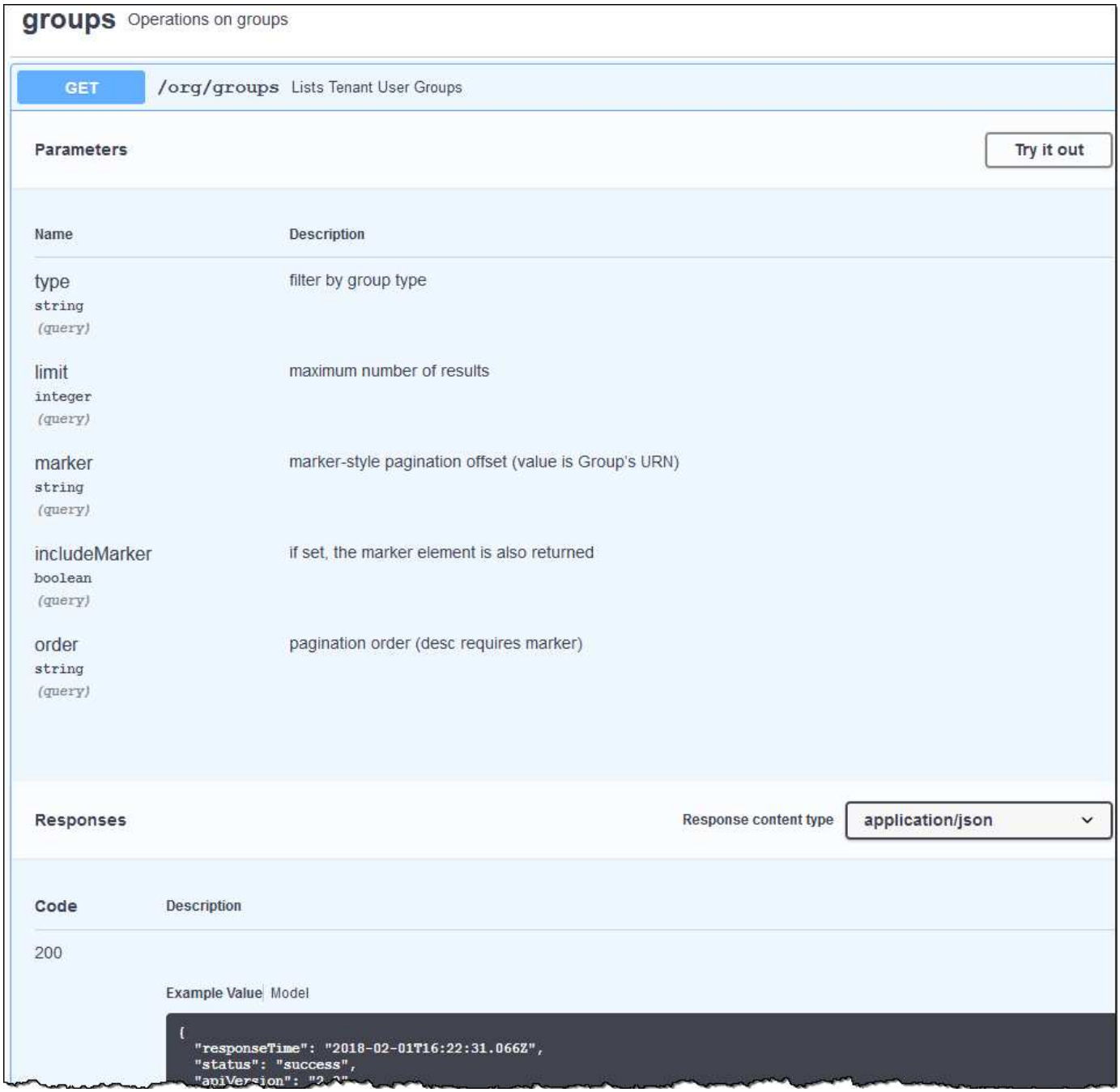
- **Containers** — Operaciones en bloques de S3 o contenedores Swift, como se indica a continuación:

Protocolo	Permiso lo permite
S3	• Creación de cucharones que cumplen las normativas y no cumplen las normativas • Modificación de la configuración de conformidad heredada • Configurar el control de coherencia para las operaciones realizadas en objetos • Creación, actualización y eliminación de la configuración de CORS de un bloque • Habilitar y deshabilitar las actualizaciones de la última hora de acceso para los objetos • Gestionar la configuración de los servicios de plataforma, incluida la replicación de CloudMirror, las notificaciones y la integración de búsqueda (metadatos-notification) • Eliminación de cucharones vacíos
Swift	Configurar el nivel de coherencia utilizado para contenedores

- **Características desactivadas** — Operaciones para ver las funciones que podrían haberse desactivado.
- **Endpoints** — Operaciones para administrar un punto final. Los extremos permiten que un bloque de S3 use un servicio externo para la replicación de CloudMirror de StorageGRID, notificaciones o integración de búsqueda.
- **Grupos** — Operaciones para administrar grupos de inquilinos locales y recuperar grupos de inquilinos federados de un origen de identidades externo.
- **Identity-source** — Operaciones para configurar un origen de identidad externo y sincronizar manualmente la información del grupo federado y del usuario.
- **Regiones** — Operaciones para determinar qué regiones se han configurado para el sistema StorageGRID.
- **s3** — Operaciones para administrar claves de acceso S3 para usuarios inquilinos.
- **s3-object-lock** — Operaciones para determinar cómo se configura el bloqueo global de objetos (cumplimiento) de S3 para el sistema StorageGRID.
- **Usuarios** — Operaciones para ver y administrar usuarios de arrendatarios.

Detalles de la operación

Al expandir cada operación de API, puede ver su acción HTTP, su URL de extremo, una lista de cualquier parámetro requerido o opcional, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



Emitir solicitudes API

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. Haga clic en la acción HTTP para ver los detalles de la solicitud.
2. 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.
3. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede hacer clic en **Modelo** para conocer los requisitos de cada campo.

4. Haga clic en **probar**.
5. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
6. Haga clic en **Ejecutar**.
7. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Información relacionada

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

"Administre StorageGRID"

Creación de versiones de la API de gestión de inquilinos

La API de gestión de inquilinos utiliza versiones para dar cabida a actualizaciones no disruptivas.

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

Cuando el software StorageGRID se instala por primera vez, solo se habilita la versión más reciente de la API de gestión de inquilinos. Sin embargo, cuando StorageGRID se actualiza a una versión de función nueva, sigue teniendo acceso a la versión de API anterior para al menos una versión de la función StorageGRID.

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

Determinar qué versiones de API son compatibles con la versión actual

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

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

Especificar una versión de API para una solicitud

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

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

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

Protección contra falsificación de solicitudes entre sitios (CSRF)

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

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

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

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

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

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

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

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

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

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

Gestión del acceso al sistema para usuarios de inquilinos

Permite a los usuarios acceder a una cuenta de inquilino mediante la importación de grupos desde un origen de identidad federado y la asignación de permisos de administración. También puede crear usuarios y grupos de inquilinos locales, a menos que el inicio de sesión único (SSO) esté vigente para todo el sistema StorageGRID.

- "Mediante la federación de identidades"
- "Gestión de grupos"
- "Gestión de usuarios locales"

Mediante la federación de identidades

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

- "Configurar un origen de identidad federado"
- "Forzar la sincronización con el origen de identidades"
- "Desactivar la federación de identidades"

Configurar un origen de identidad federado

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe utilizar Active Directory, OpenLDAP o Oracle Directory Server como proveedor de identidades. Si desea utilizar un servicio LDAP v3 que no esté en la lista, debe ponerse en contacto con el soporte técnico.
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3.

Acerca de esta tarea

Si puede configurar un servicio de federación de identidades para su inquilino depende de cómo se haya configurado su cuenta de inquilino. Es posible que el inquilino comparta el servicio de federación de identidades configurado para Grid Manager. Si ve este mensaje al acceder a la página Federación de identidades, no podrá configurar un origen de identidad federado independiente para este arrendatario.

> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione **Active Directory**, **OpenLDAP** o **otros**.

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

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

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP .
   - **Nombre único de usuario**: Nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `uid` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `uid`.
   - **UUID de usuario**: Nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único del grupo**: Nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `cn` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `cn`.
   - **UUID de grupo**: Nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para

OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.

5. En la sección Configure LDAP Server, introduzca la información sobre el servidor LDAP y las conexiones de red necesarias.
   - **Hostname**: El nombre de host del servidor o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP. El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.
   - **Nombre de usuario**: La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP. Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

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

     - `sAMAccountName` o. `uid`
     - `objectGUID`, `entryUUID`, o. `nsuniqueid`
     - `cn`
     - `memberOf` o. `isMemberOf`
   - **Contraseña**: La contraseña asociada al nombre de usuario.
   - **DN base de grupo**: La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com).

     Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.
   - **DN base de usuario**: La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.

     Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.
6. En la sección **Seguridad de la capa de transporte (TLS)**, seleccione una configuración de seguridad.
   - **Usar STARTTLS (recomendado)**: Usar STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada.
   - **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Esta opción es compatible por motivos de compatibilidad.
   - **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido.

     Esta opción no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.
7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar las conexiones.

- **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

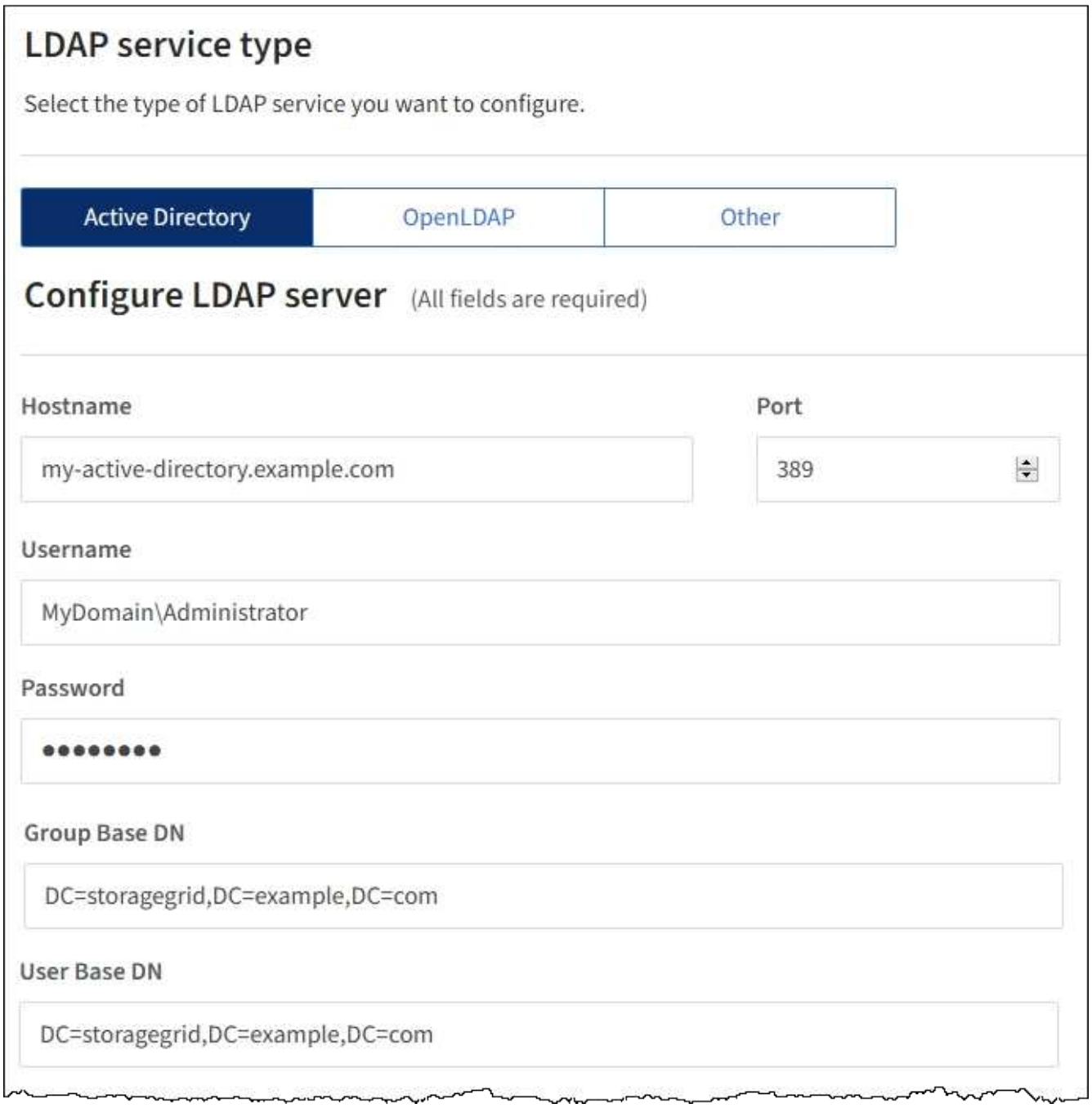
  Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

8. Seleccione **probar conexión** para validar la configuración de conexión para el servidor LDAP.

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

9. Si la conexión es válida, seleccione **Guardar**.

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



Información relacionada

"Permisos de gestión de inquilinos"

"Instrucciones para configurar un servidor OpenLDAP"

Instrucciones para configurar un servidor OpenLDAP

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

Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso en la Guía del administrador para OpenLDAP.

Indización

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

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

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

Consulte la información sobre el mantenimiento de pertenencia a grupos revertidos en la Guía del administrador para OpenLDAP.

Forzar la sincronización con el origen de identidades

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener permisos de acceso específicos.
- El origen de identidad guardado debe estar activado.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.

   Aparece la página federación de identidades. El botón **servidor de sincronización** se encuentra en la parte superior derecha de la página.

Si el origen de identidad guardado no está activado, el botón **servidor de sincronización** no estará activo.

2. Seleccione **servidor de sincronización**.

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

Información relacionada

"Permisos de gestión de inquilinos"

Desactivar la federación de identidades

Si ha configurado un servicio de federación de identidades para este inquilino, puede deshabilitar temporalmente o de forma permanente la federación de identidades para los grupos de inquilinos y usuarios. Cuando se deshabilita la federación de identidades, no hay comunicación entre el sistema StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

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

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión actualmente conservarán el acceso a la cuenta de inquilino hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- La sincronización entre el sistema StorageGRID y el origen de identidad no se llevará a cabo.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
2. Desactive la casilla de verificación **Activar federación de identidades**.
3. Seleccione **Guardar**.

Información relacionada

"Permisos de gestión de inquilinos"

Gestión de grupos

Se asignan permisos a grupos de usuarios para controlar qué tareas pueden realizar los usuarios de inquilinos. Puede importar grupos federados desde un origen de identidades, como Active Directory u OpenLDAP, o bien crear grupos locales.

Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan acceder a los recursos de S3 y Swift, según los permisos de grupo.

Permisos de gestión de inquilinos

Antes de crear un grupo de arrendatarios, tenga en cuenta qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios con el Administrador de inquilinos o la API de gestión de inquilinos. Un usuario puede pertenecer a uno o más grupos. Los permisos son acumulativos si un usuario pertenece a varios grupos.

Para iniciar sesión en el Administrador de arrendatarios o utilizar la API de administración de arrendatarios, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión pueden realizar las siguientes tareas:

- Vea la consola
- Cambiar su propia contraseña (para usuarios locales)

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.

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Permiso	Descripción
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos. **Nota:** los usuarios de Swift deben tener permiso acceso raíz para iniciar sesión en la cuenta de arrendatario.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino **Nota:** los usuarios de Swift deben tener el permiso de Administrador de Swift para realizar cualquier operación con la API de REST de Swift.
Gestione sus propias credenciales de S3	Solo inquilinos de S3. Permite a los usuarios crear y eliminar sus propias claves de acceso S3. Los usuarios que no tienen este permiso no ven la opción de menú **STORAGE (S3)** > **My S3 access keys**.

Permiso	Descripción
Administrar todos los depósitos	• Inquilinos S3: Permite a los usuarios usar el administrador de inquilinos y la API de gestión de inquilinos para crear y eliminar bloques S3, así como para gestionar la configuración de todos los bloques de S3 de la cuenta del inquilino, independientemente de las políticas de grupo o bloque de S3. Los usuarios que no tienen este permiso no ven la opción de menú **Cuchos**. • Inquilinos Swift: Permite a los usuarios de Swift controlar el nivel de coherencia de los contenedores Swift mediante la API de gestión de inquilinos. **Nota:** sólo puede asignar el permiso Administrar todos los cucharones a grupos Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.
Gestionar extremos	Solo inquilinos de S3. Permite a los usuarios usar el administrador de inquilinos o la API de gestión de inquilinos crear o editar extremos que se usan como destino de los servicios de plataforma StorageGRID. Los usuarios que no tienen este permiso no ven la opción de menú **terminales de servicios de plataforma**.

Información relacionada

"Use S3"

"Use Swift"

Creación de grupos para un inquilino de S3

Es posible gestionar permisos para grupos de usuarios S3 importando grupos federados o creando grupos locales.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione **Crear grupo**.
3. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

4. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. 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.
   - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.
7. Seleccione los permisos de grupo para este grupo.

   Consulte la información sobre los permisos de administración de inquilinos.

8. Seleccione **continuar**.
9. Seleccione una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo.

- **Sin acceso S3**: Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se conceda el acceso mediante una política de bloques. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
- **Acceso de sólo lectura**: Los usuarios de este grupo tienen acceso de sólo lectura a los recursos S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
- **Acceso completo**: Los usuarios de este grupo tienen acceso completo a los recursos S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
- **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto. Consulte las instrucciones para implementar una aplicación cliente S3 para obtener información detallada acerca de las políticas de grupo, incluidos la sintaxis del idioma y ejemplos.

10. Si ha seleccionado **personalizado**, introduzca la directiva de grupo. Cada política de grupo tiene un límite de tamaño de 5,120 bytes. Debe introducir una cadena con formato JSON válida.

    En este ejemplo, sólo se permite a los miembros del grupo enumerar y acceder a una carpeta que coincida con su nombre de usuario (prefijo de clave) en el bloque especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la directiva de bloque deben tenerse en cuenta al determinar la privacidad de estas carpetas.

11. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:
    - Grupo federado: **Crear grupo**
    - Grupo local: **Continuar**

    Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**.

Este paso no aparece para grupos federados.

12. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

    Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando agregue nuevos usuarios.

13. Seleccione **Finalizar**.

    El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

"Use S3"

Creación de grupos para un inquilino Swift

Es posible gestionar los permisos de acceso para una cuenta de inquilino de Swift mediante la importación de grupos federados o la creación de grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que se requiere para gestionar los contenedores y los objetos de una cuenta de inquilino de Swift.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione **Crear grupo**.
3. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

4. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. 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.
   - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.
7. Establezca el permiso Grupo.
   - Active la casilla de verificación **acceso raíz** si los usuarios necesitan iniciar sesión en el Administrador de inquilinos o la API de administración de inquilinos. (Predeterminado)
   - Anule la selección de la casilla de verificación **acceso raíz** si los usuarios no necesitan acceso al Administrador de inquilinos o a la API de administración de inquilinos. Por ejemplo, anule la selección de la casilla de verificación de las aplicaciones que no necesitan acceder al arrendatario. A

continuación, asigne el permiso **Swift Administrator** para permitir que estos usuarios administren contenedores y objetos.

8. Seleccione **continuar**.
9. Active la casilla de verificación **Swift Administrator** si el usuario necesita poder utilizar la API de REST de Swift.

   Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

10. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:
    - Grupo federado: **Crear grupo**
    - Grupo local: **Continuar**

      Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**. Este paso no aparece para grupos federados.

11. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

    Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando cree nuevos usuarios.

12. Seleccione **Finalizar**.

    El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

"Use Swift"

Ver y editar detalles del grupo

Al ver los detalles de un grupo, puede cambiar el nombre para mostrar del grupo, los permisos, las directivas y los usuarios que pertenecen al grupo.

Lo que necesitará

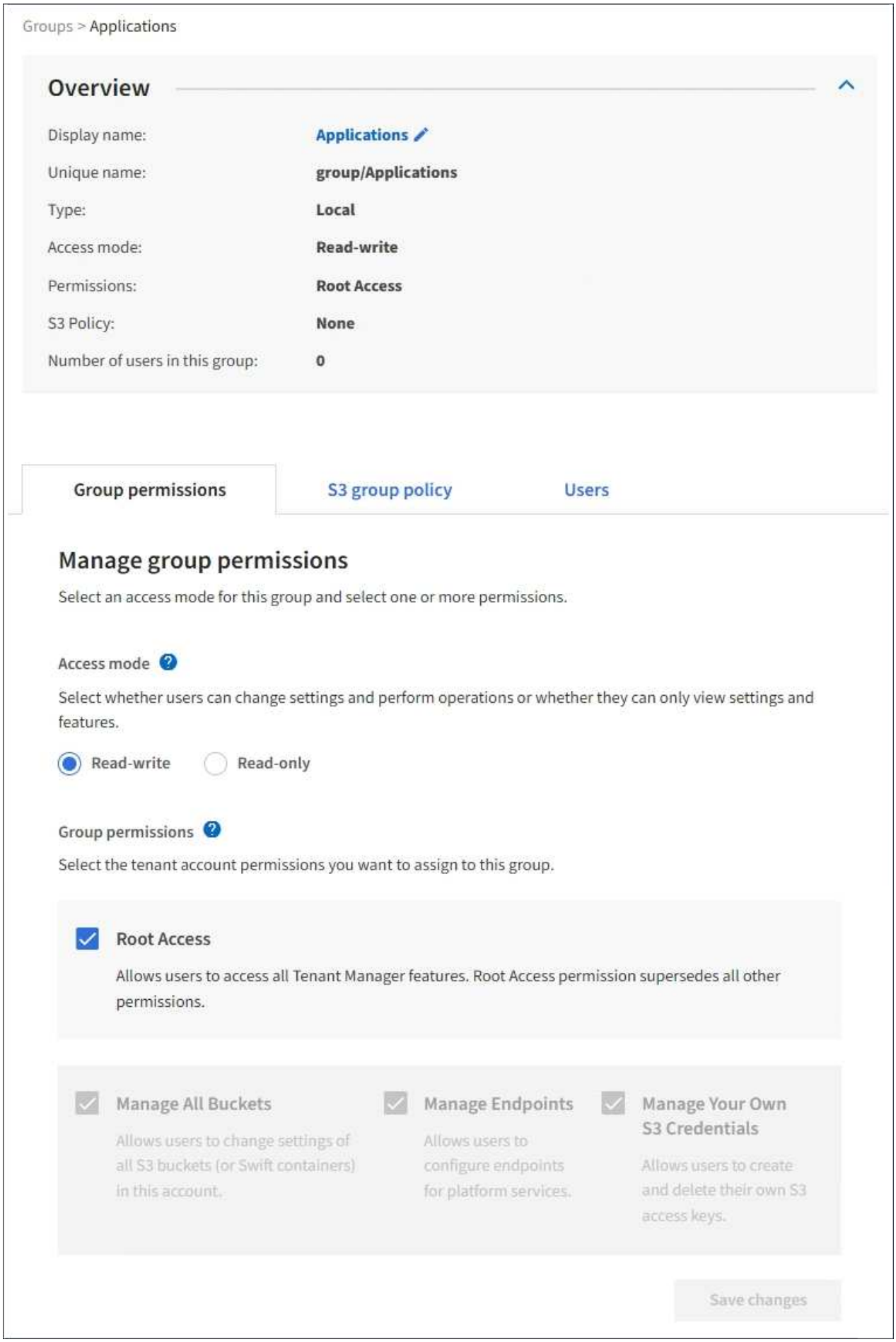
- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo cuyos detalles desee ver o editar.

   También puede seleccionar **acciones** > **Ver detalles del grupo**.

   Aparece la página de detalles del grupo. En el siguiente ejemplo, se muestra la página de detalles del grupo S3.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Realice cambios en la configuración del grupo según sea necesario.

   Para asegurarse de que se guardan los cambios, seleccione **Guardar cambios** después de realizar cambios en cada sección. Cuando se guarden los cambios, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

   a. De forma opcional, seleccione el nombre para mostrar o el icono de edición para actualizar el nombre para mostrar.

      No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

   b. Si lo desea, actualice los permisos.

   c. Para la política de grupo, realice los cambios adecuados para su inquilino S3 o Swift.

      - Si va a editar un grupo para un inquilino de S3, seleccione de forma opcional una política de grupo S3 diferente. Si selecciona una política de S3 personalizada, actualice la cadena JSON según sea necesario.
      - Si está editando un grupo para un inquilino Swift, también puede activar o desactivar la casilla de verificación **Swift Administrator**.

        Para obtener más información sobre el permiso de administrador de Swift, consulte las instrucciones para crear grupos para un inquilino Swift.

   d. Opcionalmente, agregue o elimine usuarios.

4. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya cambiado.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Creación de grupos para un inquilino de S3"

"Creación de grupos para un inquilino Swift"

Agregar usuarios a un grupo local

Puede agregar usuarios a un grupo local según sea necesario.

Lo que necesitará

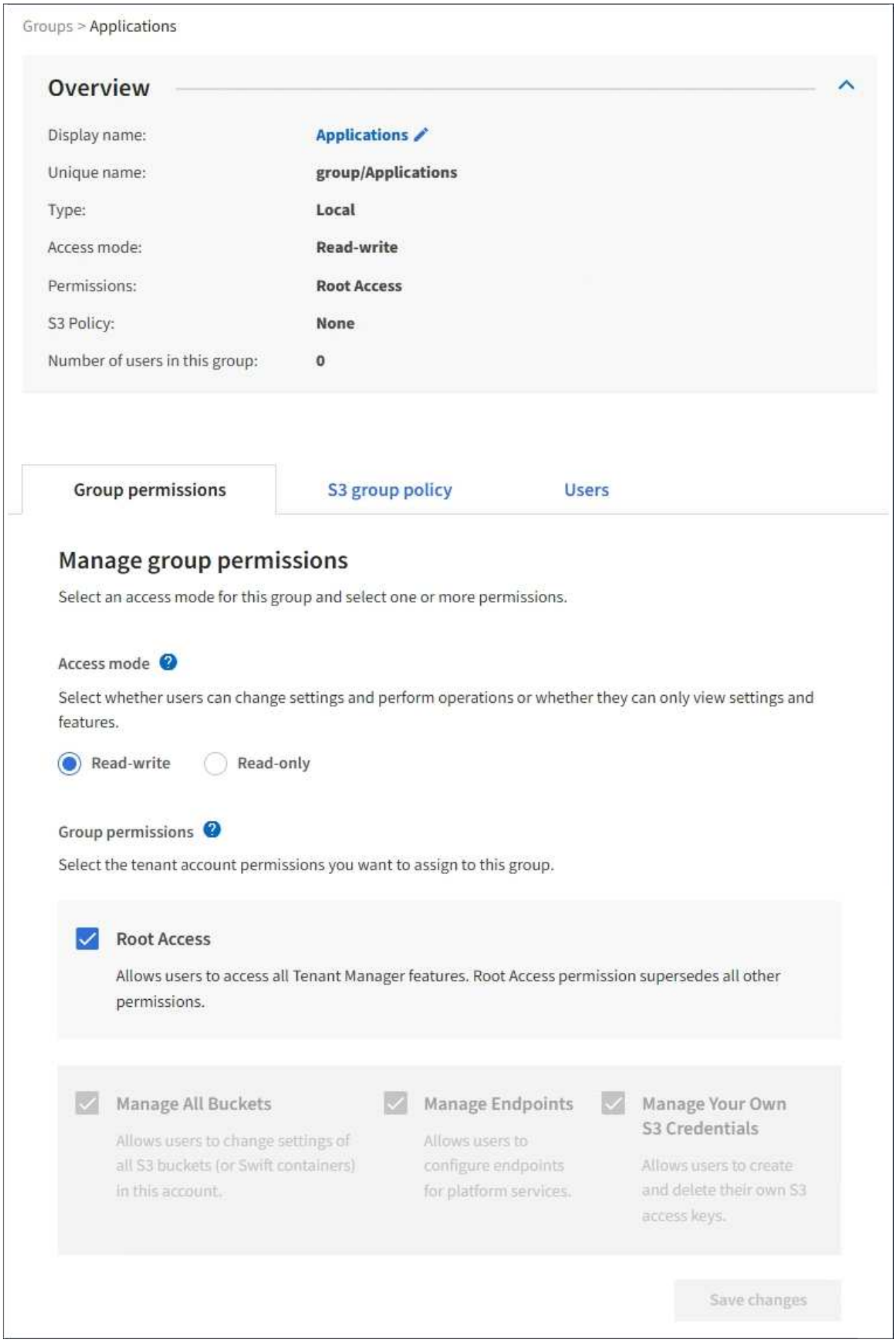
- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

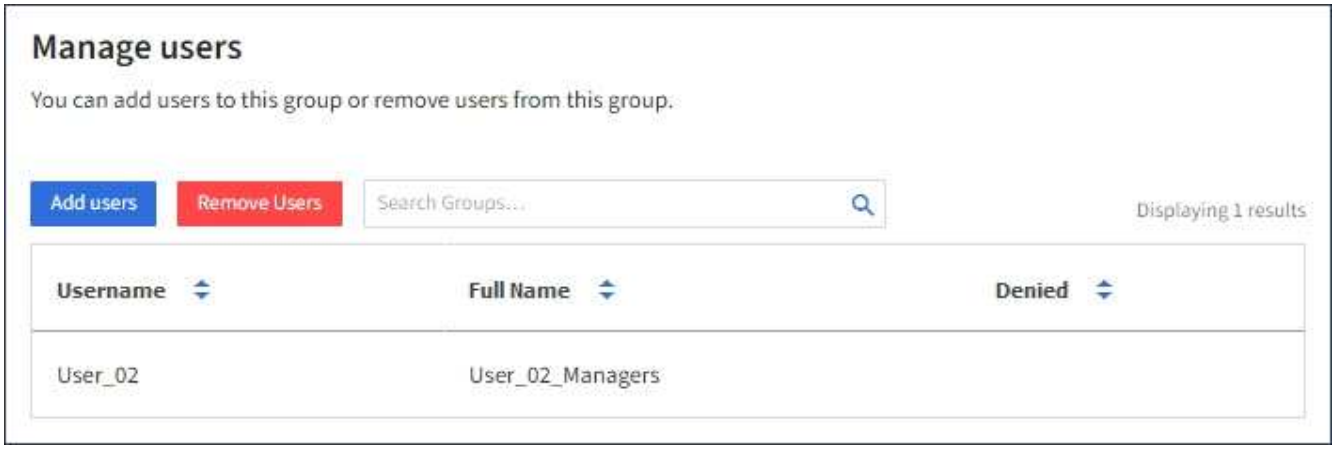
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo local al que desea añadir usuarios.

   También puede seleccionar **acciones** > **Ver detalles del grupo**.

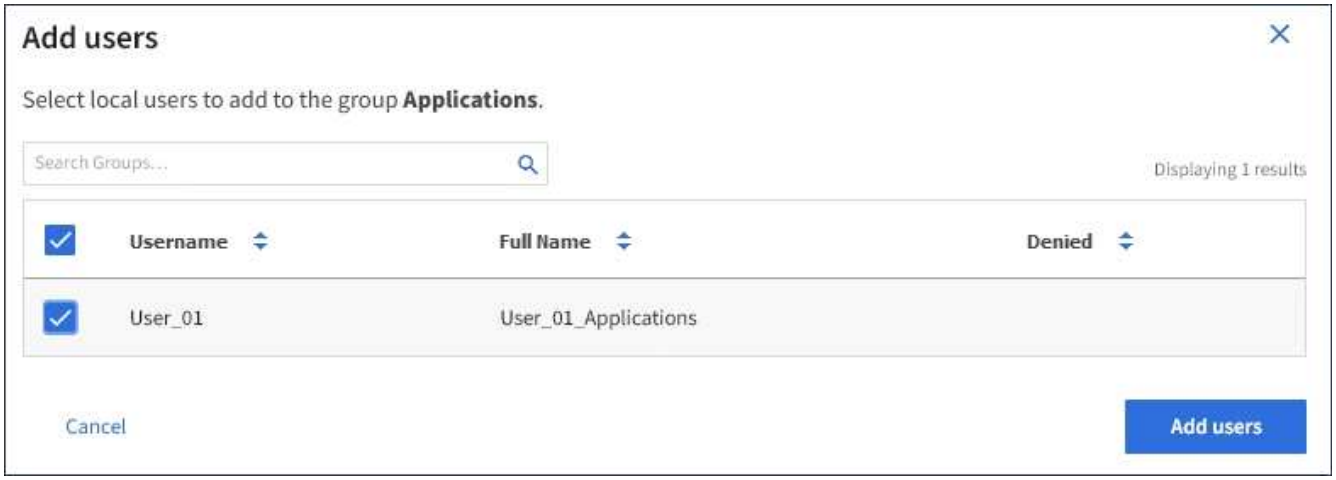
   Aparece la página de detalles del grupo.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Seleccione **gestionar usuarios** y, a continuación, seleccione **Agregar usuarios**.



4. Seleccione los usuarios que desea agregar al grupo y, a continuación, seleccione **Agregar usuarios**.



Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Edición de un nombre de grupo

Puede editar el nombre para mostrar de un grupo. No se puede editar el nombre único de un grupo.

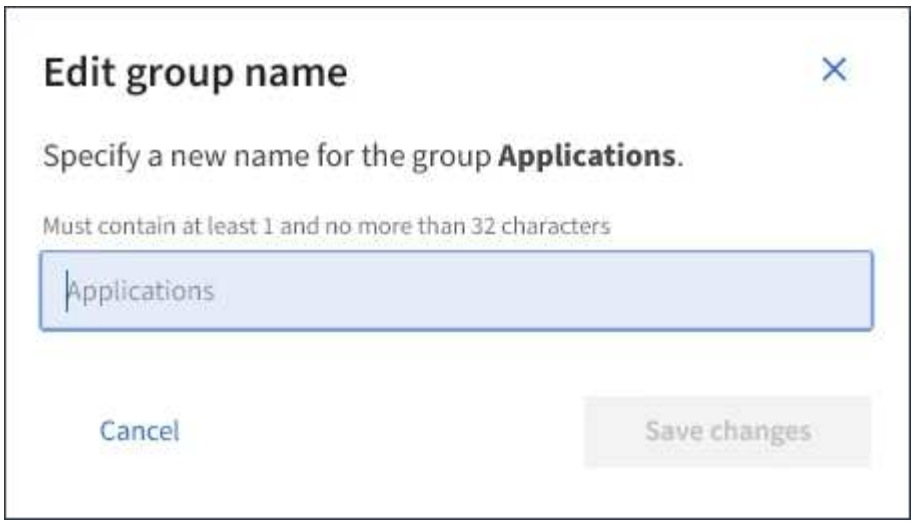
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo cuyo nombre para mostrar desee editar.
3. Seleccione **acciones** > **Editar nombre de grupo**.

   Aparece el cuadro de diálogo Editar nombre del grupo.



4. Si está editando un grupo local, actualice el nombre para mostrar según sea necesario.

   No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

5. Seleccione **Guardar cambios**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Duplicación de un grupo

Puede crear nuevos grupos más rápidamente duplicando un grupo existente.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.
3. Seleccione **Duplicar grupo**. Para obtener detalles adicionales sobre cómo crear un grupo, consulte las instrucciones para crear grupos para un inquilino S3 o para un inquilino Swift.
4. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

5. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el

nombre para mostrar más adelante.

- **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.

6. Seleccione **continuar**.
7. Según sea necesario, modifique los permisos para este grupo.
8. Seleccione **continuar**.
9. Según sea necesario, si va a duplicar un grupo para un inquilino S3, seleccione opcionalmente una directiva diferente de los botones de opción * Agregar directiva S3*. Si seleccionó una política personalizada, actualice la cadena JSON como sea necesario.
10. Seleccione **Crear grupo**.

Información relacionada

"Creación de grupos para un inquilino de S3"

"Creación de grupos para un inquilino Swift"

"Permisos de gestión de inquilinos"

Eliminar un grupo

Puede eliminar un grupo del sistema. Cualquier usuario que sólo pertenezca a ese grupo ya no podrá iniciar sesión en el Administrador de inquilinos ni utilizar la cuenta de arrendatario.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione las casillas de verificación de los grupos que desea eliminar.
3. Seleccione **acciones** > **Eliminar grupo**.

   Aparecerá un mensaje de confirmación.

4. Seleccione **Eliminar grupo** para confirmar que desea eliminar los grupos indicados en el mensaje de confirmación.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Gestión de usuarios locales

Puede crear usuarios locales y asignarles grupos locales para determinar las funciones a las que pueden acceder estos usuarios. El Administrador de arrendatarios incluye un usuario local predefinido denominado «'root'». Aunque puede agregar y quitar usuarios locales, no puede quitar el usuario raíz.

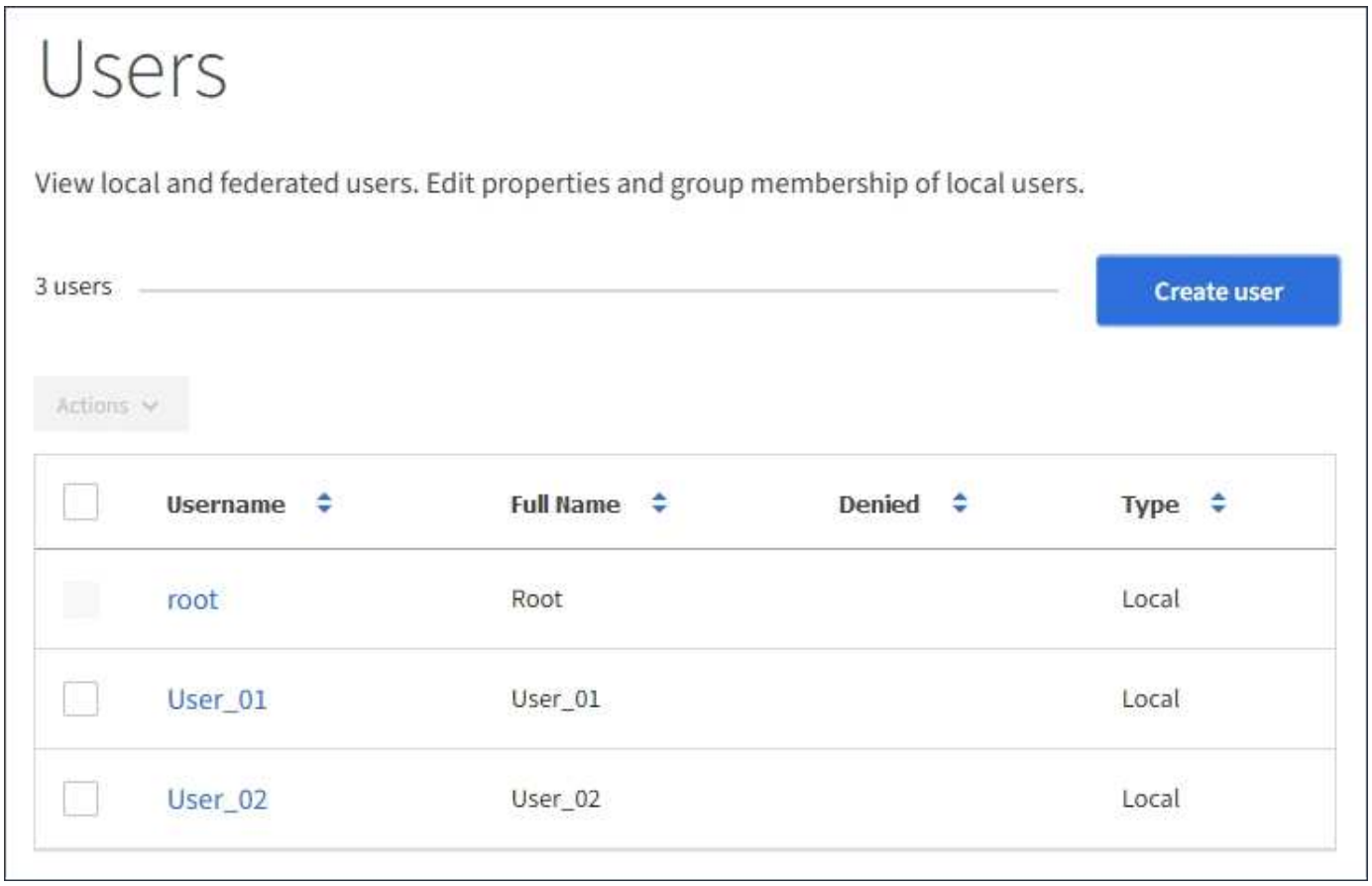
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios de lectura y escritura que tenga el permiso acceso raíz.

> Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el administrador de inquilinos o la API de gestión de inquilinos, aunque puedan usar las aplicaciones cliente S3 o Swift para acceder a los recursos del inquilino, en función de los permisos de grupo.

Acceso a la página usuarios

Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.



Creación de usuarios locales

Es posible crear usuarios locales y asignarles a uno o varios grupos locales para controlar sus permisos de acceso.

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de gestión ni políticas de grupo S3 aplicadas. Es posible que estos usuarios tengan acceso a bloques de S3 otorgado a través de una política de bloques.

Los usuarios de Swift que no pertenecen a ningún grupo no tienen permisos de gestión ni acceso al contenedor de Swift.

Pasos

1. Seleccione **Crear usuario**.
2. Complete los siguientes campos.
   - **Nombre completo**: El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
   - **Nombre de usuario**: El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.
   - **Contraseña**: Contraseña que se utiliza cuando el usuario inicia sesión.
   - **Confirmar contraseña**: Escriba la misma contraseña que escribió en el campo Contraseña.

- **Denegar acceso**: Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

  Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario para iniciar sesión.

3. Seleccione **continuar**.
4. Asigne el usuario a uno o más grupos locales.

   Los usuarios que no pertenecen a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan.

5. Seleccione **Crear usuario**.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Editar los detalles del usuario

Al editar los detalles de un usuario, puede cambiar el nombre completo y la contraseña del usuario, agregar el usuario a grupos diferentes e impedir que el usuario acceda al arrendatario.

Pasos

1. En la lista usuarios, seleccione el nombre del usuario cuyos detalles desee ver o editar.

   Como alternativa, puede seleccionar la casilla de verificación para el usuario y, a continuación, seleccionar **acciones** > **Ver detalles del usuario**.

2. Realice los cambios necesarios en la configuración del usuario.
   a. Cambie el nombre completo del usuario según sea necesario seleccionando el nombre completo o el icono de edición  En la sección Descripción general.

      No puede cambiar el nombre de usuario.

   b. En la ficha **Contraseña**, cambie la contraseña del usuario según sea necesario.
   c. En la ficha **Access**, permita que el usuario inicie sesión (seleccione **no**) o impida que el usuario inicie sesión (seleccione **Sí**) según sea necesario.
   d. En la ficha **grupos**, agregue el usuario a grupos o elimine el usuario de los grupos según sea necesario.
   e. Según sea necesario para cada sección, seleccione **Guardar cambios**.

      Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Duplicación de usuarios locales

Puede duplicar un usuario local para crear un usuario nuevo más rápidamente.

Pasos

1. En la lista usuarios, seleccione el usuario que desea duplicar.
2. Seleccione **Duplicar usuario**.
3. Modifique los campos siguientes para el nuevo usuario.

- **Nombre completo**: El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
- **Nombre de usuario**: El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.
- **Contraseña**: Contraseña que se utiliza cuando el usuario inicia sesión.
- **Confirmar contraseña**: Escriba la misma contraseña que escribió en el campo Contraseña.
- **Denegar acceso**: Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

  Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario para iniciar sesión.

4. Seleccione **continuar**.
5. Seleccione uno o más grupos locales.

   Los usuarios que no pertenecen a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan.

6. Seleccione **Crear usuario**.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Eliminación de usuarios locales

Es posible eliminar de forma permanente usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

Con el Administrador de inquilinos, puede eliminar usuarios locales, pero no usuarios federados. Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. En la lista usuarios, seleccione la casilla de verificación del usuario local que desea eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. En el cuadro de diálogo de confirmación, seleccione **Eliminar usuario** para confirmar que desea eliminar al usuario del sistema.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Gestión de cuentas de inquilinos de S3

Puede usar el administrador de inquilinos para gestionar claves de acceso S3, así como para crear y gestionar bloques de S3.

- "Gestión de claves de acceso de S3"
- "Gestión de bloques de S3"

Gestión de claves de acceso de S3

Cada usuario de una cuenta de inquilino de S3 debe tener una clave de acceso para almacenar y recuperar objetos en el sistema StorageGRID. Una clave de acceso consta de un ID de clave de acceso y una clave de acceso secreta.

Acerca de esta tarea

Las claves de acceso S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tengan el permiso **Administrar sus propias credenciales de S3** pueden crear o quitar sus propias claves de acceso S3.
- Los usuarios que tienen el permiso **acceso raíz** pueden administrar las claves de acceso para la cuenta raíz de S3 y el resto de usuarios. Las claves de acceso raíz proporcionan acceso completo a todos los bloques y objetos para el inquilino, a menos que se deshabilite explícitamente mediante una política de bloque.

StorageGRID admite la autenticación Signature versión 2 y Signature versión 4. No se permite el acceso de cuenta cruzada a menos que una política de bloque lo habilite explícitamente.

Crear sus propias claves de acceso S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a los bloques y los objetos de la cuenta de inquilino de S3.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.

Acerca de esta tarea

Puede crear una o varias claves de acceso S3 que le permiten crear y gestionar bloques para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nuevo ID de clave de acceso y clave de acceso secreta. Por motivos de seguridad, no cree más claves de las necesarias y elimine las claves que no esté utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- Establezca un tiempo de caducidad para sus llaves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta están expuestos accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo para la seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no tendrá que establecer un tiempo de caducidad para sus claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

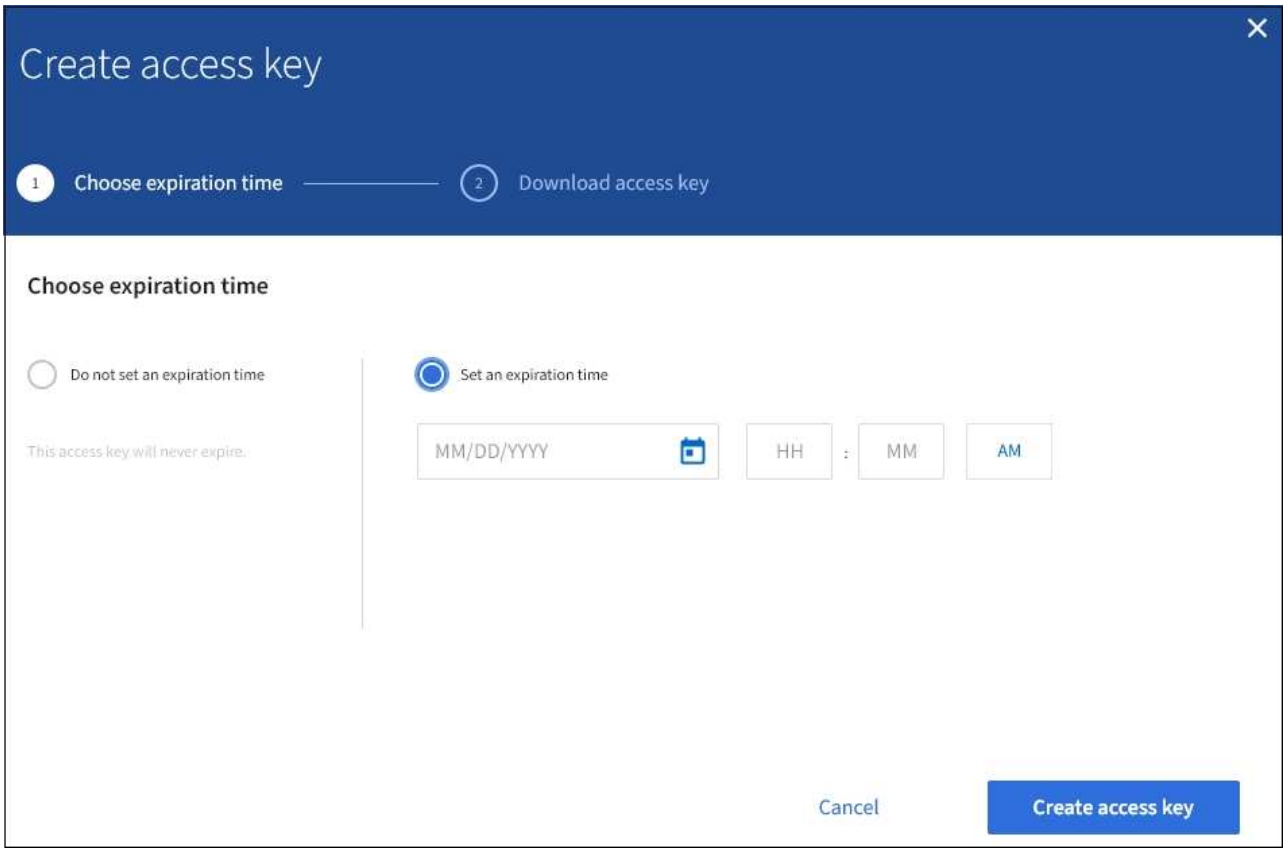
Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.

   Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.

2. Seleccione **Crear clave**.
3. Debe realizar una de las siguientes acciones:
   - Seleccione **no establezca un tiempo de caducidad** para crear una clave que no caducará. (Predeterminado)
   - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.

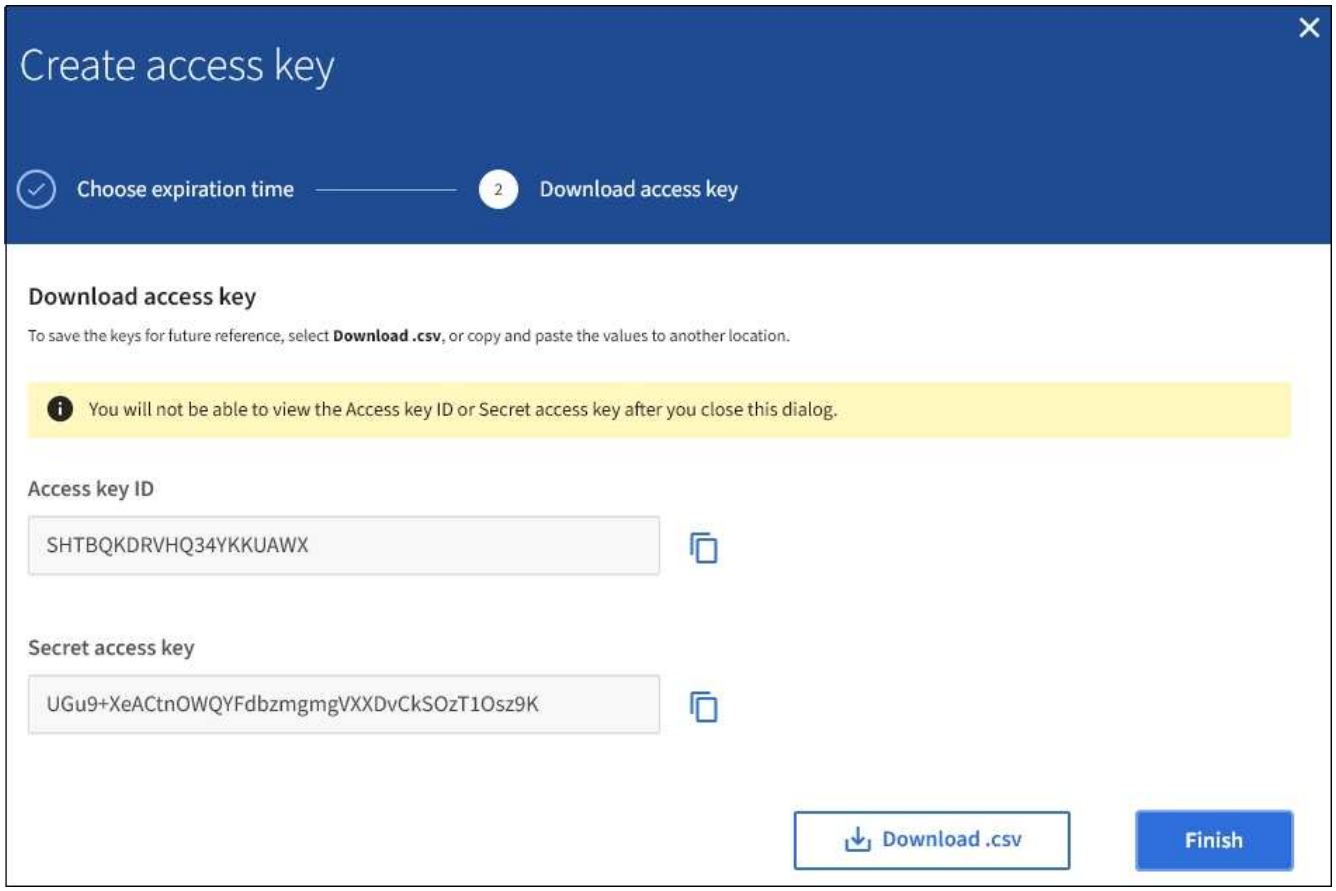


4. Seleccione **Crear clave de acceso**.

   Aparece el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la clave de acceso secreta.

5. 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.

   No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información.



6. Seleccione **Finalizar**.

   La nueva clave aparece en la página Mis claves de acceso. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Ver las claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de caducidad, de modo que puede determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves o eliminar claves que ya no utilice.

Lo que necesitará

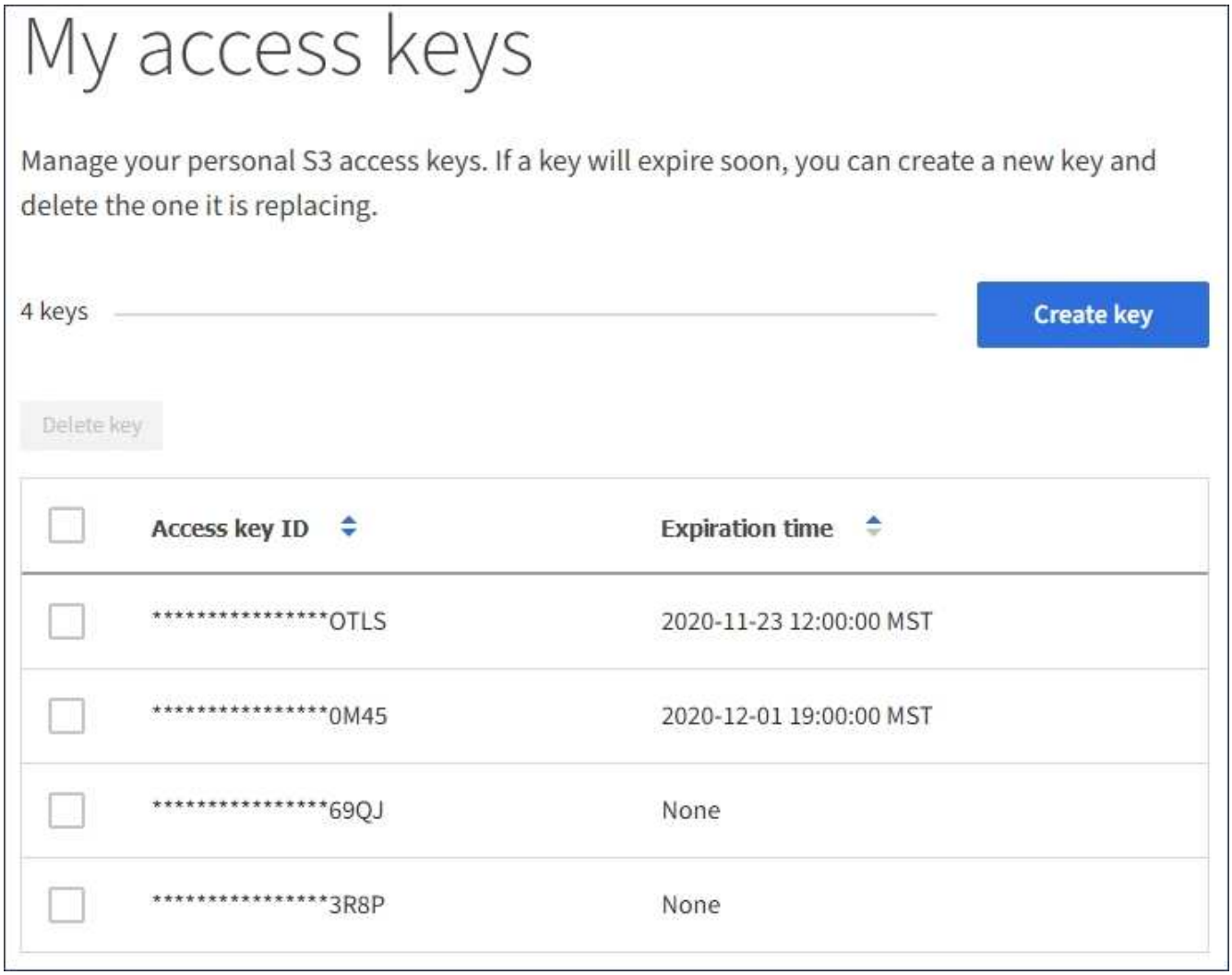
- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.

   Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.



2. Ordene las teclas por **tiempo de caducidad** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves y elimine manualmente las claves que ya no utilice.

   Si crea claves nuevas antes de que caduquen las claves existentes, puede empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

   Las claves caducadas se eliminan automáticamente.

Información relacionada

"Crear sus propias claves de acceso S3"

"Eliminar sus propias claves de acceso de S3"

Eliminar sus propias claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede eliminar sus propias claves de acceso S3. Cuando se elimina una clave de acceso, ya no se puede utilizar

para acceder a los objetos y los bloques de la cuenta de inquilino.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

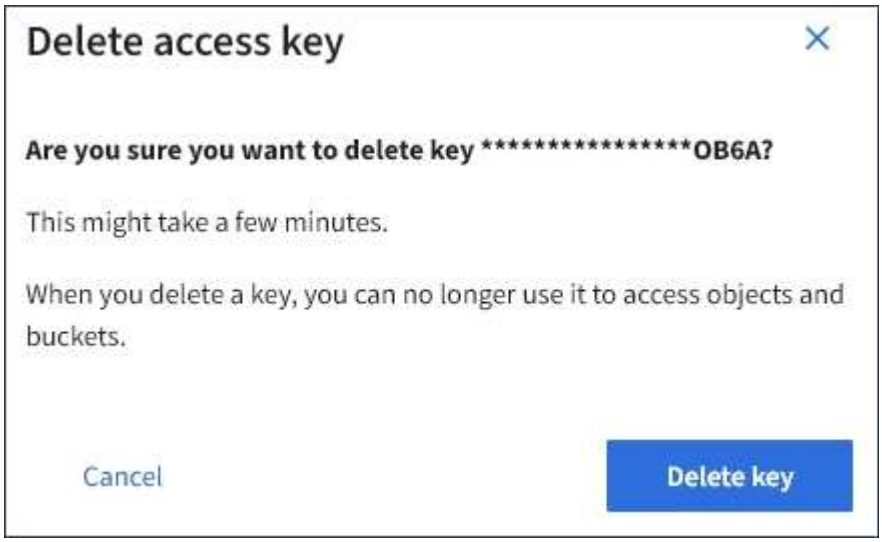
Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.

   Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.

2. Seleccione la casilla de comprobación de cada clave de acceso que desea quitar.
3. Seleccione **tecla Eliminar**.

   Se muestra un cuadro de diálogo de confirmación.



4. Seleccione **tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Crear las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene el permiso apropiado, puede crear claves de acceso S3 para otros usuarios, como las aplicaciones que necesitan acceso a bloques y objetos.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

Puede crear una o varias claves de acceso de S3 para otros usuarios, de modo que puedan crear y gestionar bloques para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con el nuevo ID de clave de acceso y la clave de acceso secreta. Por motivos de seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se estén utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- Establezca un tiempo de caducidad para que las claves limiten el acceso del usuario a un determinado período de tiempo. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo para la seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no tendrá que establecer un tiempo de caducidad para las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

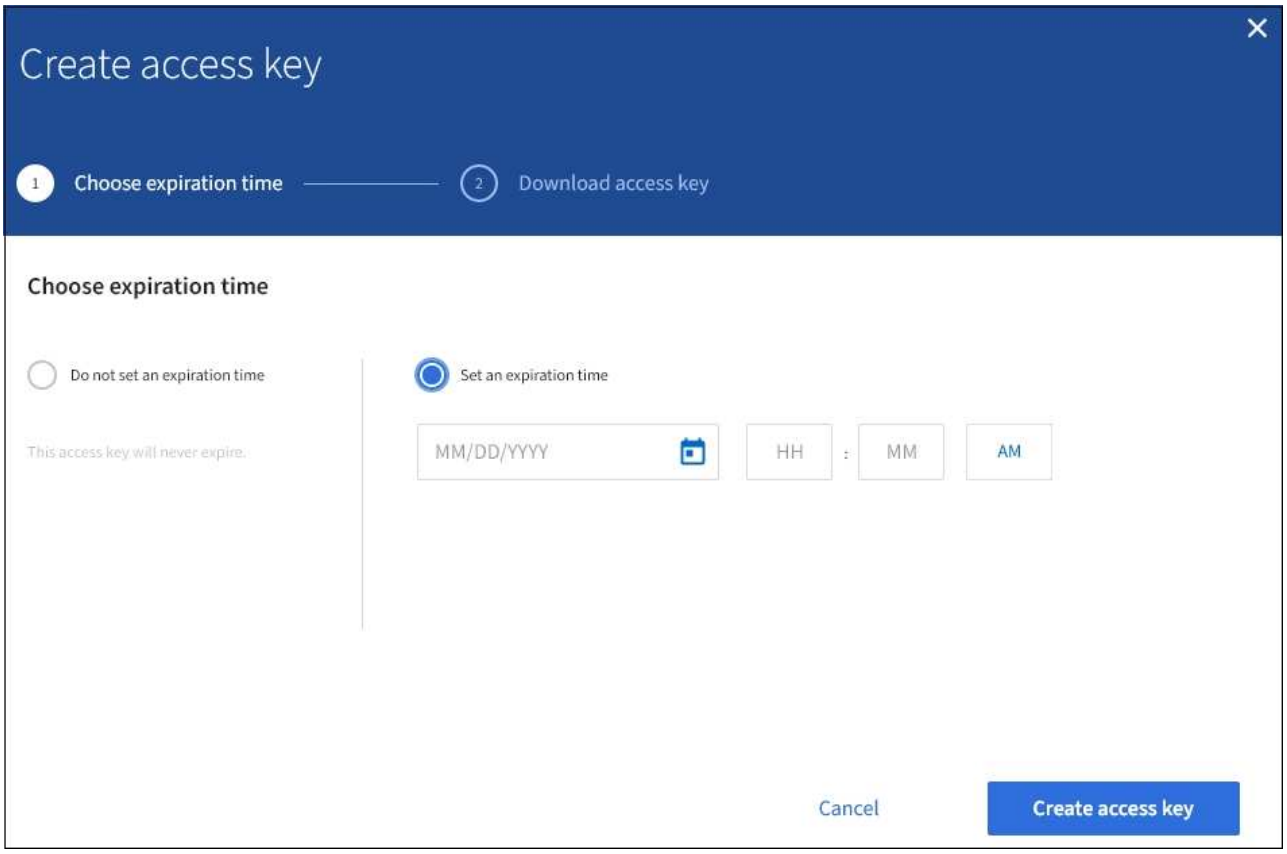
> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

   Aparece la página de detalles del usuario.

3. Seleccione **teclas de acceso** y, a continuación, seleccione **tecla de creación**.
4. Debe realizar una de las siguientes acciones:
   - Seleccione **no establezca un tiempo de caducidad** para crear una clave que no caduque. (Predeterminado)
   - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.

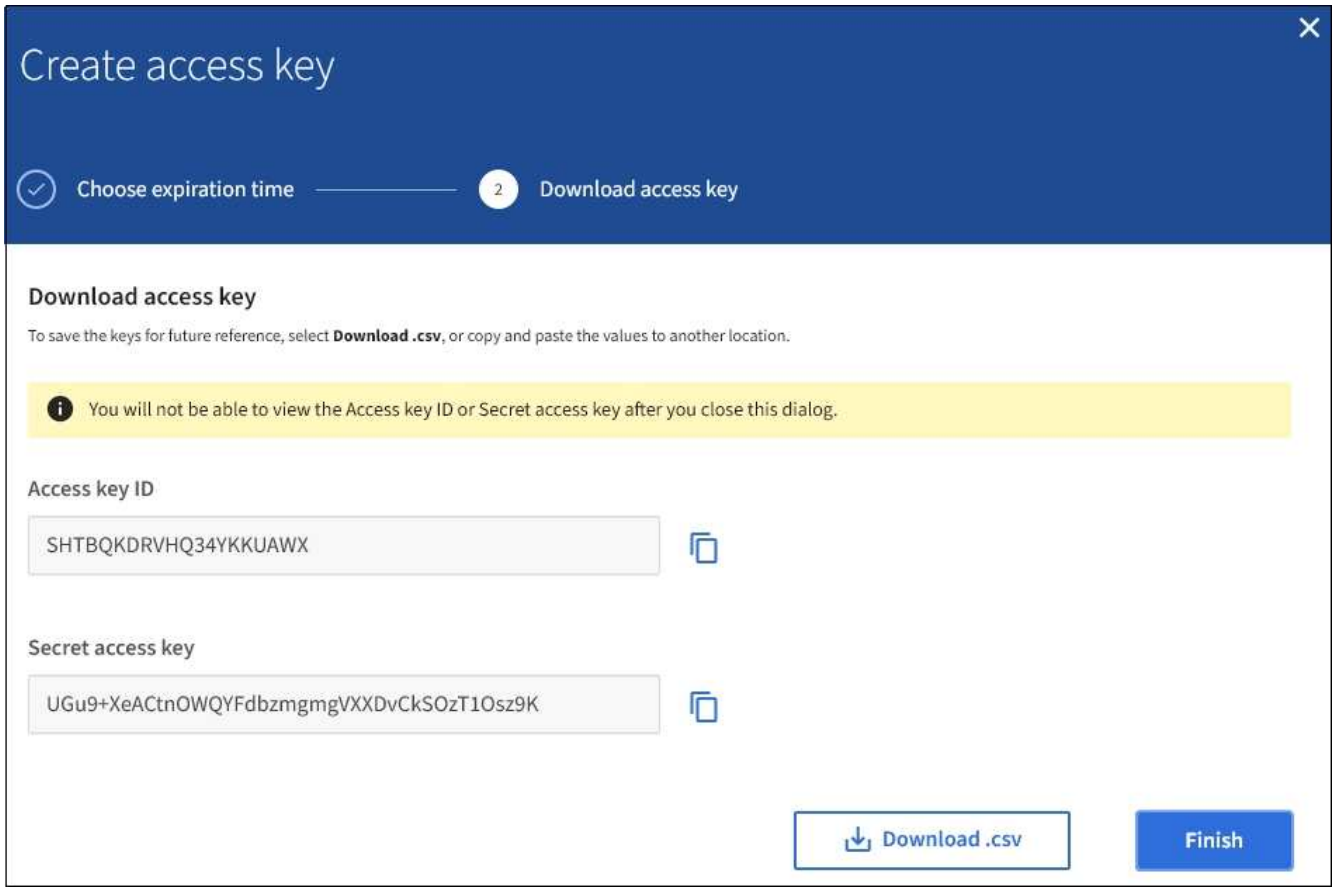


5. Seleccione **Crear clave de acceso**.

   Se muestra el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la clave de acceso secreta.

6. 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.

   No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información.



7. Seleccione **Finalizar**.

   La nueva clave aparece en la ficha teclas de acceso de la página de detalles del usuario. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Ver las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de caducidad para que pueda determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no estén en uso.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso acceso raíz.

> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

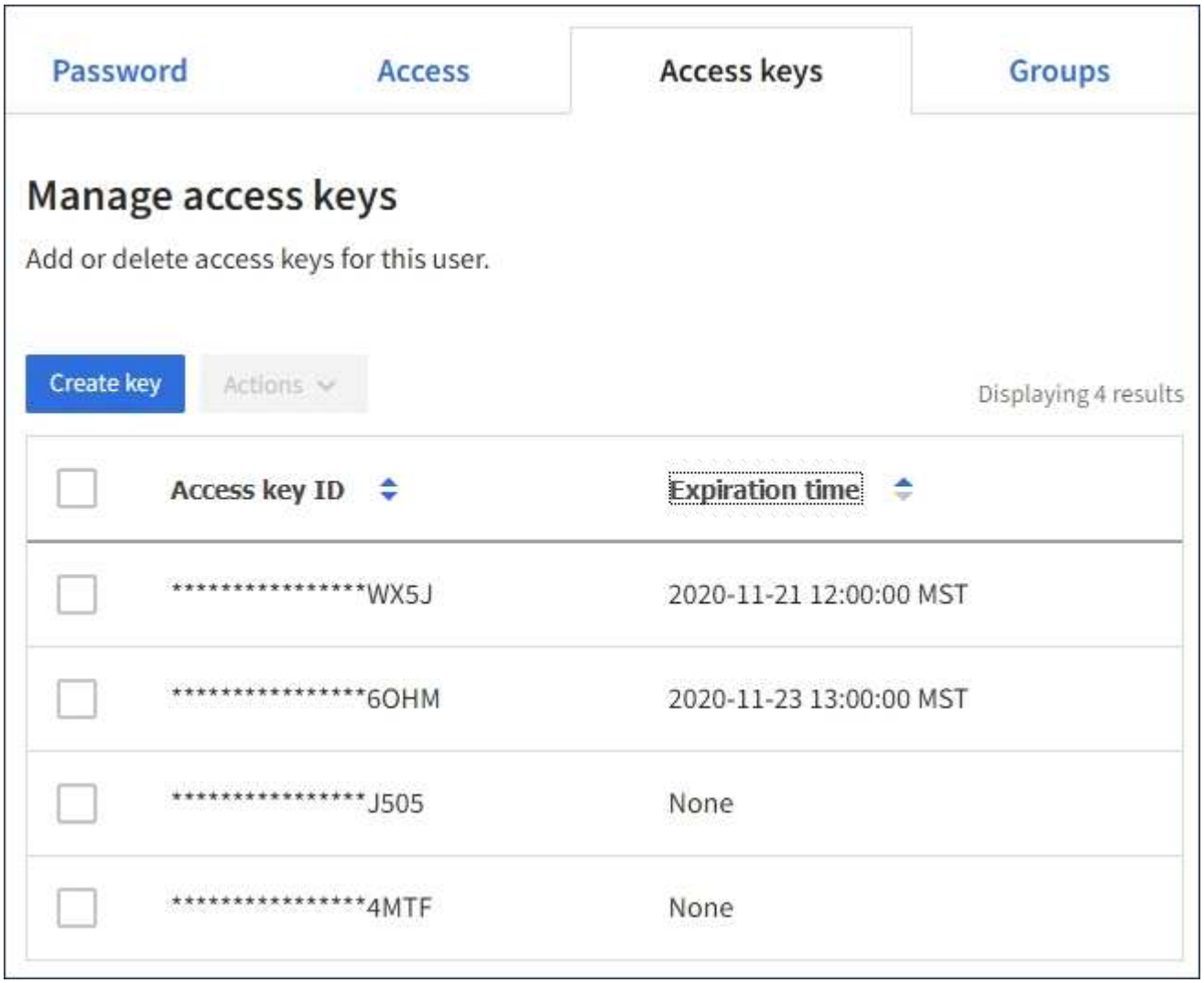
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.

   Aparece la página Users (usuarios) y enumera los usuarios existentes.

2. Seleccione el usuario cuyas claves de acceso de S3 desee ver.

   Aparece la página de detalles de usuario.

3. Seleccione **teclas de acceso**.



4. Ordene las teclas por **tiempo de caducidad** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las que ya no estén en uso.

   Si crea claves nuevas antes de que caduquen las claves existentes, el usuario podrá empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

   Las claves caducadas se eliminan automáticamente.

Información relacionada

"Crear las claves de acceso S3 de otro usuario"

"Eliminar las claves de acceso de S3 de otro usuario"

Eliminación de las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso acceso raíz.

> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.

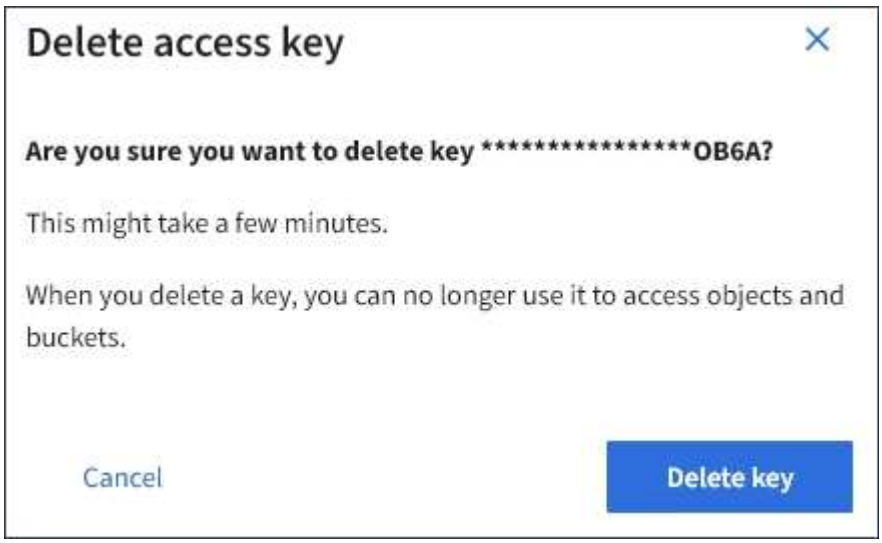
   Aparece la página Users (usuarios) y enumera los usuarios existentes.

2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

   Aparece la página de detalles de usuario.

3. Seleccione **teclas de acceso** y, a continuación, active la casilla de verificación de cada clave de acceso que desee eliminar.
4. Seleccione **acciones** > **Borrar clave seleccionada**.

   Se muestra un cuadro de diálogo de confirmación.



5. Seleccione **tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden

tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

"Permisos de gestión de inquilinos"

Gestión de bloques de S3

Si usa un inquilino de S3 con los permisos adecuados, puede crear, ver y eliminar bloques de S3, actualizar la configuración de nivel de coherencia, configurar el uso compartido de recursos de origen cruzado (CORS), habilitar y deshabilitar las opciones de actualización del tiempo de acceso anterior y gestionar servicios de plataforma de S3.

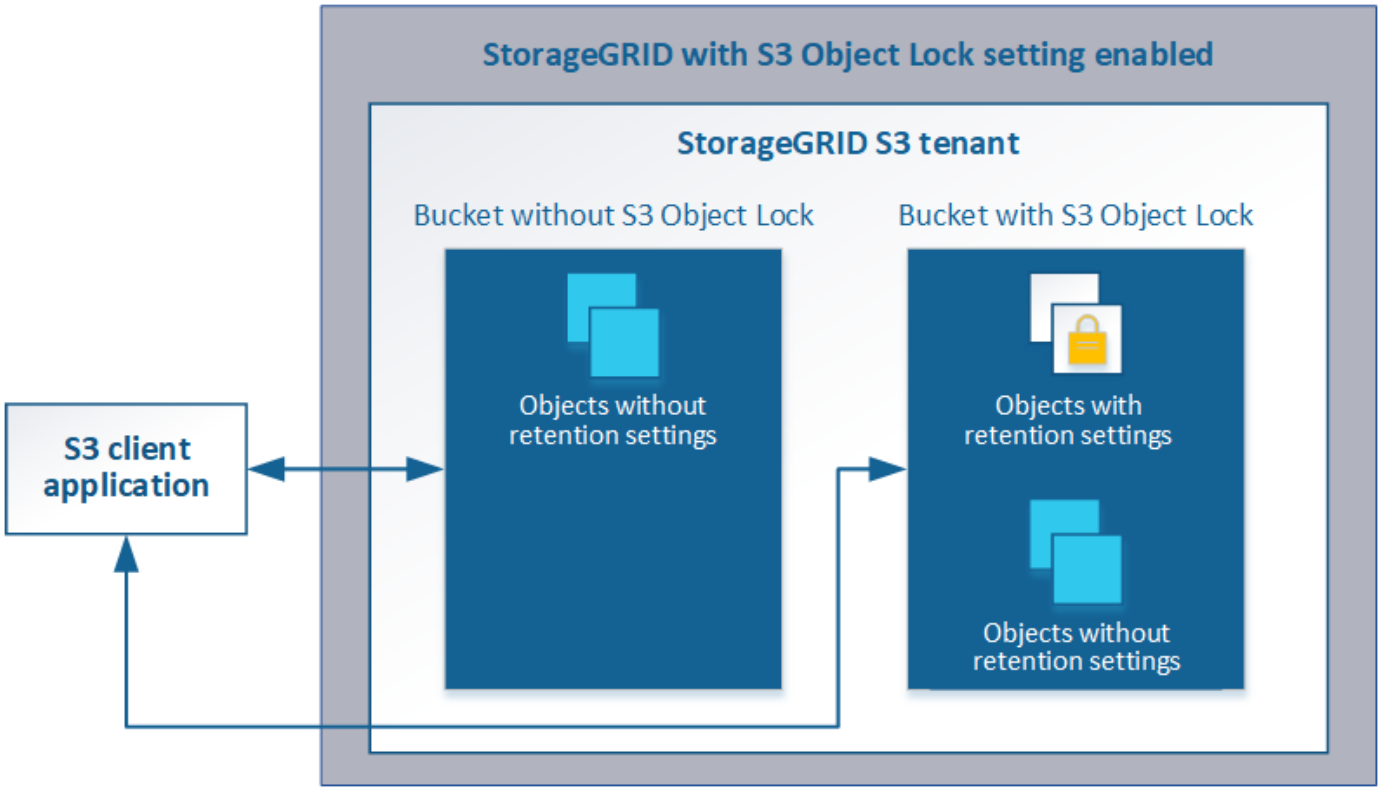
Uso del bloqueo de objetos de S3

Puede usar la función de bloqueo de objetos S3 en StorageGRID si los objetos deben cumplir los requisitos normativos de retención.

¿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 bloque tiene habilitada la función S3 Object Lock, las aplicaciones cliente S3 pueden especificar, opcionalmente, la configuración de retención para cualquier versión del objeto en ese bloque. Una versión de objeto debe tener la configuración de retención especificada para estar protegida por S3 Object Lock.



La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Si un bloque tiene habilitado el bloqueo de objetos S3, la aplicación cliente S3 puede especificar, de manera opcional, la siguiente configuración de retención a nivel de objeto al crear o actualizar un objeto:

- **Retener-hasta-fecha**: Si la fecha retener-hasta-fecha de una versión de objeto es en el futuro, el objeto puede ser recuperado, pero no puede ser modificado o eliminado. Según sea necesario, se puede aumentar la fecha de retención hasta de un objeto, pero esta fecha no se puede disminuir.
- **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.

Para obtener información detallada sobre estos ajustes, vaya a "'uso del bloqueo de objetos S3'" en "Operaciones y limitaciones compatibles con la API REST de S3".

Gestión de bloques que cumplen con las normativas heredadas

La función de bloqueo de objetos S3 sustituye la función Compliance disponible en versiones anteriores de StorageGRID. Si ha creado cubos compatibles con una versión anterior de StorageGRID, puede seguir gestionando la configuración de estos bloques; sin embargo, ya no puede crear nuevos bloques compatibles. Para obtener instrucciones, consulte el artículo de la base de conocimientos de NetApp.

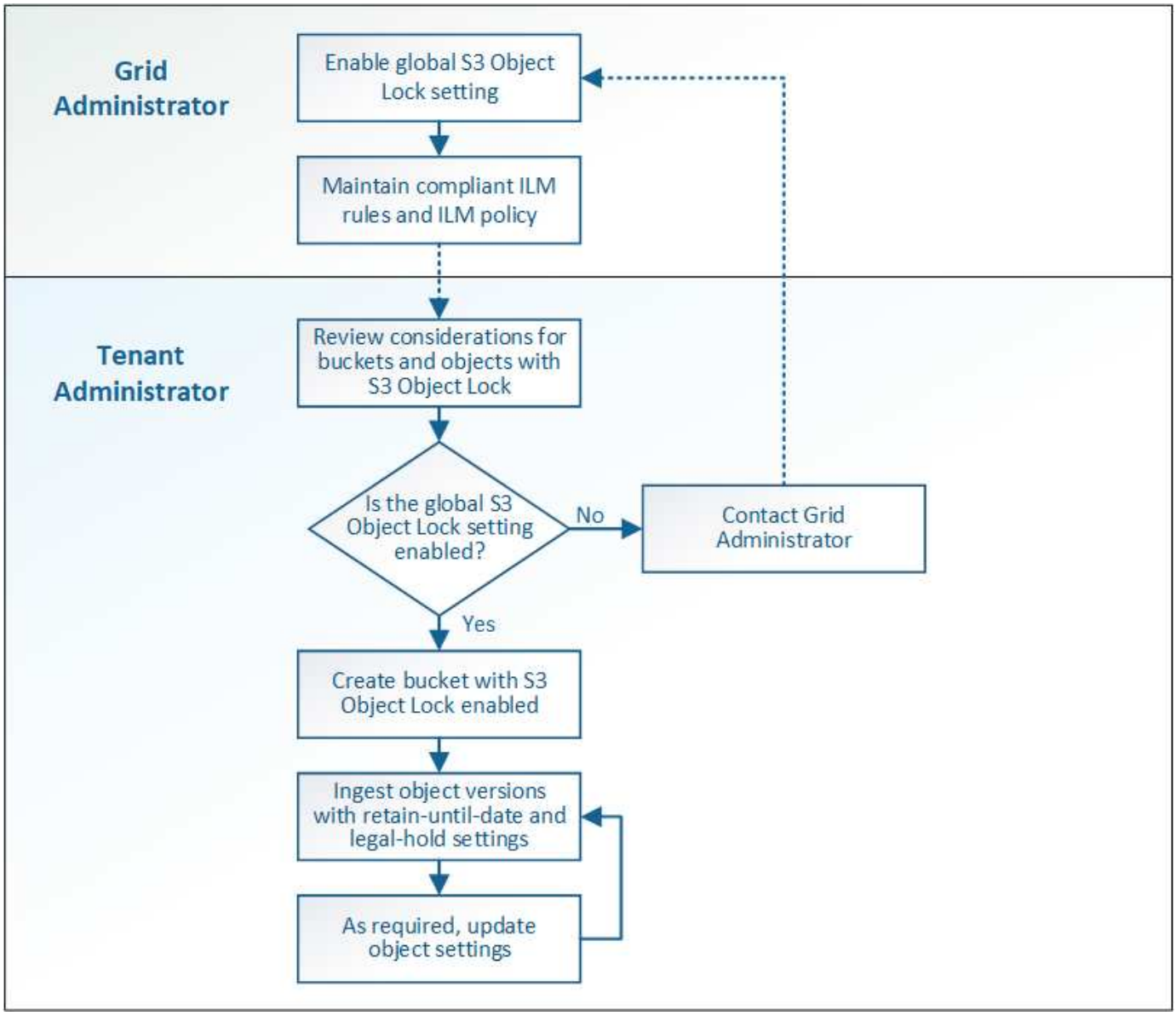
"Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Flujo de trabajo de bloqueo de objetos de S3

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar la función de bloqueo de objetos de S3 en StorageGRID.

Para poder crear bloques con el bloqueo de objetos S3 habilitado, el administrador de grid debe habilitar el valor global de bloqueo de objetos S3 para todo el sistema StorageGRID. El administrador del grid también debe asegurarse de que la política de gestión del ciclo de vida de la información (ILM) sea « conforme»; debe cumplir los requisitos de los bloques con la función S3 Object Lock habilitada. Para obtener más información, póngase en contacto con el administrador de grid o consulte las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Una vez que se habilita la opción global de bloqueo de objetos S3, se pueden crear bloques con el bloqueo de objetos S3 habilitado. Posteriormente, puede usar la aplicación cliente S3 para especificar opcionalmente la configuración de retención para cada versión del objeto.



Información relacionada

"Gestión de objetos con ILM"

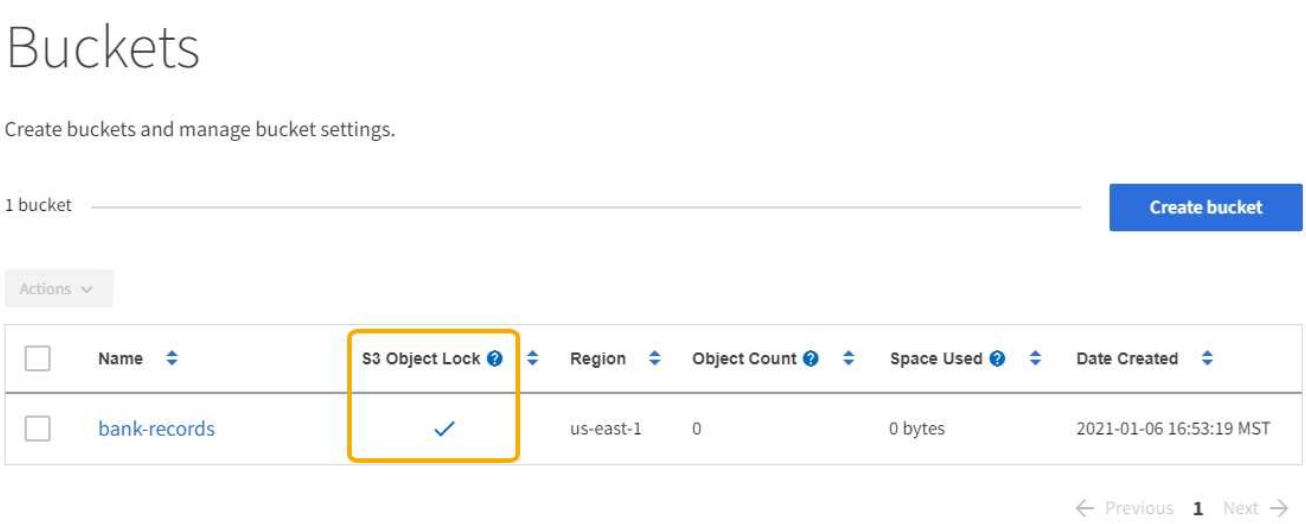
Requisitos para el bloqueo de objetos de S3

Antes de habilitar S3 Object Lock para un bloque, revise los requisitos para los bloques y objetos de S3 Object Lock y el ciclo de vida de los objetos en bloques con S3 Object Lock habilitado.

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.

  Este ejemplo del Administrador de inquilinos muestra un bloque 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 es posible habilitar el bloqueo de objetos de S3 para un bloque existente.
- Se requiere el versionado de bloques con S3 Object Lock. Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque.
- Después de crear un bloque con el bloqueo de objetos S3 habilitado, no se puede deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones de ese bloque.
- Un bloque StorageGRID con el bloqueo de objetos S3 habilitado no tiene un período de retención predeterminado. En su lugar, la aplicación cliente S3 puede especificar opcionalmente una fecha de retención y una configuración de conservación legal para cada versión del objeto que se agrega a ese bloque.
- Se admite la configuración del ciclo de vida de bloques para los bloques del ciclo de vida de objetos S3.
- 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

- La aplicación cliente S3 debe especificar la configuración de retención de cada objeto que tenga que protegerse mediante el bloqueo de objetos S3.
- Puede aumentar la fecha de retención hasta una versión de objeto, pero nunca puede disminuir este valor.
- Si recibe una notificación de una acción legal pendiente o una investigación normativa, puede conservar la información relevante colocando una retención legal en una versión del objeto. Cuando una versión de objeto se encuentra bajo una retención legal, ese objeto no se puede eliminar de StorageGRID, aunque haya alcanzado su fecha de retención. Tan pronto como se levante la retención legal, la versión del objeto se puede eliminar si se ha alcanzado la fecha de retención.
- El bloqueo de objetos de S3 requiere el uso de bloques con versiones. 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 bloque con el bloqueo de objetos S3 habilitado atraviesa tres etapas:

1. **Procesamiento de objetos**

- Al añadir una versión de objeto a un bloque con el bloqueo de objetos S3 habilitado, la aplicación cliente S3 puede especificar, de manera opcional, la configuración de retención del objeto (retener hasta la fecha, la conservación legal o ambos). A continuación, StorageGRID genera metadatos para ese objeto, que incluye un identificador de objeto (UUID) único y la fecha y la hora de procesamiento.
- Después de procesar una versión de objeto con configuración de retención, sus datos y los metadatos definidos por el usuario de S3 no se pueden modificar.
- StorageGRID almacena los metadatos del objeto de forma independiente de los datos del objeto. Mantiene tres copias de todos los metadatos de objetos en cada sitio.

2. **Retención de objetos**
   - StorageGRID almacena varias copias del objeto. El número y el tipo exactos de copias y las ubicaciones del almacenamiento se determinan según las reglas conformes de la política de ILM activa.
3. **Eliminación de objetos**
   - Un objeto se puede eliminar cuando se alcanza su fecha de retención.
   - No se puede eliminar un objeto que se encuentra bajo una retención legal.

Crear un bloque de S3

Puede usar el administrador de inquilinos para crear bloques S3 para los datos de objetos. Al crear un bloque, debe especificar el nombre y la región del bloque. Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, de manera opcional, puede habilitar el bloqueo de objetos S3 para el bloque.

Lo que necesitará

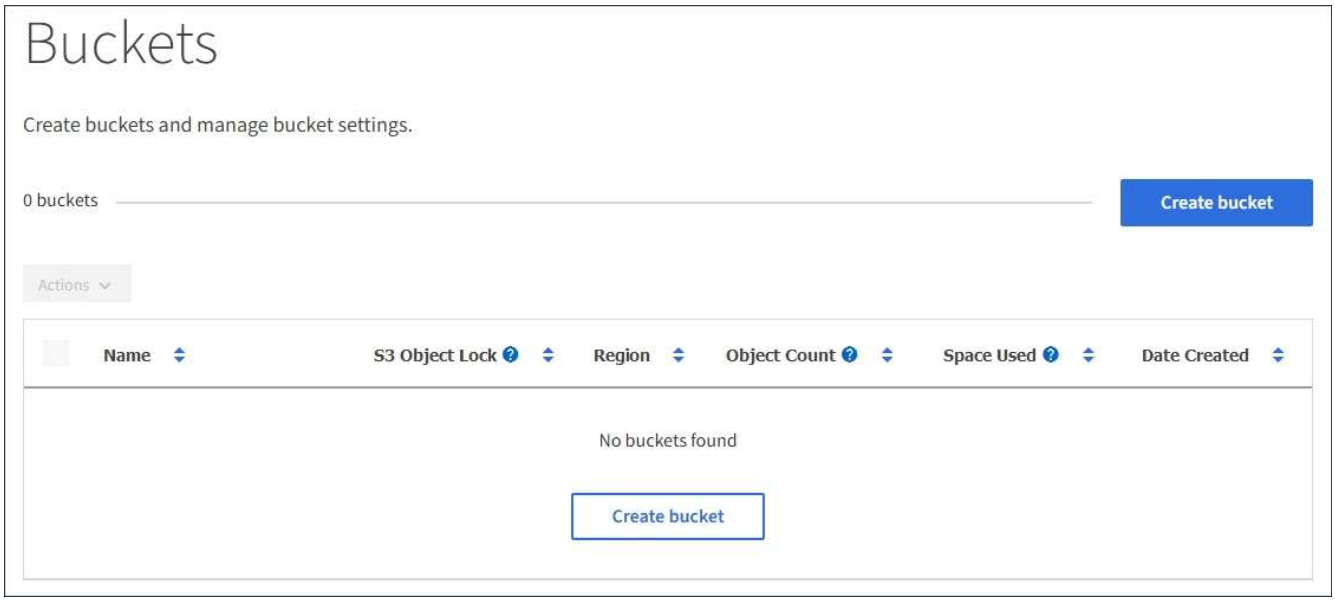
- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Si planea crear un bloque con bloqueo de objetos S3, la configuración global de bloqueo de objetos S3 debe haber estado habilitada para el sistema StorageGRID y debe haber revisado los requisitos para los bloques y objetos de bloqueo de objetos S3.

  "Uso del bloqueo de objetos de S3"

Pasos

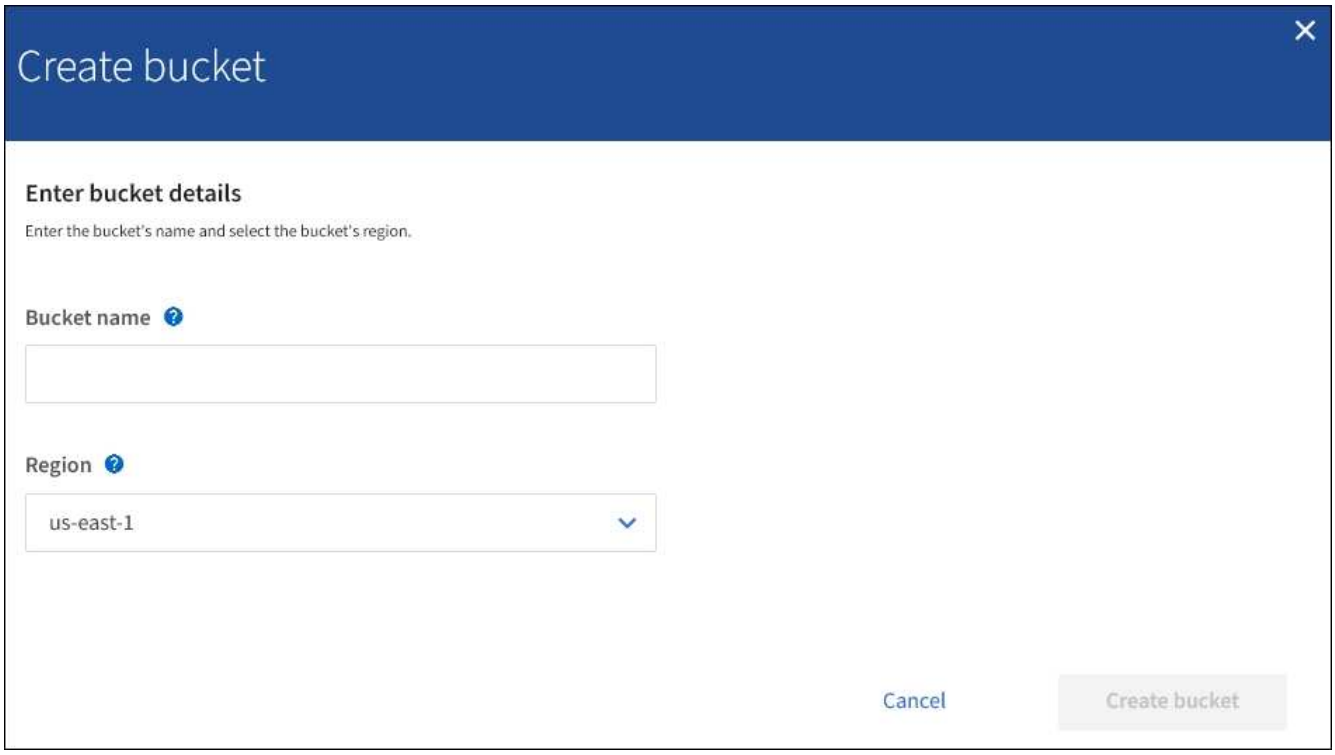
1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

   Aparece la página Cuchos y muestra todos los cestillos que ya se han creado.



2. Seleccione **Crear cucharón**.

   Se mostrará el asistente Create bucket.



> Si la opción de configuración global de bloqueo de objetos S3 está habilitada, Create bucket incluye un segundo paso para la gestión del bloqueo de objetos S3 para el bloque.

3. Introduzca un nombre único para el bloque.

> No se puede cambiar el nombre del bloque después de crear el bloque.

Los nombres de los bloques deben cumplir con las siguientes reglas:

- Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino).
- Debe ser compatible con DNS.
- Debe incluir al menos 3 y no más de 63 caracteres.
- Puede ser una serie de una o más etiquetas, con etiquetas adyacentes separadas por un punto. Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones.
- No debe ser una dirección IP con formato de texto.
- No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor.

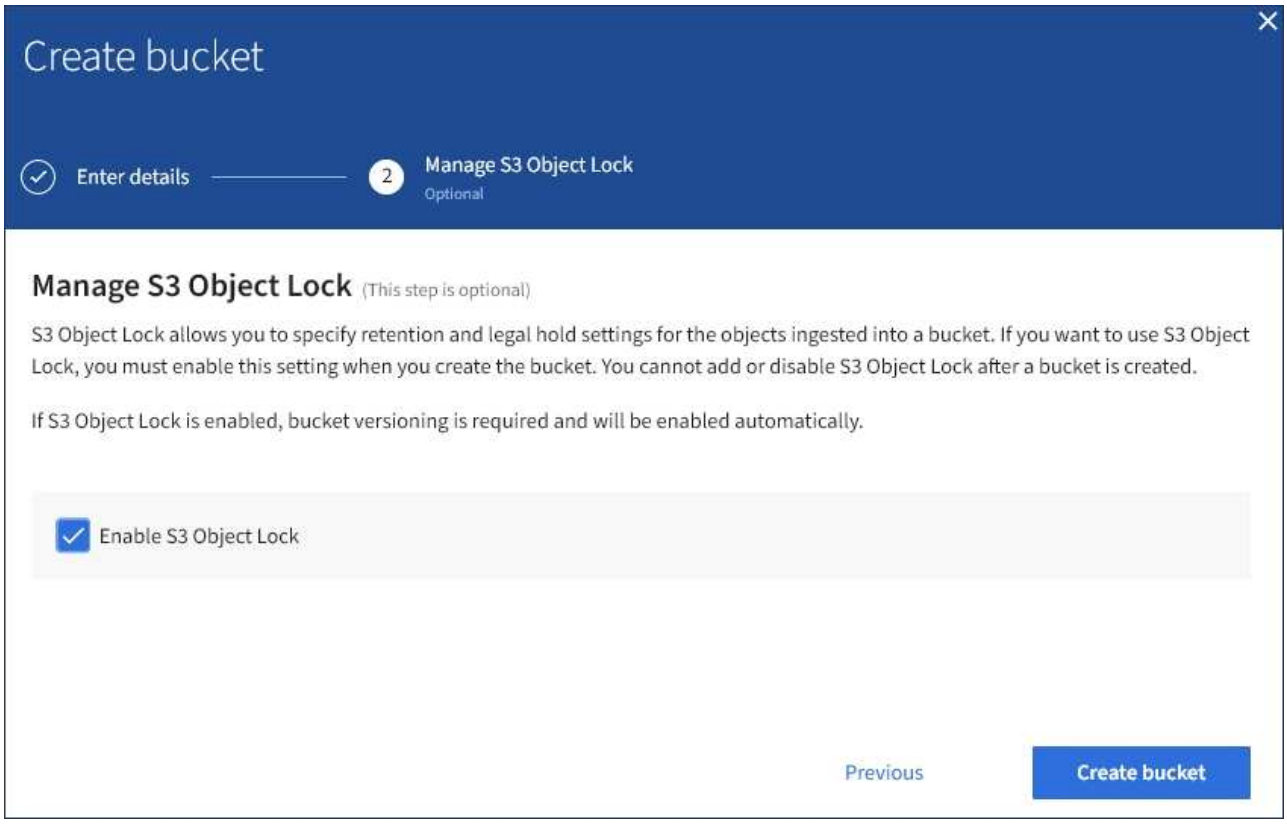
> Para obtener más información, consulte la documentación de Amazon Web Services (AWS).

4. Seleccione la región para este segmento.

   El administrador de StorageGRID gestiona las regiones disponibles. La región de un bloque puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los bloques se crean en la `us-east-1` región.

> No se puede cambiar la región después de crear el bloque.

5. Seleccione **Crear cucharón** o **continuar**.
   - Si el valor global de bloqueo de objetos S3 no está habilitado, seleccione **Crear bloque**. El cucharón se crea y se agrega a la tabla de la página Cuches.
   - Si el valor global de bloqueo de objetos S3 está activado, seleccione **continuar**. Paso 2, se muestra Manage S3 Object Lock.



6. De manera opcional, seleccione la casilla de comprobación para habilitar S3 Object Lock para este bloque.

   El bloqueo de objetos S3 debe estar habilitado para el bloque antes de que una aplicación cliente S3 pueda especificar la configuración de retención legal y hasta la fecha para los objetos agregados al bloque.

   > No se puede habilitar o deshabilitar S3 Object Lock después de crear el bloque.

   > Si habilita S3 Object Lock para un bloque, el control de versiones de bloques se habilita automáticamente.

7. Seleccione **Crear cucharón**.

   El cucharón se crea y se agrega a la tabla de la página Cuches.

Información relacionada

"Gestión de objetos con ILM"

"API de gestión de inquilinos"

"Use S3"

Ver los detalles de bloques de S3

Puede ver una lista de las configuraciones de bloques y bloques en su cuenta de inquilino.

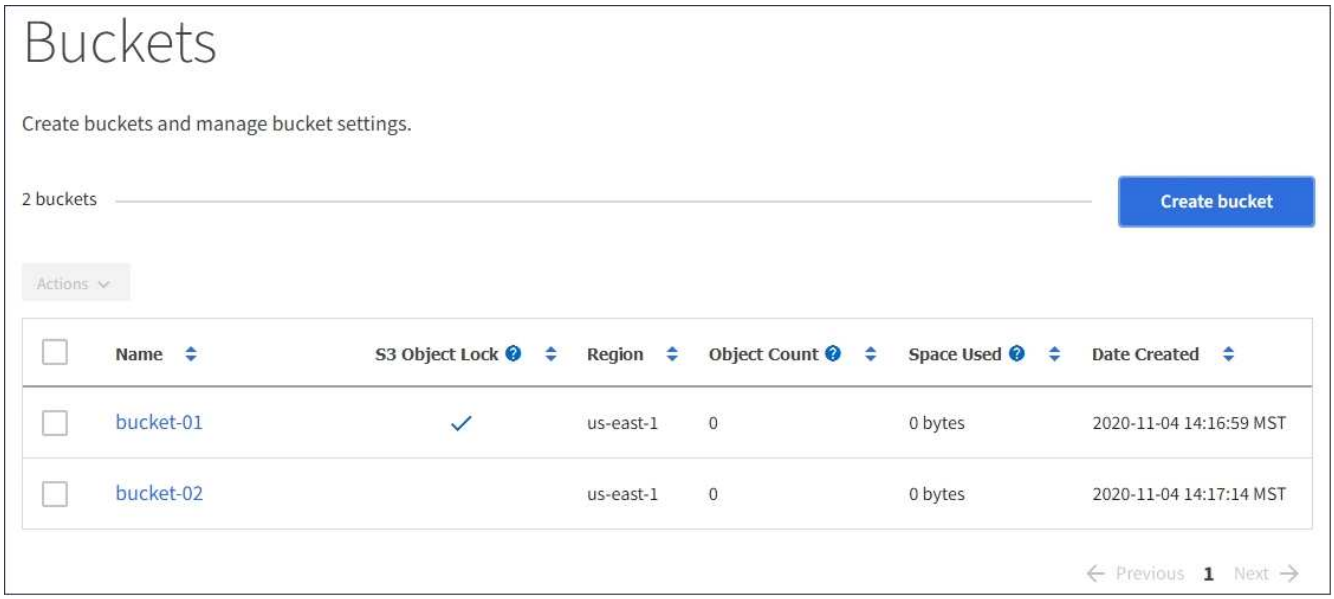
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

   Aparece la página Cuchos y enumera todos los cucharones de la cuenta de arrendatario.



2. Revisar la información de cada bloque.

   Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder por la lista.

   - Nombre: Nombre único del bloque, que no se puede cambiar.
   - S3 Object Lock: Si está habilitado el bloqueo de objetos de S3 para este bloque.

     Esta columna no se muestra si la configuración global de bloqueo de objetos S3 está deshabilitada. Esta columna también muestra información para todos los segmentos compatibles anteriores.

   - Región: La región del cucharón, que no se puede cambiar.
   - Recuento de objetos: El número de objetos de este bloque.
   - Espacio utilizado: Tamaño lógico de todos los objetos de este bloque. El tamaño lógico no incluye el espacio real necesario para las copias replicadas o con código de borrado o para los metadatos de objetos.
   - Fecha de creación: La fecha y la hora en que se creó el segmento.

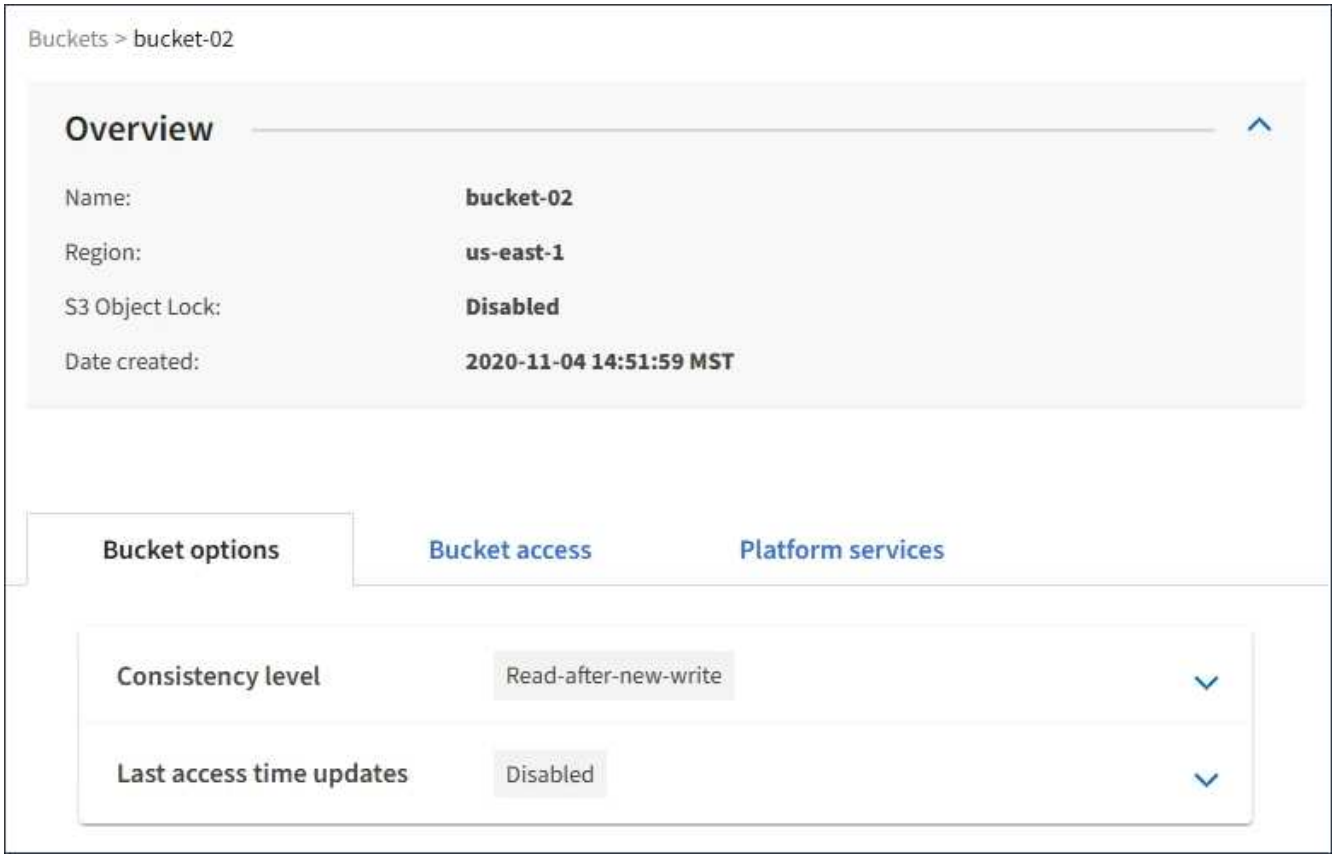
   > Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo.

3. Para ver y gestionar la configuración de un bloque, seleccione el nombre del bloque.

   Aparece la página de detalles bucket.

   Esta página le permite ver y editar la configuración para las opciones de bloque, el acceso a bloque y los servicios de plataforma.

   Consulte las instrucciones para configurar cada ajuste o servicio de plataforma.



Información relacionada

"Cambiar el nivel de coherencia"

"Habilitar o deshabilitar las actualizaciones de la hora del último acceso"

"Configuración de uso compartido de recursos de origen cruzado (CORS)"

"Configurar la replicación de CloudMirror"

"Configuración de notificaciones de eventos"

"Configurar el servicio de integración de búsqueda"

Cambiar el nivel de coherencia

Si usa un inquilino de S3, puede usar el administrador de inquilinos o la API de gestión de inquilinos para cambiar el control de coherencia para las operaciones realizadas en los objetos en los bloques S3.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El nivel de coherencia establece una compensación entre la disponibilidad de los objetos y la coherencia de dichos objetos en los diferentes nodos y sitios de almacenamiento. En general, debe utilizar el nivel de

consistencia de **lectura tras escritura nueva** para sus cucharones. Si el nivel de consistencia de **lectura tras escritura nueva** no cumple los requisitos de la aplicación cliente, puede cambiar el nivel de consistencia estableciendo el nivel de consistencia de la cuchara o utilizando la `Consistency-Control` encabezado. La `Consistency-Control` el encabezado anula el nivel de consistencia del cucharón.

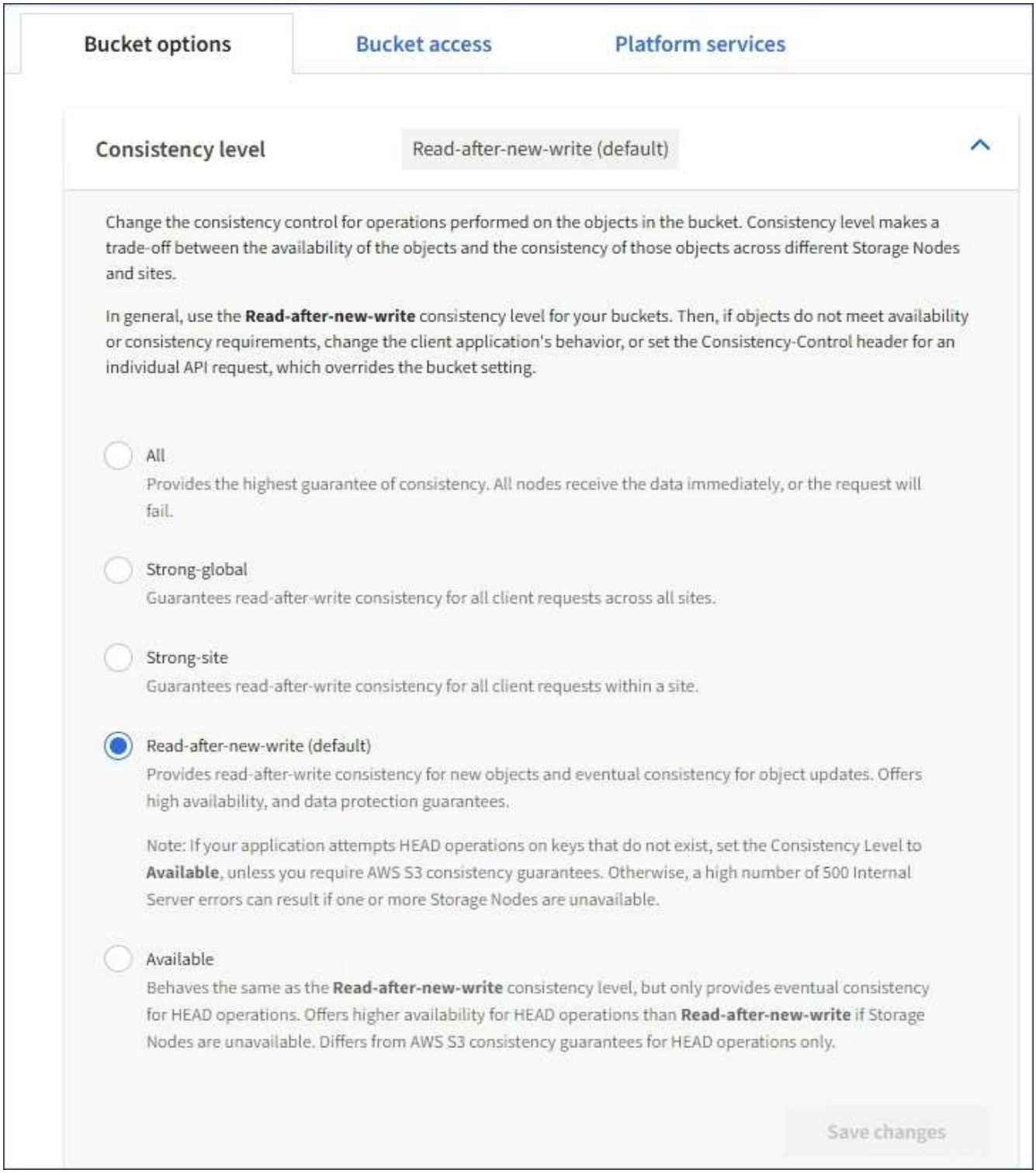
> Cuando se cambia el nivel de consistencia de un cubo, solo se garantiza que los objetos que se ingieren después del cambio alcancen el nivel revisado.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque** > **nivel de coherencia**.



4. Seleccione un nivel de coherencia para las operaciones realizadas en los objetos de este bloque.

Nivel de coherencia	Descripción
Todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.

Nivel de coherencia	Descripción
Fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
Sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
Read-after-new-write (predeterminado)	Proporciona coherencia de lectura tras escritura para los objetos nuevos y consistencia final para las actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Coincide con las garantías de coherencia de Amazon S3. **Nota:** Si su aplicación intenta realizar operaciones HEAD en claves que no existen, establezca el nivel de consistencia en **disponible**, a menos que necesite garantías de consistencia de Amazon S3. De lo contrario, un número elevado de 500 errores internos del servidor pueden producirse si uno o más nodos de almacenamiento no están disponibles.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia de **lectura tras escritura nueva**, pero sólo proporciona consistencia eventual para las operaciones DE CABEZAL. Ofrece una mayor disponibilidad para operaciones CON CABEZAL que **lectura tras escritura nueva** si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

5. Seleccione **Guardar cambios**.

Información relacionada

"Permisos de gestión de inquilinos"

Habilitar o deshabilitar las actualizaciones de la hora del último acceso

Cuando los administradores de grid crean las reglas de gestión del ciclo de vida de la información (ILM) para un sistema StorageGRID, puede especificar si desea mover ese objeto a una ubicación de almacenamiento diferente. Si usa un inquilino de S3, puede aprovechar esas reglas al habilitar actualizaciones en la última hora de acceso para los objetos de un bloque de S3.

Estas instrucciones sólo se aplican a los sistemas StorageGRID que incluyen al menos una regla de ILM que utiliza la opción **última hora de acceso** en sus instrucciones de colocación. Puede ignorar estas instrucciones si el sistema StorageGRID no incluye dicha regla.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Last Access Time es una de las opciones disponibles para la instrucción de colocación **Reference Time** para una regla de ILM. Si se establece el tiempo de referencia de una regla en tiempo de último acceso, los

administradores de la cuadrícula pueden especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento en función de cuándo se recuperaron por última vez esos objetos (se leen o se visualizan).

Por ejemplo, para asegurarse de que los objetos que se ven recientemente permanecen en un almacenamiento más rápido, el administrador de grid puede crear una regla de ILM que especifique lo siguiente:

- Los objetos que se han recuperado durante el último mes deben permanecer en los nodos de almacenamiento local.
- Los objetos que no se han recuperado en el último mes deben moverse a una ubicación externa.

> Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

De forma predeterminada, las actualizaciones de la hora del último acceso están desactivadas. Si el sistema StorageGRID incluye una regla de ILM que utiliza la opción **Hora de último acceso** y desea que esta opción se aplique a los objetos de este bloque, debe habilitar las actualizaciones para el último tiempo de acceso para los bloques S3 especificados en esa regla.

> La actualización del último tiempo de acceso cuando se recupera un objeto puede reducir el rendimiento de la StorageGRID, especialmente en objetos pequeños.

El impacto en el rendimiento se produce con las actualizaciones del último tiempo de acceso porque StorageGRID debe realizar estos pasos adicionales cada vez que se recuperan los objetos:

- Actualice los objetos con nuevas marcas de tiempo
- Añada los objetos a la cola de ILM para poder reevaluarlos según las reglas y políticas actuales de ILM

La tabla resume el comportamiento aplicado a todos los objetos del bloque cuando la hora de último acceso está desactivada o habilitada.

Tipo de solicitud	Comportamiento si la hora del último acceso está desactivada (valor predeterminado)		Comportamiento si la hora del último acceso está activada	
	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	No	Sí	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí	Sí	Sí

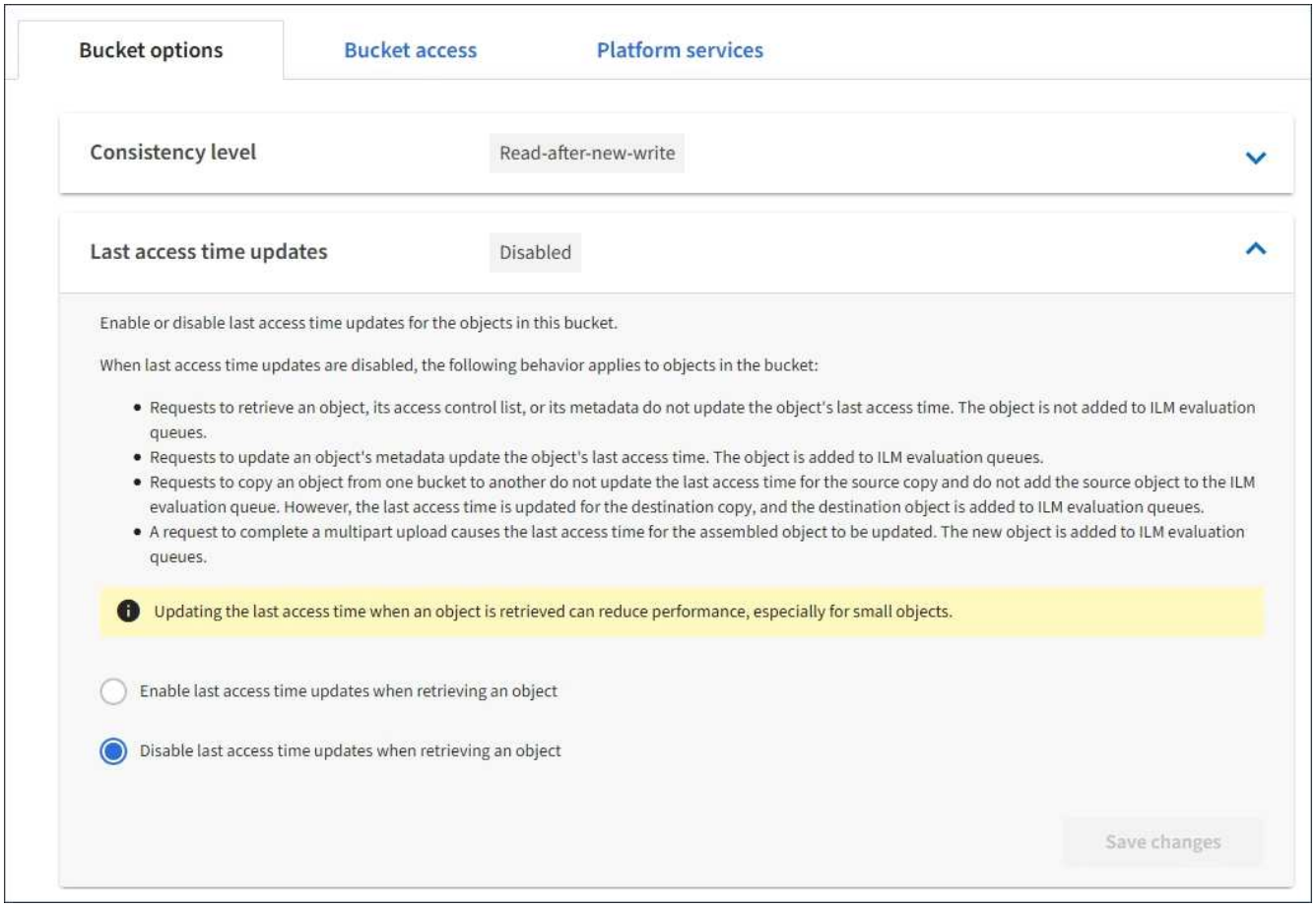
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque** > **actualizaciones del último tiempo de acceso**.
4. Seleccione el botón de opción adecuado para activar o desactivar las actualizaciones de la hora del último acceso.



5. Seleccione **Guardar cambios**.

Información relacionada

"Permisos de gestión de inquilinos"

"Gestión de objetos con ILM"

Configuración de uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bloque de S3 si desea que dicho bloque y los objetos de ese bloque sean accesibles a las aplicaciones web de otros dominios.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite que las aplicaciones web de cliente de un dominio accedan a los recursos de un dominio diferente. Por ejemplo, supongamos que se utiliza un bloque de S3 llamado `Images` para almacenar gráficos. Configurando CORS para `Images` bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web `http://www.example.com`.

Pasos

1. Utilice un editor de texto para crear el XML necesario para habilitar CORS.

   Este ejemplo muestra el XML utilizado para habilitar CORS para un bloque de S3. Este XML permite a cualquier dominio enviar solicitudes GET al bloque, pero sólo permite el `http://www.example.com` Dominio para enviar solicitudes DE PUBLICACIÓN Y ELIMINACIÓN. Se permiten todos los encabezados de las solicitudes.

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

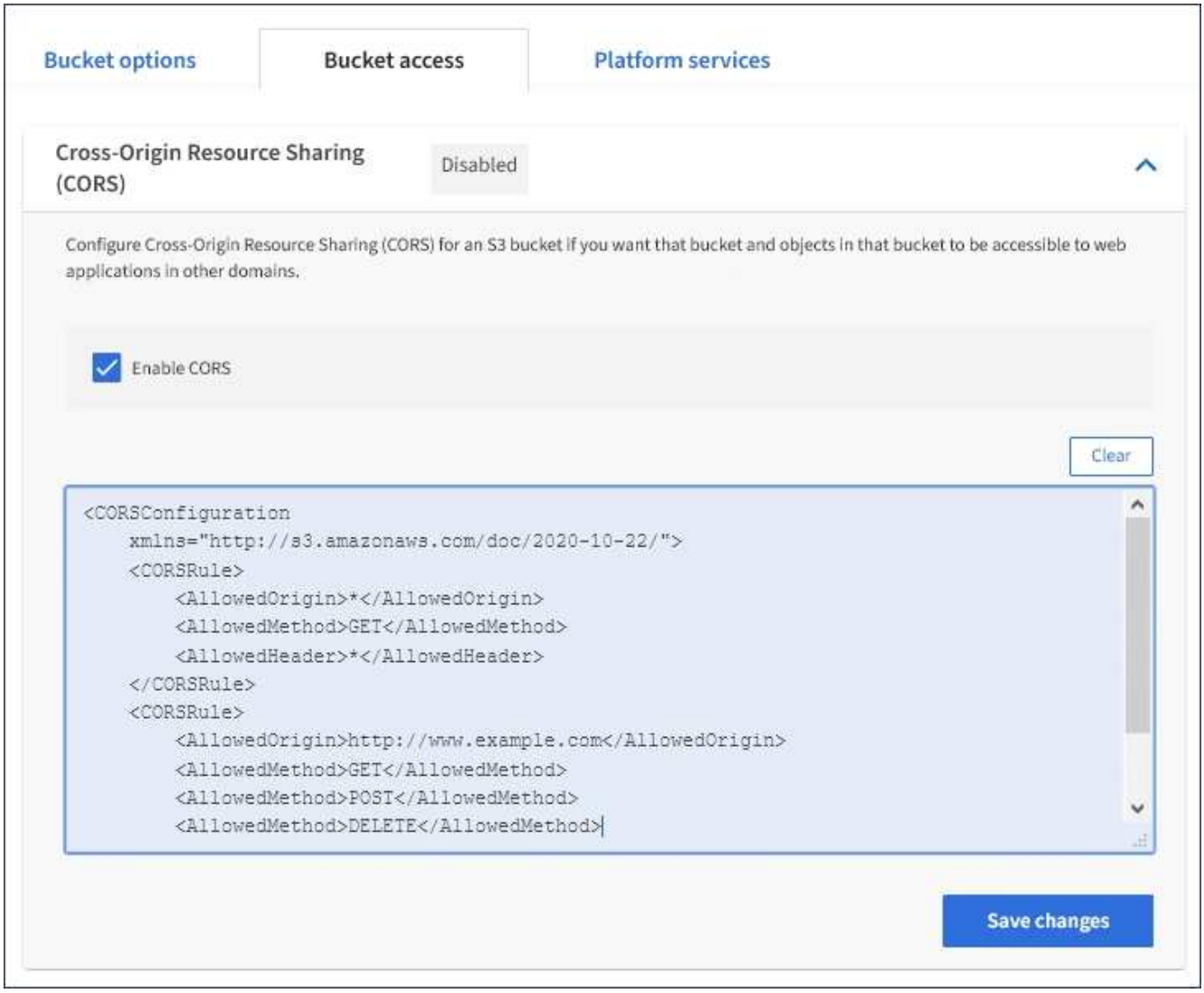
   Para obtener más información acerca del XML de configuración de CORS, consulte "Documentación de Amazon Web Services (AWS): Guía para desarrolladores de Amazon simple Storage Service".

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

3. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

4. Seleccione **acceso a bloque** > **uso compartido de recursos de origen cruzado (CORS)**.
5. Seleccione la casilla de verificación **Activar CORS**.
6. Pegue el XML de configuración de CORS en el cuadro de texto y seleccione **Guardar cambios**.



7. Para modificar la configuración de CORS para el bloque, actualice el XML de configuración de CORS en el cuadro de texto o seleccione **Borrar** para volver a empezar. A continuación, seleccione **Guardar cambios**.
8. Para desactivar CORS para el cucharón, desactive la casilla de verificación **Activar CORS** y, a continuación, seleccione **Guardar cambios**.

Eliminar un bloque de S3

Puede usar el administrador de inquilinos para eliminar un bloque de S3 que esté vacío.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.

- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

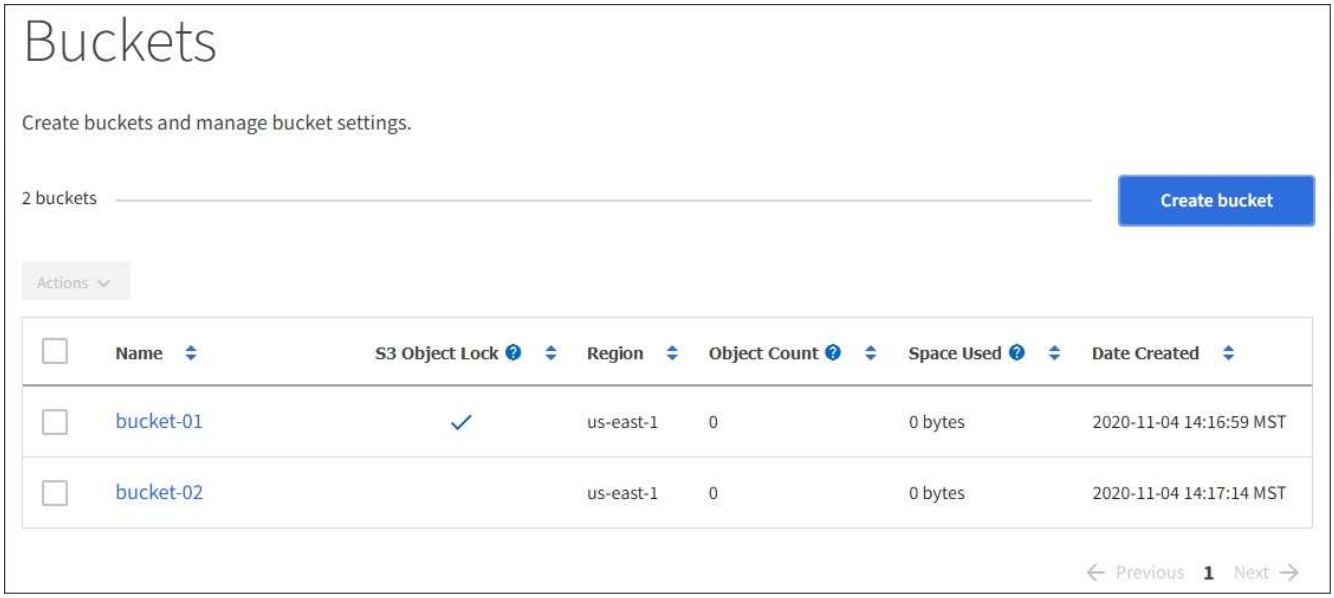
Estas instrucciones describen cómo eliminar un bloque de S3 mediante el administrador de inquilinos. También se pueden eliminar bloques S3 con la API de gestión de inquilinos o la API DE REST de S3.

No puede eliminar un bloque de S3 si contiene objetos o versiones de objetos no actuales. Para obtener información sobre cómo se eliminan los objetos con versiones S3, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

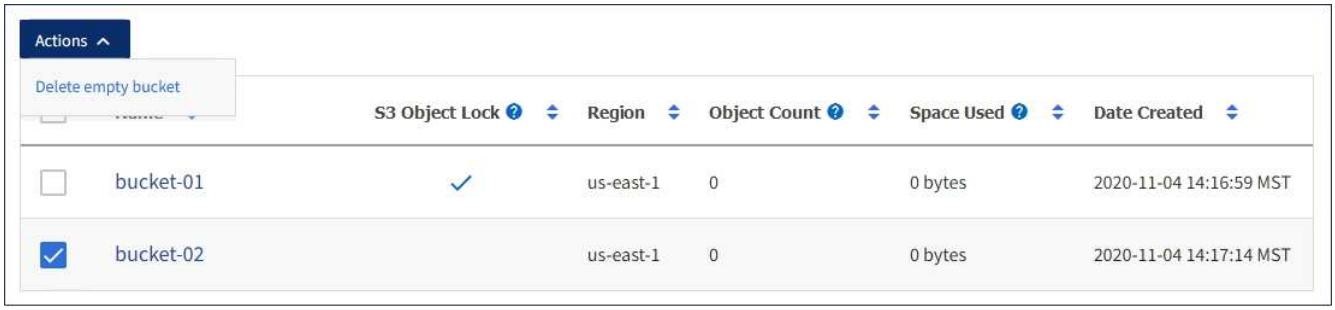
   Aparece la página Buckets y muestra todos los bloques S3 existentes.



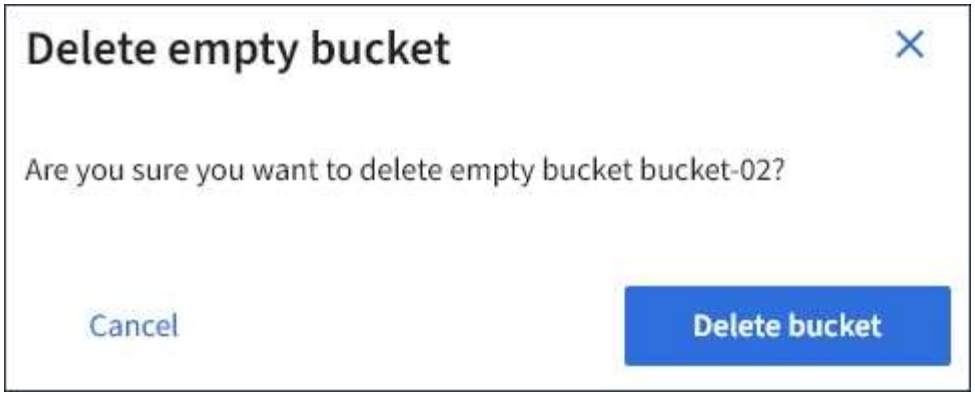
2. Seleccione la casilla de verificación para el segmento vacío que desea eliminar.

   El menú acciones está activado.

3. En el menú acciones, seleccione **Eliminar segmento vacío**.



   Aparecerá un mensaje de confirmación.



4. Si está seguro de que desea eliminar el bloque, seleccione **Eliminar bloque**.

   StorageGRID confirma que el cucharón está vacío y, a continuación, elimina el cucharón. Esta operación puede llevar algunos minutos.

   Si el segmento no está vacío, aparece un mensaje de error. Debe eliminar todos los objetos antes de poder eliminar el bloque.

Información relacionada

"Gestión de objetos con ILM"

Gestión de servicios de plataforma S3

Si se permite el uso de servicios de plataforma para su cuenta de inquilino de S3, podrá usar servicios de plataforma para aprovechar los servicios externos y configurar la replicación de CloudMirror, notificaciones e integración de búsqueda para bloques de S3.

- "¿Qué servicios de plataforma son"
- "Consideraciones sobre el uso de servicios de plataforma"
- "Configuración de extremos de servicios de plataforma"
- "Configurar la replicación de CloudMirror"
- "Configuración de notificaciones de eventos"
- "Utilizando el servicio de integración de búsqueda"

¿Qué servicios de plataforma son

Los servicios de plataforma de StorageGRID pueden ayudarle a implementar una estrategia de cloud híbrido.

Si se permite el uso de servicios de plataforma para su cuenta de inquilino, puede configurar los siguientes servicios para cualquier bloque de S3:

- **Duplicación de CloudMirror**: El servicio de replicación de CloudMirror de StorageGRID se utiliza para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

  Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

  > La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.

- **Notificaciones**: Las notificaciones de eventos por bloque se usan para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon simple Notification Service™ (SNS) externo especificado.

  Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

  > Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

- **Servicio de integración de búsqueda**: El servicio de integración de búsqueda se usa para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos utilizando el servicio externo.

  Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

  > Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Puesto que la ubicación objetivo de los servicios de la plataforma suele ser externa a la puesta en marcha de StorageGRID, los servicios de plataforma le proporcionan la potencia y la flexibilidad que se obtiene al utilizar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bloque de S3. Por ejemplo, podría configurar el servicio CloudMirror y las notificaciones en un bloque de StorageGRID S3 de manera que pueda reflejar objetos específicos en Amazon simple Storage Service, al tiempo que envía una notificación sobre cada objeto de ese tipo a una aplicación de supervisión de terceros para ayudarle a realizar un seguimiento de los gastos de AWS.

> Un administrador de StorageGRID debe habilitar el uso de servicios de plataforma para cada cuenta de inquilino mediante el Administrador de grid o la API de gestión de grid.

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con extremos externos que se configuran mediante el administrador de inquilinos o la API de gestión de inquilinos. Cada extremo representa un destino externo, como un bloque

de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple (SNS) o un clúster de Elasticsearch alojado localmente, en AWS u otros lugares.

Después de crear un extremo, puede habilitar un servicio de plataforma para un bloque agregando la configuración XML al bloque. La configuración XML identifica los objetos en los que debe actuar el bloque, la acción que debe tomar el bloque y el extremo que el bloque debe utilizar para el servicio.

Debe agregar configuraciones XML independientes para cada servicio de plataforma que desee configurar. Por ejemplo:

1. Si desea que todos los objetos con las claves comiencen `/images` Para replicarse en un bloque de Amazon S3, debe añadir una configuración de replicación al bloque de origen.
2. Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
3. Por último, si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsquedas.

El formato de la configuración XML está regido por las API DE REST de S3 que se usan para implementar los servicios de plataforma StorageGRID:

Servicio de plataforma	API REST DE S3
Replicación de CloudMirror	• OBTENGA la replicación de Bucket • PUT Bucket replication
Notificaciones	• OBTENGA la notificación DE BUCKET • NOTIFICACIÓN DE PUT Bucket
Integración de búsqueda	• OBTENGA la configuración de notificación de metadatos del bloque de datos • PUT bucket metadata notification Configuration Estas operaciones están personalizadas en StorageGRID.

Consulte las instrucciones para implementar aplicaciones cliente de S3 para obtener detalles sobre cómo StorageGRID implementa estas API.

Información relacionada

"Use S3"

"El servicio de replicación de CloudMirror"

"Notificaciones para bloques"

"Descripción del servicio de integración de búsqueda"

"Consideraciones sobre el uso de servicios de plataforma"

El servicio de replicación de CloudMirror

Puede habilitar la replicación de CloudMirror para un bloque de S3 si desea que StorageGRID replique los objetos especificados que se añadan al bloque en uno o más bloques de destino.

La replicación de CloudMirror opera con independencia de la política de ILM activa de la cuadrícula. El servicio CloudMirror replica los objetos cuando se almacenan en el bloque de origen y los envía al Lo antes posible. de bloque de destino. La entrega de objetos replicados se activa cuando la ingesta de objetos se realiza correctamente.

Si habilita la replicación de CloudMirror para un bloque existente, solo se replican los nuevos objetos agregados a ese bloque. No se replican ningún objeto existente en el bloque. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente ejecutando una copia de objeto.

> Si va a usar la replicación de CloudMirror para copiar objetos en un destino de AWS S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario en cada encabezado DE solicitud PUT a 2 KB. Si un objeto tiene metadatos definidos por el usuario mayores de 2 KB, ese objeto no se replicará.

En StorageGRID, puede replicar los objetos de un solo bloque en varios bloques de destino. Para ello, especifique el destino de cada regla en el XML de configuración de replicación. No se puede replicar un objeto en más de un bloque a la vez.

Además, puede configurar la replicación de CloudMirror en bloques con versiones o sin versiones, y puede especificar un bloque con versiones o sin versiones como destino. Puede utilizar cualquier combinación de cubos con versiones y sin versiones. Por ejemplo, puede especificar un bloque con versiones como destino para un bloque de origen sin versiones o viceversa. También puede replicar entre cubos sin versiones.

El comportamiento de eliminación del servicio de replicación CloudMirror es el mismo que el comportamiento de eliminación del servicio de replicación entre regiones (CRR) proporcionado por Amazon S3 — al eliminar un objeto de un bloque de origen nunca se elimina un objeto replicado en el destino. Si se van a crear versiones de los cubos de origen y de destino, se replica el marcador de borrado. Si el bloque de destino no tiene versiones, al eliminar un objeto del bloque de origen no se replicará el marcador DELETE en el bloque de destino ni se eliminará el objeto de destino.

A medida que los objetos se replican en el segmento de destino, StorageGRID los Marca como «réplicas». Un bloque StorageGRID de destino no replicará objetos marcados como réplicas de nuevo, lo que le protegerá de bucles de replicación accidentales. Este marcado de réplica es interno en StorageGRID y no le impide utilizar AWS CRR cuando se utiliza un bloque de Amazon S3 como destino.

> El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica`. Esta Marca evita una duplicación en cascada. StorageGRID admite un CloudMirror bidireccional entre dos grids.

La singularidad y el orden de los eventos en el segmento de destino no están garantizados. Puede que más de una copia idéntica de un objeto de origen se proporcione en el destino como resultado de las operaciones realizadas para garantizar un éxito en la entrega. En raras ocasiones, cuando se actualiza el mismo objeto de forma simultánea desde dos o más sitios StorageGRID distintos, es posible que la ordenación de las operaciones en el bloque de destino no coincida con la ordenación de eventos en el bloque de origen.

La replicación de CloudMirror suele configurarse para utilizar un bloque de S3 externo como destino. Sin embargo, también puede configurar la replicación para que utilice otra implementación de StorageGRID o

cualquier servicio compatible con S3.

Información relacionada

"Configurar la replicación de CloudMirror"

Notificaciones para bloques

Es posible habilitar la notificación de eventos para un bloque de S3 si desea que StorageGRID envíe notificaciones sobre eventos especificados a un servicio de notificación simple (SNS) de destino.

Puede configurar las notificaciones de eventos asociando XML de configuración de notificaciones a un bloque de origen. El XML de configuración de notificaciones sigue las convenciones de S3 para configurar las notificaciones de bloques, con el tema SNS de destino especificado como URN de un extremo.

Las notificaciones de eventos se crean en el bloque de origen tal y como se especifica en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto se realiza correctamente, se crea una notificación sobre ese evento y se pone en cola para su entrega.

La singularidad y el orden de las notificaciones no están garantizados. Como resultado de las operaciones realizadas para garantizar el éxito en la entrega, se podría enviar más de una notificación de un evento al destino. Además, como la entrega es asíncrona, no se garantiza que la ordenación del tiempo de las notificaciones en el destino coincida con la ordenación de eventos del bloque de origen, especialmente en las operaciones que se originan en diferentes sitios de StorageGRID. Puede utilizar el `sequencer` Introduzca el mensaje de evento para determinar el orden de los eventos de un objeto determinado, como se describe en la documentación de Amazon S3.

Notificaciones y mensajes compatibles

Las notificaciones de eventos de StorageGRID siguen la API de Amazon S3 con las siguientes limitaciones:

- No es posible configurar una notificación para los siguientes tipos de eventos. Estos tipos de evento **no** son compatibles.
  - `s3:ReducedRedundancyLostObject`
  - `s3:ObjectRestore:Completed`
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en la tabla:

Nombre de clave	Valor de StorageGRID
EventSource	`sgws:s3`
AwsRegion	no incluido
x-amz-id-2	no incluido
arn	`urn:sgws:s3:::bucket_name`

Información relacionada

"Configuración de notificaciones de eventos"

Descripción del servicio de integración de búsqueda

Puede habilitar la integración de búsqueda para un bloque de S3 si desea usar un servicio de búsqueda y análisis de datos externo para sus metadatos de objetos.

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asíncrona los metadatos de objetos de S3 a un extremo de destino cada vez que se actualiza un objeto o sus metadatos. A continuación, puede usar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático que proporciona el servicio de destino para buscar, analizar y obtener información de sus datos de objetos.

Puede activar el servicio de integración de búsqueda para cualquier bloque con versiones o sin versiones. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos al bloque que especifica los objetos en los que actuar y el destino de los metadatos del objeto.

Las notificaciones se generan en forma de un documento JSON denominado con el nombre del bloque, el nombre del objeto y el ID de versión, si los hubiera. Cada notificación de metadatos contiene un conjunto estándar de metadatos del sistema para el objeto, además de todas las etiquetas del objeto y los metadatos del usuario.

> Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indizado un documento, no se pueden editar los tipos de campo del documento en el índice.

Las notificaciones se generan y se ponen en cola para su entrega siempre que:

- Se crea un objeto.
- Se elimina un objeto, incluso cuando se eliminan objetos como resultado del funcionamiento de la política de ILM de la cuadrícula.
- Los metadatos o las etiquetas de los objetos son añadidos, actualizados o eliminados. El conjunto completo de metadatos y etiquetas se envía siempre al momento de la actualización, no sólo los valores modificados.

Después de agregar XML de configuración de notificación de metadatos a un bloque, se envían notificaciones para los objetos nuevos que cree y para los objetos que modifique mediante la actualización de sus datos, metadatos de usuario o etiquetas. Sin embargo, las notificaciones no se envían para ningún objeto que ya estaba en el bloque. Para garantizar que los metadatos de objeto de todos los objetos del bloque se envíen al destino, debe realizar una de las siguientes acciones:

- Configure el servicio de integración de búsqueda inmediatamente después de crear el bloque y antes de agregar ningún objeto.
- Realice una acción en todos los objetos que ya están en el bloque que activará un mensaje de notificación de metadatos que se enviará al destino.

El servicio de integración de búsqueda StorageGRID admite un clúster de Elasticsearch como destino. Al igual que con los demás servicios de plataforma, el destino se especifica en el extremo cuyo URN se utiliza en el XML de configuración del servicio. Utilice *Interoperability Matrix Tool* para determinar las versiones compatibles de Elasticsearch.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

"XML de configuración para la integración de búsqueda"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configurar el servicio de integración de búsqueda"

Consideraciones sobre el uso de servicios de plataforma

Antes de implementar los servicios de la plataforma, revise las recomendaciones y consideraciones sobre el uso de estos servicios.

Consideraciones sobre el uso de servicios de plataforma

Consideración	Detalles
Supervisión del extremo de destino	Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo.
Limitación de punto final de destino	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.

Consideración	Detalles
Solicitud de garantías	StorageGRID garantiza la realización de pedidos de operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se encuentren en el mismo sitio, el estado del objeto final (para replicación) será siempre igual al estado en StorageGRID. StorageGRID hace todo un esfuerzo por intentar solicitar solicitudes cuando se realizan operaciones en todos los sitios de StorageGRID. Por ejemplo, si escribe un objeto inicialmente en el sitio A y después sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el bloque de destino sea el más nuevo.
Eliminaciones de objetos condicionados por ILM	Para que coincida con el comportamiento de eliminación de los servicios CRR y SNS de AWS, las solicitudes de notificación de CloudMirror y eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de ILM de StorageGRID. Por ejemplo, no se envían solicitudes de notificaciones de eventos o CloudMirror si una regla de ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.

Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite el `x-amz-replication-status` encabezado.
Tamaño del objeto	El tamaño máximo de los objetos que se pueden replicar en un bloque de destino mediante el servicio de replicación de CloudMirror es 5 TB, que es el mismo que el tamaño máximo de objeto admitido por StorageGRID.
Versiones de bloques e ID de versión	Si el bloque de S3 de origen de StorageGRID tiene habilitado el control de versiones, también debe habilitar el control de versiones para el bloque de destino. Al usar el control de versiones, tenga en cuenta que el orden de las versiones de objetos en el bloque de destino es el mejor esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. **Nota**: Los ID de versión para el cucharón de origen en StorageGRID no están relacionados con los ID de versión para el cubo de destino.

Etiquetado para versiones de objetos	El servicio CloudMirror no replica ninguna solicitud DE etiquetado de objetos PUT ni ELIMINA solicitudes de etiquetado de objetos que proporcionen un ID de versión, debido a las limitaciones en el protocolo S3. Como los ID de versión del origen y del destino no están relacionados, no hay manera de garantizar que se replique una actualización de etiqueta a un ID de versión específico. Por el contrario, el servicio CloudMirror replica las solicitudes DE etiquetado PUT Object o ELIMINA las solicitudes de etiquetado de objetos que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).
Cargas en varias partes y. `ETag` valores	Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el `ETag` el valor del objeto reflejado será diferente al `ETag` valor del objeto original.
Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta procesar un objeto en el bloque de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud de SSE-C, se produce un error en la operación.
Bloque con S3 Object Lock habilitado	Si el bloque de destino S3 para la replicación de CloudMirror tiene la función S3 Object Lock habilitada, la operación de replicación generará un error ACCESSDENIED.

Información relacionada

"Use S3"

Configuración de extremos de servicios de plataforma

Para poder configurar un servicio de plataforma para un bloque, debe configurar al menos un extremo para que sea el destino del servicio de plataforma.

El acceso a servicios de la plataforma está habilitado por inquilino por un administrador de StorageGRID. Para crear o utilizar un extremo de servicios de plataforma, debe ser un usuario inquilino con permiso Administrar extremos o acceso raíz, en una cuadrícula cuya red se haya configurado para permitir que los nodos de almacenamiento accedan a recursos de extremo externos. Si desea obtener más información, póngase en contacto con el administrador de StorageGRID.

Qué es un extremo de servicios de plataforma

Al crear un extremo de servicios de plataforma, se especifica la información que StorageGRID necesita para acceder al destino externo.

Por ejemplo, si desea replicar objetos de un bloque de StorageGRID a un bloque de S3, debe crear un extremo de servicios de plataforma que incluya la información y las credenciales que StorageGRID necesita para acceder al bloque de destino en AWS.

Cada tipo de servicio de plataforma requiere su propio extremo, por lo que debe configurar al menos un extremo para cada servicio de plataforma que tenga previsto utilizar. Después de definir un extremo de servicios de plataforma, se utiliza URN del extremo como destino en el XML de configuración utilizado para habilitar el servicio.

Puede utilizar el mismo extremo que el destino para más de un bloque de origen. Por ejemplo, se pueden configurar varios bloques de origen para que envíen metadatos de objetos al mismo extremo de integración de búsqueda, de modo que se puedan realizar búsquedas en varios bloques. También es posible configurar un bloque de origen para que use más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de SNS y notificaciones sobre la eliminación de objetos a un segundo tema SNS.

Extremos para la replicación de CloudMirror

StorageGRID admite extremos de replicación que representan bloques de S3. Estos bloques se pueden alojar en Amazon Web Services, la misma puesta en marcha de StorageGRID remota o en otro servicio.

Extremos para notificaciones

StorageGRID admite los extremos del servicio de notificación simple (SNS). No se admiten extremos de AWS Lambda o simple Queue Service (SQS).

Extremos del servicio de integración de búsqueda

StorageGRID admite extremos de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o en los clouds de AWS u otros lugares.

El extremo de integración de búsqueda hace referencia a un índice y un tipo específicos de Elasticsearch. Debe crear el índice en Elasticsearch antes de crear el extremo en StorageGRID o se producirá un error en la creación del extremo. No es necesario crear el tipo antes de crear el extremo. StorageGRID creará el tipo si es necesario al enviar metadatos de objetos al extremo.

Información relacionada

"Administre StorageGRID"

Se especifica el URN para un extremo de servicios de plataforma

Al crear un extremo de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará el URN para hacer referencia al extremo cuando cree XML de configuración para el servicio de plataforma. El URN de cada extremo debe ser único.

StorageGRID valida los extremos de los servicios de la plataforma a medida que se crean. Antes de crear un extremo de servicios de plataforma, confirme que el recurso especificado en el extremo existe y que se puede alcanzar.

URN elementos

El URN de un extremo de servicios de plataforma debe comenzar con cualquiera de los dos `arn:aws` o. `urn:mysite`, como se indica a continuación:

- Si el servicio está alojado en AWS, utilice `arn:aws`.
- Si el servicio se aloja localmente, utilice `urn:mysite`

Por ejemplo, si especifica el URN para un extremo de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws`.

El siguiente elemento de URN especifica el tipo de servicio de plataforma, como se indica a continuación:

Servicio	Tipo
Replicación de CloudMirror	s3
Notificaciones	sns
Integración de búsqueda	es

Por ejemplo, para seguir especificando URN para un extremo de CloudMirror alojado en StorageGRID, debería añadir `s3` para conseguirlo `urn:sgws:s3`.

El elemento final del URN identifica el recurso de destino específico en el URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	nombre del bloque
Notificaciones	sns-topic-name
Integración de búsqueda	`domain-name/index-name/type-name` **Nota:** Si el clúster Elasticsearch está **no** configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

Urnas para servicios alojados en AWS

Para entidades AWS, el URN completo es un ARN válido de AWS. Por ejemplo:

- Replicación de CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificaciones:

```
arn:aws:sns:region:account-id:topic-name
```

- Integración de búsqueda:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Para un extremo de integración de búsqueda de AWS, la `domain-name` debe incluir la cadena literal `domain/`, como se muestra aquí.

Servicios alojados localmente

Al usar servicios alojados localmente en lugar de servicios de cloud, puede especificar el URN de cualquier forma que cree una URN válida y única, siempre y cuando URN incluya los elementos necesarios en la tercera y última posición. Puede dejar los elementos indicados por opcional en blanco o puede especificarlos de cualquier forma que le ayude a identificar el recurso y hacer que el URN sea único. Por ejemplo:

- Replicación de CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

En el caso de un extremo de CloudMirror alojado en StorageGRID, es posible especificar una URN válida que comience por `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificaciones:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- Integración de búsqueda:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> Para los extremos de integración de búsqueda alojados localmente, el `domain-name` Element puede ser cualquier cadena siempre que el URN del extremo sea único.

Creación de un extremo de servicios de plataforma

Debe crear al menos un extremo del tipo correcto para poder habilitar un servicio de plataforma.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.
- Se debe haber creado el recurso al que hace referencia el extremo de servicios de la plataforma:
  - Replicación de CloudMirror: Bloque de S3
  - Notificación de eventos: Tema SNS
  - Notificación de búsqueda: Índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Debe tener la información sobre el recurso de destino:
  - Host y puerto para el Identificador uniforme de recursos (URI)

    Si piensa utilizar un bloque alojado en un sistema StorageGRID como extremo para la replicación de CloudMirror, póngase en contacto con el administrador de grid para determinar los valores que debe introducir.

  - Nombre del recurso único (URN)

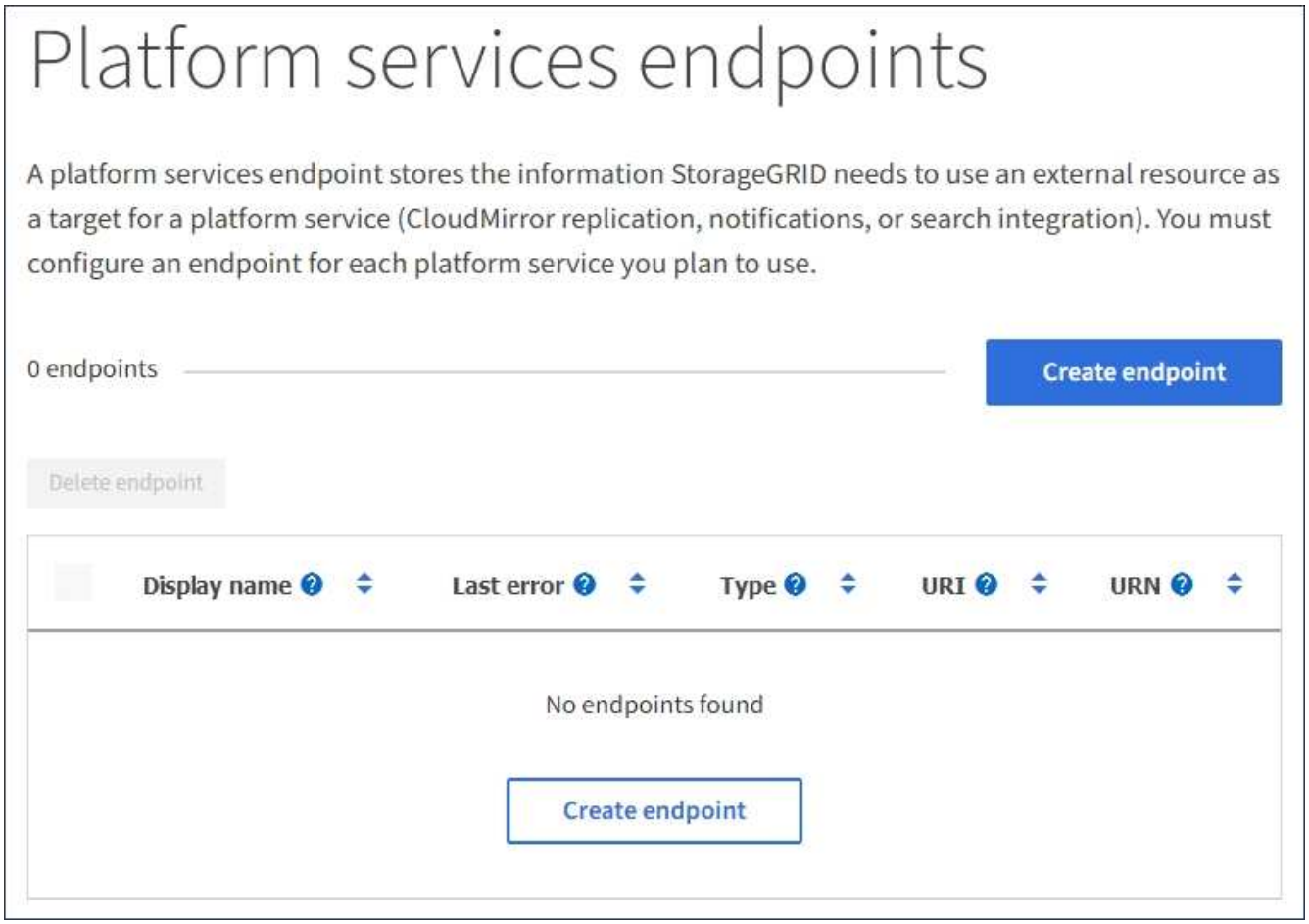
    "Se especifica el URN para un extremo de servicios de plataforma"

  - Credenciales de autenticación (si es necesario):
    - Clave de acceso: ID de clave de acceso y clave de acceso secreta
    - Basic HTTP: Nombre de usuario y contraseña
  - Certificado de seguridad (si se utiliza un certificado de CA personalizado)

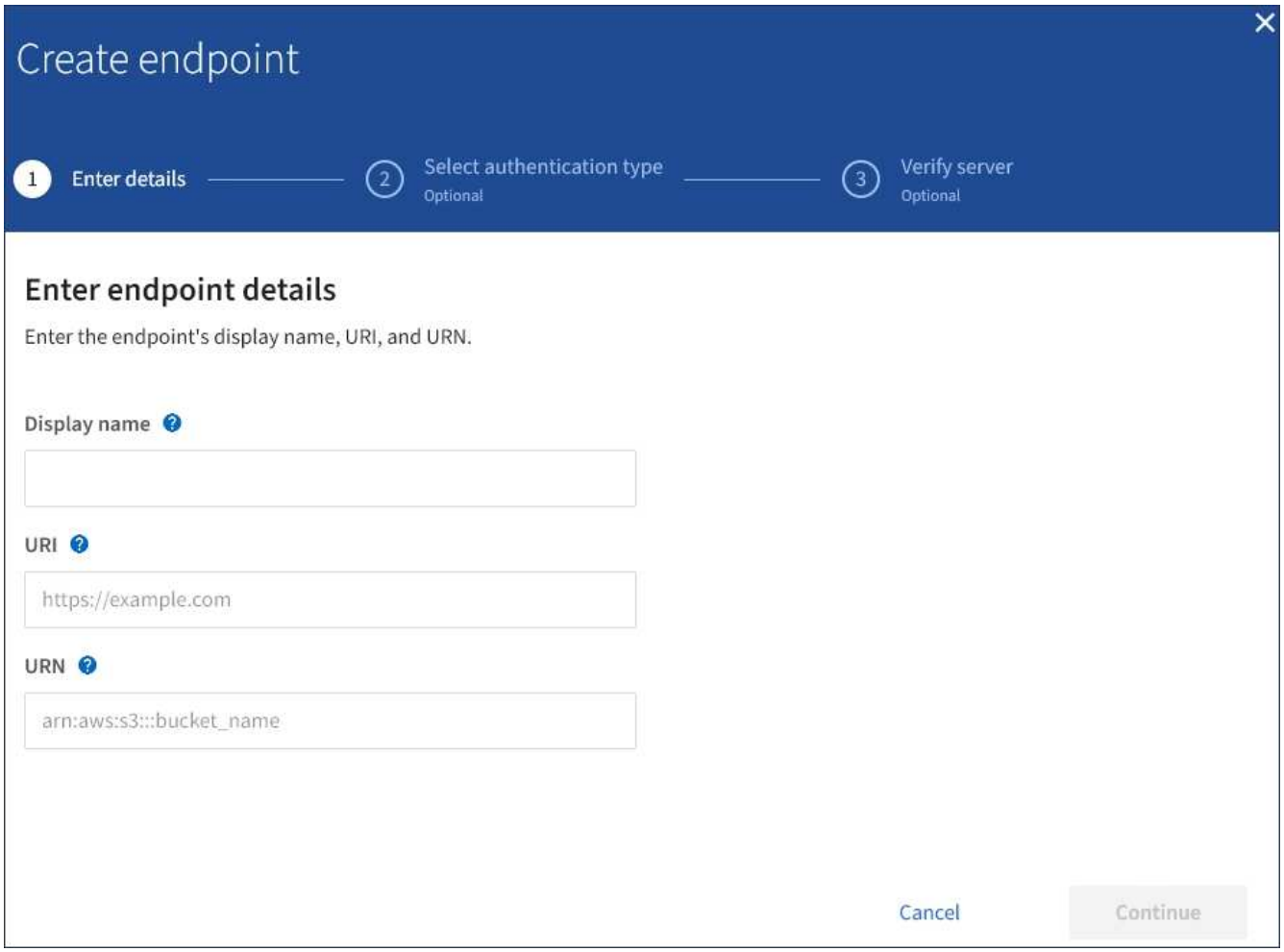
Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma.



2. Seleccione **Crear punto final**.



3. Introduzca un nombre para mostrar para describir brevemente el extremo y su propósito.

   El tipo de servicio de plataforma que admite el extremo se muestra junto al nombre del extremo cuando se muestra en la página de extremos, por lo que no es necesario incluir esa información en el nombre.

4. En el campo **URI**, especifique el Identificador de recursos único (URI) del extremo.

   Utilice uno de los siguientes formatos:

   ```
   https://host:port
   http://host:port
   ```

   Si no especifica un puerto, el puerto 443 se utiliza para los URI HTTPS y el puerto 80 se utiliza para los URI HTTP.

   Por ejemplo, el URI para un bloque alojado en StorageGRID podría ser:

   ```
   https://s3.example.com:10443
   ```

   En este ejemplo: `s3.example.com` Representa la entrada DNS para la IP virtual (VIP) del grupo de alta disponibilidad (ha) de StorageGRID, y. `10443` representa el puerto definido en el extremo del equilibrador

de carga.

> Siempre que sea posible, debe conectarse a un grupo de alta disponibilidad de nodos de equilibrio de carga para evitar un único punto de error.

Del mismo modo, el URI para un bloque alojado en AWS podría ser:

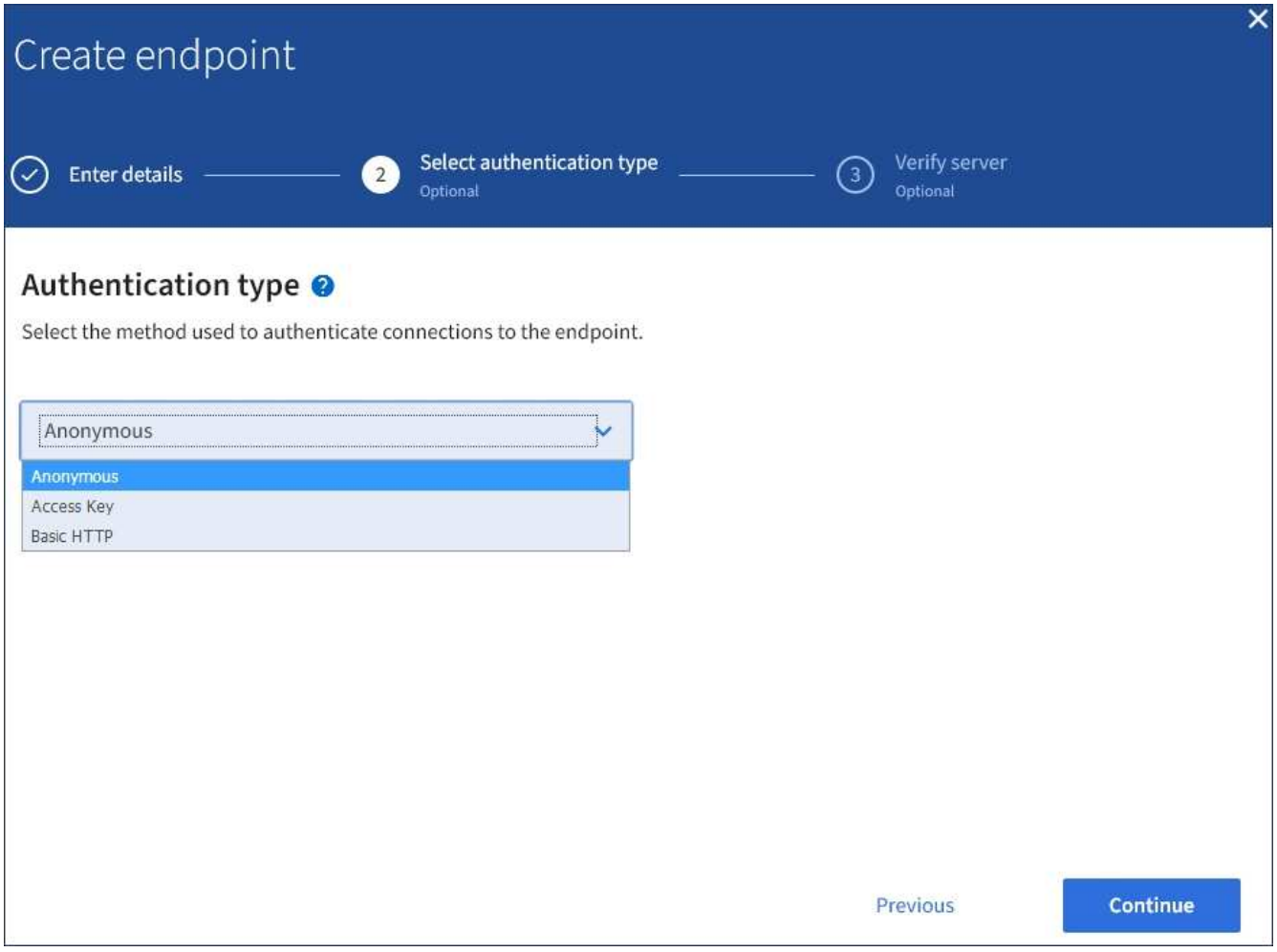
```
https://s3-aws-region.amazonaws.com
```

> Si se utiliza el extremo para el servicio de replicación de CloudMirror, no incluya el nombre de bloque en el URI. Incluye el nombre de bloque en el campo **URN**.

5. Introduzca el nombre de recurso único (URN) para el extremo.

> No es posible cambiar el URN de un extremo una vez que se creó el extremo.

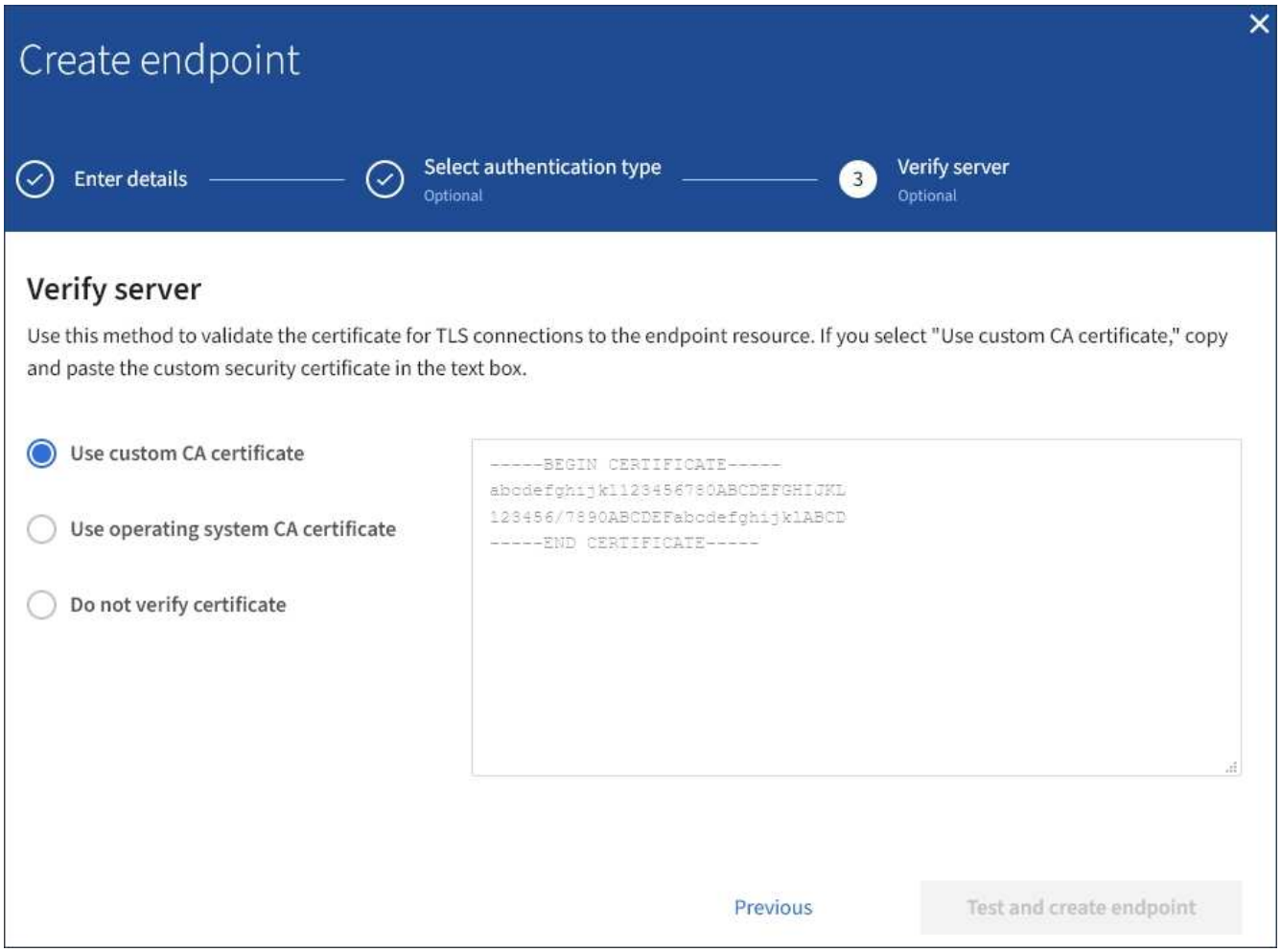
6. Seleccione **continuar**.
7. Seleccione un valor para **Tipo de autenticación** y, a continuación, introduzca las credenciales necesarias.



Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña

8. Seleccione **continuar**.
9. Seleccione un botón de opción para **verificar servidor** para elegir cómo se verifica la conexión TLS con el extremo.



Tipo de verificación del certificado	Descripción
Utilizar certificado de CA personalizado	Usar un certificado de seguridad personalizado. Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto **Certificado CA**.
Utilizar certificado de CA del sistema operativo	Utilice el certificado de CA predeterminado instalado en el sistema operativo para asegurar las conexiones.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica. Esta opción no es segura.

10. Seleccione **probar y crear punto final**.
    - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
    - Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el punto final para corregir el error, seleccione **Volver a los detalles del punto final** y actualice la información. A continuación, seleccione **probar y crear punto final**.

> Se produce un error en la creación de extremos si los servicios de plataforma no están habilitados para su cuenta de inquilino. Póngase en contacto con el administrador de StorageGRID.

Una vez que haya configurado un extremo, puede utilizar su URN para configurar un servicio de plataforma.

Información relacionada

"Se especifica el URN para un extremo de servicios de plataforma"

"Configurar la replicación de CloudMirror"

"Configuración de notificaciones de eventos"

"Configurar el servicio de integración de búsqueda"

Comprobación de la conexión para un extremo de servicios de plataforma

Si la conexión a un servicio de plataforma ha cambiado, puede probar la conexión del extremo para validar que el recurso de destino existe y que se puede acceder a él utilizando las credenciales especificadas.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.

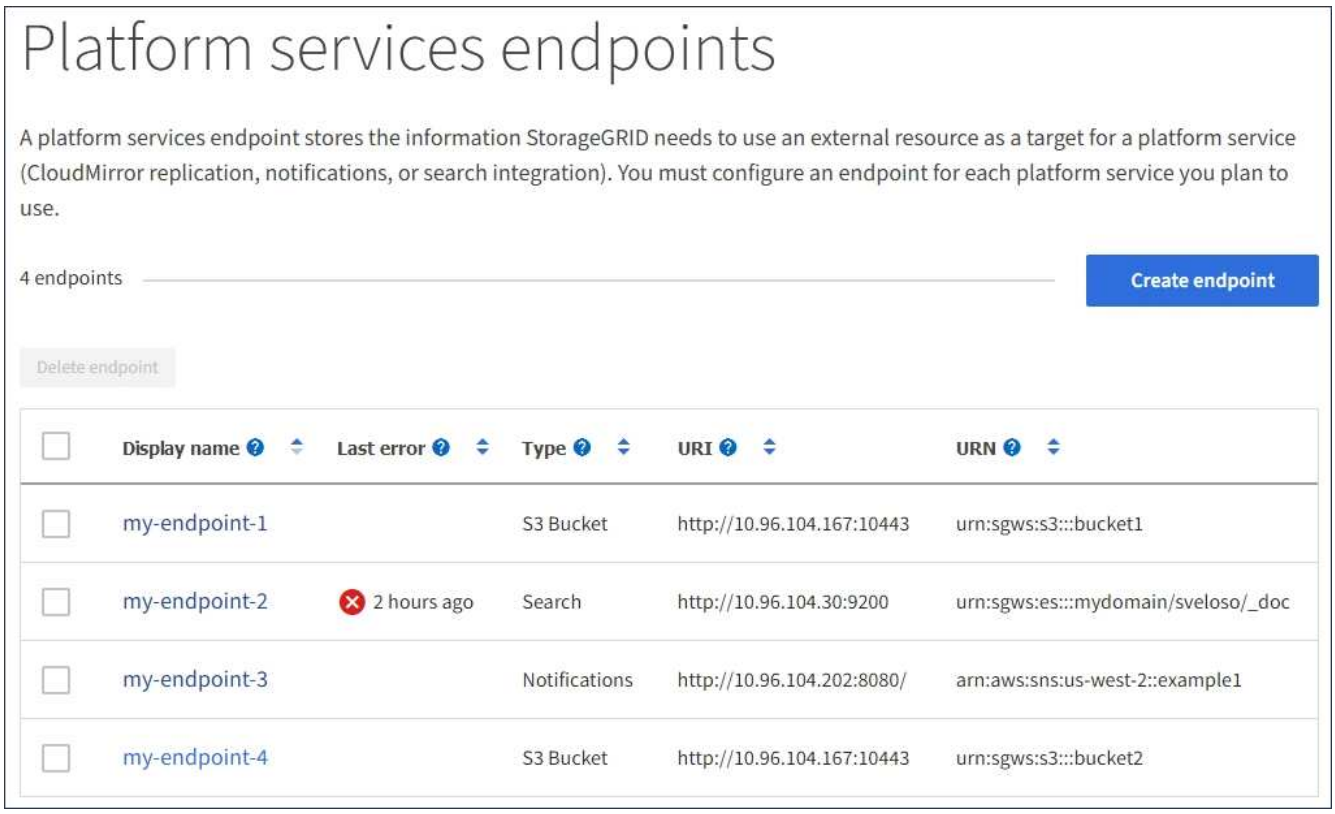
Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

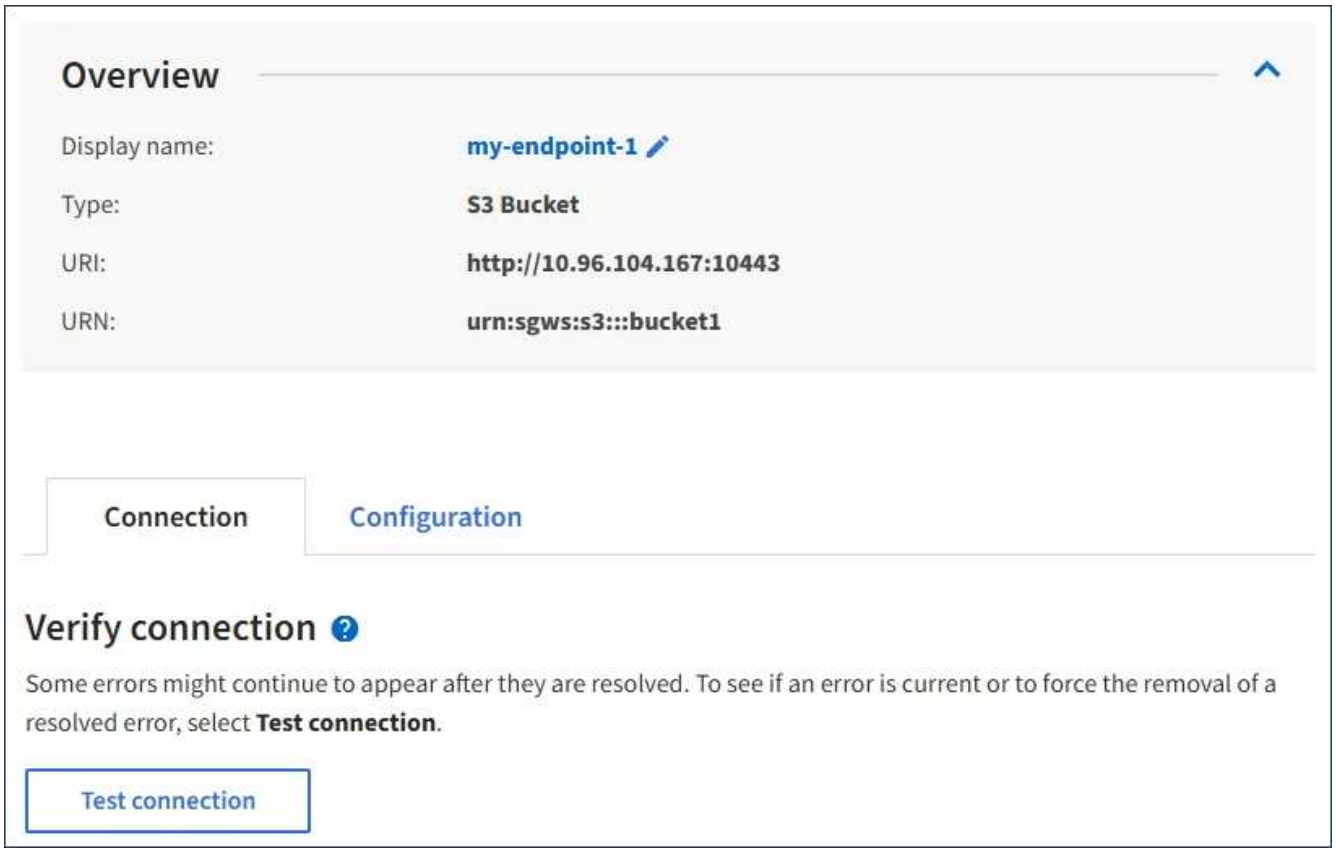
1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.



2. Seleccione el extremo cuya conexión desea probar.

   Aparece la página de detalles del extremo.



3. Seleccione **probar conexión**.
   - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
   - Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el extremo para corregir el error, seleccione **Configuración** y actualice la información. A continuación, seleccione **probar y guardar los cambios**.

Edición de un extremo de servicios de plataforma

Puede editar la configuración de un extremo de servicios de plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que deba actualizar las credenciales caducadas o cambiar el URI para apuntar a un índice de Elasticsearch de backup para la conmutación por error. No se puede cambiar el URN de un extremo de servicios de plataforma.

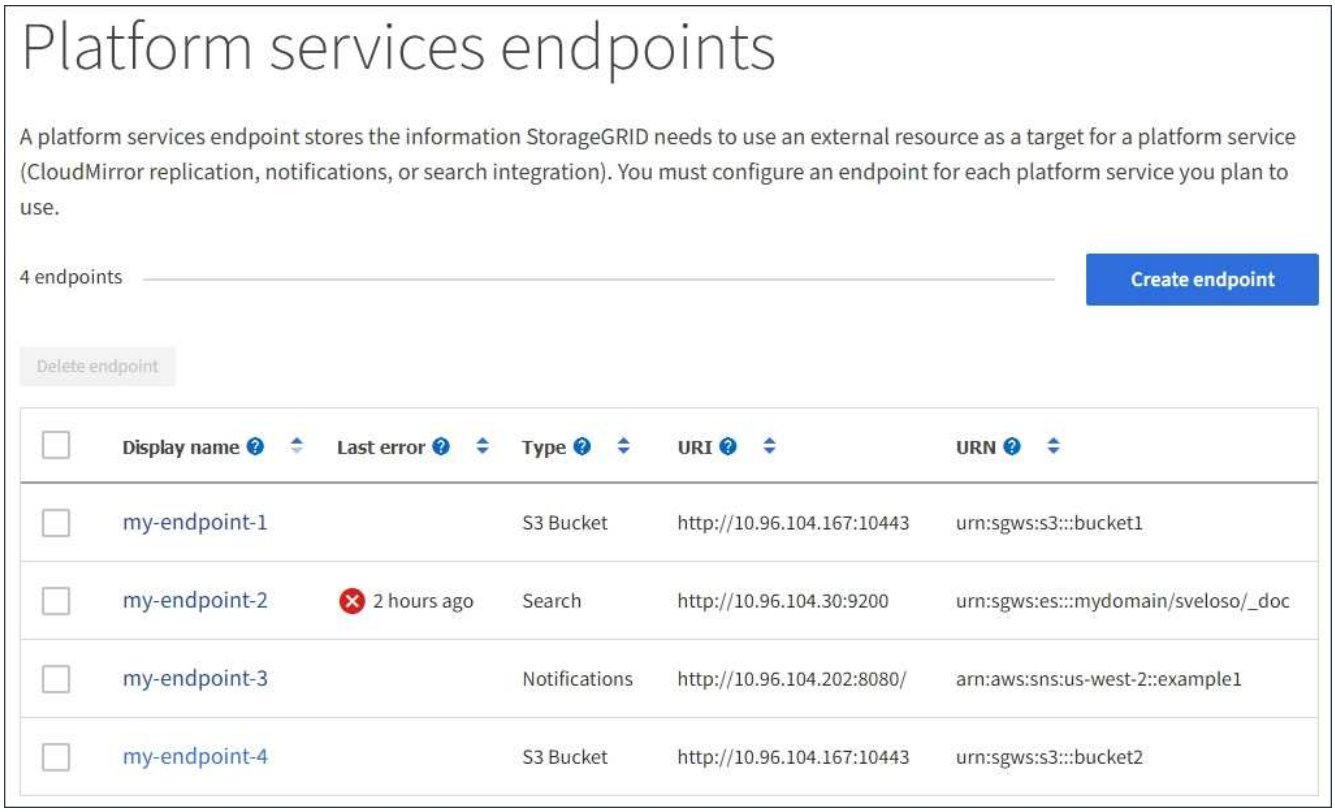
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

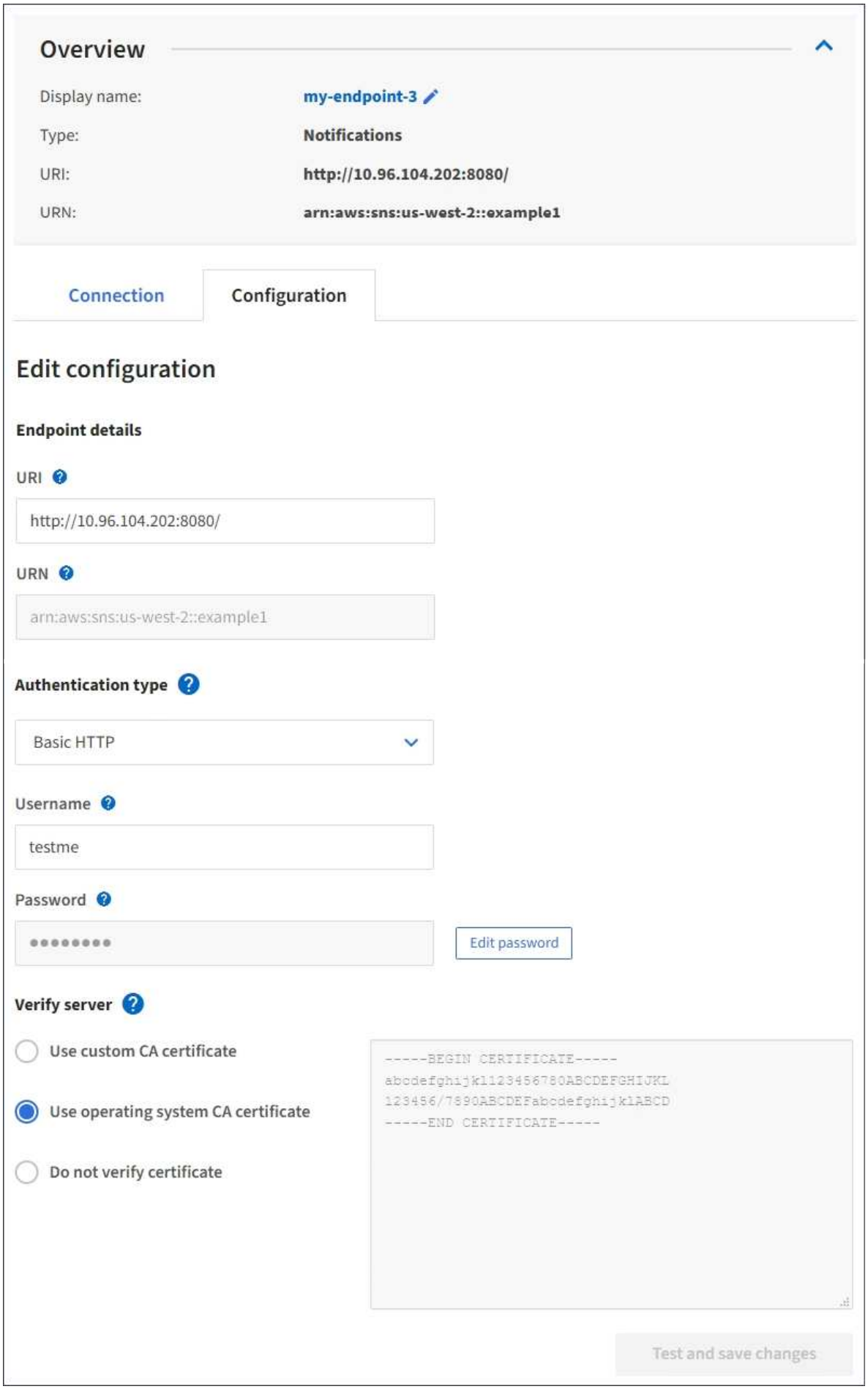
   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.



2. Seleccione el extremo que desea editar.

   Aparece la página de detalles del extremo.

3. Seleccione **Configuración**.


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. Según sea necesario, cambie la configuración del extremo.

   > No es posible cambiar el URN de un extremo una vez que se creó el extremo.

   a. Para cambiar el nombre para mostrar del extremo, seleccione el icono de edición .
   b. Según sea necesario, cambie el URI.
   c. Según sea necesario, cambie el tipo de autenticación.
      - Para la autenticación HTTP básica, cambie el nombre de usuario según sea necesario. Cambie la contraseña según sea necesario; para ello, seleccione **Editar contraseña** e introduzca la nueva contraseña. Si necesita cancelar los cambios, seleccione **Revert password EDIT**.
      - Para la autenticación de la clave de acceso, cambie la clave según sea necesario seleccionando **Editar clave S3** y pegando un nuevo ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar los cambios, seleccione **Revert S3 key EDIT**.
   d. Según sea necesario, cambie el método para verificar el servidor.
5. Seleccione **probar y guardar los cambios**.
   - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión al extremo se verifica desde un nodo en cada sitio.
   - Aparece un mensaje de error si se produce un error en la validación del extremo. Modifique el extremo para corregir el error y, a continuación, seleccione **probar y guardar los cambios**.

Información relacionada

"Creación de un extremo de servicios de plataforma"

Eliminación de un extremo de servicios de plataforma

Puede eliminar un extremo si ya no desea utilizar el servicio de plataforma asociado.

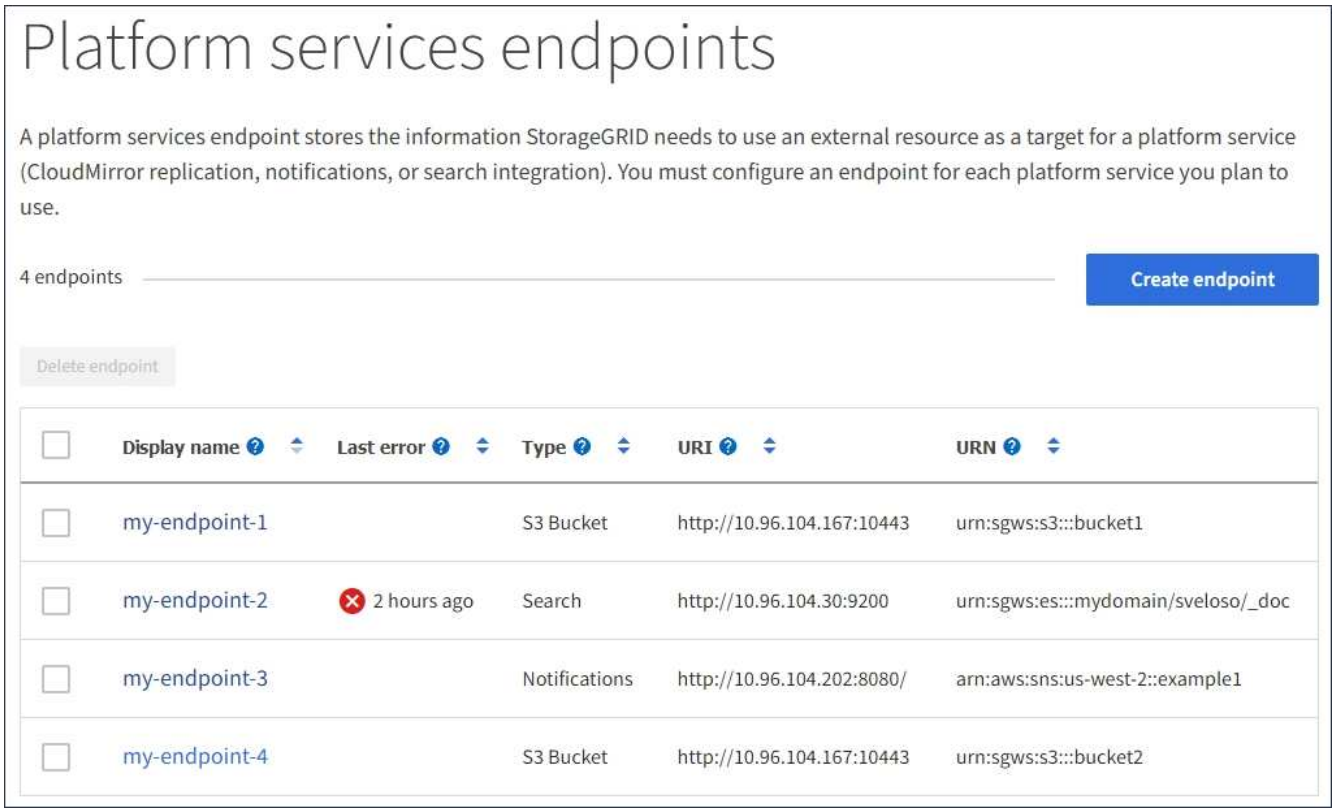
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso **Administrar endpoints**.

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.

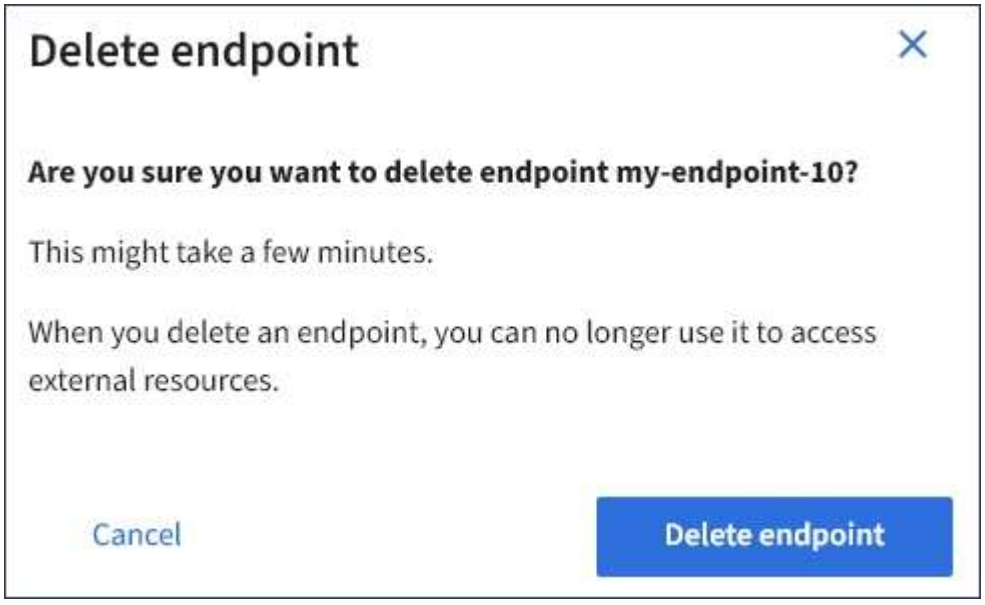


2. Seleccione la casilla de comprobación de cada extremo que desea eliminar.

> Si elimina un extremo de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para todos los bloques que utilicen el extremo. Se descartarán las solicitudes que aún no se hayan completado. Se continuarán generando todas las solicitudes nuevas hasta que cambie la configuración de bloque para que ya no haga referencia a URN eliminado. StorageGRID informará de estas solicitudes como errores irrecuperables.

3. Seleccione **acciones** > **Eliminar punto final**.

   Aparecerá un mensaje de confirmación.



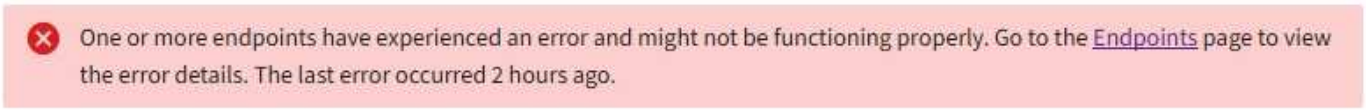
4. Seleccione **Eliminar punto final**.

Resolución de problemas de errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un extremo de servicios de plataforma, se muestra un mensaje en el Panel de control. En la página Platform Services Endpoints, la columna Last error indica durante cuánto tiempo se produjo el error. No se muestra ningún error si los permisos asociados con las credenciales de un extremo son incorrectos.

Determinar si se ha producido un error

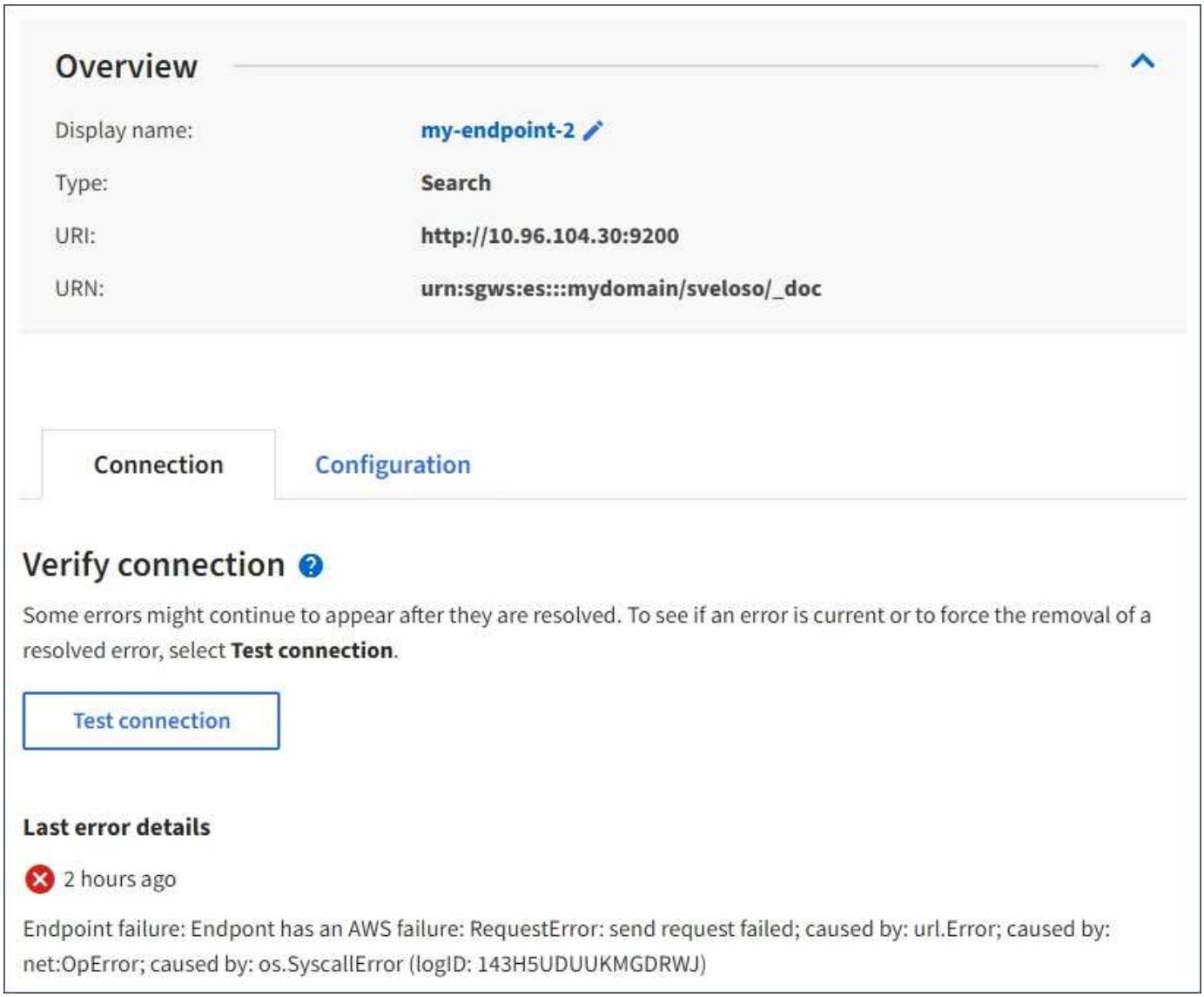
Si se han producido errores de extremo de servicios de plataforma en los últimos 7 días, la consola del administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.



El mismo error que aparece en el panel también aparece en la parte superior de la página de extremos de servicios de plataforma. Para ver un mensaje de error más detallado:

Pasos

1. En la lista de puntos finales, seleccione el extremo que tiene el error.
2. En la página de detalles del punto final, seleccione **Conexión**. Esta pestaña muestra sólo el error más reciente de un punto final e indica cuánto tiempo se produjo el error. Errores que incluyen el icono X rojo ocurrió en los últimos 7 días.



Comprobando si un error sigue estando actualizado

Es posible que algunos errores sigan apareciendo en la columna **último error** incluso después de que se hayan resuelto. Para ver si un error es actual o para forzar la eliminación de un error resuelto de la tabla:

Pasos

1. Seleccione el extremo.

   Aparece la página de detalles del extremo.

2. Seleccione **Conexión** > **probar conexión**.

Al seleccionar **probar conexión**, StorageGRID valida que el extremo de servicios de la plataforma existe y que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

Resolución de errores de punto final

Puede utilizar el mensaje **último error** de la página de detalles del punto final para ayudar a determinar qué está causando el error. Es posible que algunos errores requieran que edite el extremo para resolver el problema. Por ejemplo, se puede producir un error CloudMirroring si StorageGRID no puede acceder al

bloque de S3 de destino porque no tiene los permisos de acceso correctos o si la clave de acceso ha caducado. El mensaje es "'es necesario actualizar las credenciales del punto final o el acceso al destino'" y los detalles son "'ACCESSDENIED'" o "'InvalidAccessKeyId'".

Si necesita editar el extremo para resolver un error: Si selecciona **probar y guardar cambios**, StorageGRID validará el extremo actualizado y confirmará que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

Pasos

1. Seleccione el extremo.
2. En la página de detalles del punto final, seleccione **Configuración**.
3. Edite la configuración del extremo según sea necesario.
4. Seleccione **Conexión** > **probar conexión**.

Credenciales de extremo con permisos insuficientes

Cuando StorageGRID valida un extremo de servicios de plataforma, confirma que las credenciales del extremo se pueden utilizar para ponerse en contacto con el recurso de destino y realiza una comprobación básica de permisos. Sin embargo, StorageGRID no valida todos los permisos necesarios para ciertas operaciones de servicios de plataforma. Por este motivo, si recibe un error al intentar utilizar un servicio de plataforma (como "'403 Prohibido'"), compruebe los permisos asociados con las credenciales del punto final.

Solución de problemas de servicios de plataforma adicionales

Para obtener información adicional sobre la solución de problemas de los servicios de la plataforma, consulte las instrucciones para administrar StorageGRID.

"Administre StorageGRID"

Información relacionada

"Creación de un extremo de servicios de plataforma"

"Comprobación de la conexión para un extremo de servicios de plataforma"

"Edición de un extremo de servicios de plataforma"

Configurar la replicación de CloudMirror

El servicio de replicación de CloudMirror es uno de los tres servicios de plataforma StorageGRID. Puede usar la replicación de CloudMirror para replicar automáticamente objetos en un bloque de S3 externo.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para actuar como origen de replicación.
- El extremo que pretende usar como destino de la replicación de CloudMirror ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia los objetos de un bloque de origen en un bloque de destino que se especifique en un extremo. Para habilitar la replicación de CloudMirror en un bloque, debe crear y aplicar un XML de configuración de replicación de bloques válido. El XML de configuración de replicación debe usar la URN de un extremo de bloque de S3 para cada destino.

> La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.

Para obtener información general sobre la replicación de bloques y cómo configurarla, consulte la documentación de Amazon sobre la replicación entre regiones (CRR). Para obtener más información sobre cómo StorageGRID implementa la API de configuración de replicación de bloques de S3, consulte las instrucciones para implementar aplicaciones cliente S3.

Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los objetos nuevos agregados al bloque, pero no los objetos existentes en el bloque. Debe actualizar los objetos existentes para activar la replicación.

Si se especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones en el extremo de S3 de destino. El extremo de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir las recomendaciones que proporciona el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su bloque de origen:

   Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, tal y como se especifica en la API de replicación de S3. Al configurar XML:

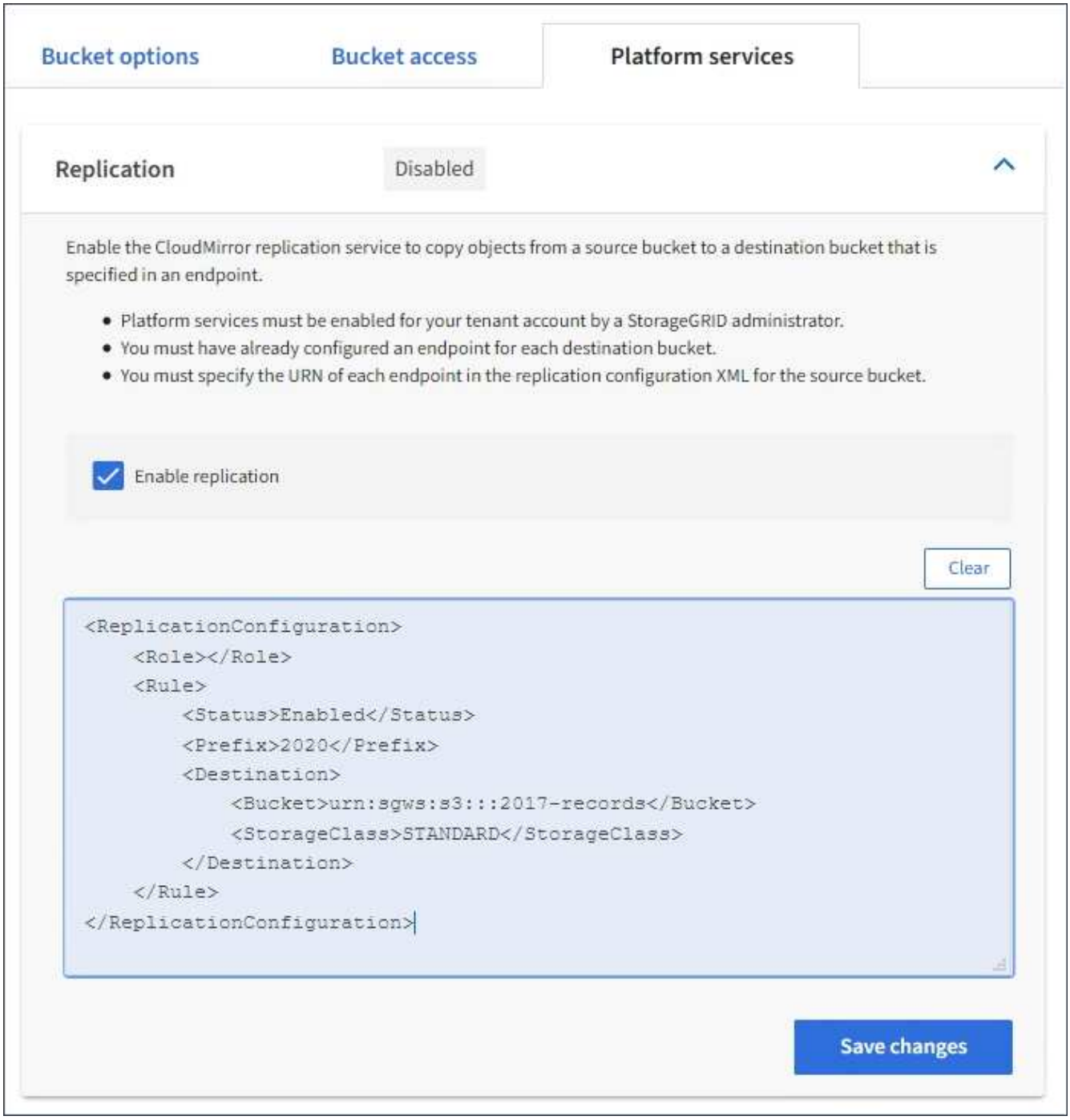
   - Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más información.
   - Use el URN de un extremo de bloque de S3 como destino.
   - Si lo desea, puede agregar el `<StorageClass>` y especifique una de las siguientes opciones:
     - `STANDARD`: La clase de almacenamiento predeterminada. Si no se especifica una clase de almacenamiento al cargar un objeto, el `STANDARD` se utiliza la clase de almacenamiento.
     - `STANDARD_IA`: (Estándar - acceso poco frecuente.) Utilice esta clase de almacenamiento para los datos a los que se accede con menor frecuencia; sin embargo, este proceso requiere un acceso rápido cuando sea necesario.
     - `REDUCED_REDUNDANCY`: Utilice esta clase de almacenamiento para datos no críticos y reproducibles que se pueden almacenar con menos redundancia que el `STANDARD` clase de almacenamiento.
   - Si especifica un `Role` En el XML de configuración se ignorará. StorageGRID no utiliza este valor.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **replicación**.
5. Active la casilla de verificación **Activar replicación**.
6. Pegue el XML de configuración de replicación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que la replicación está configurada correctamente:
   a. Añada un objeto al bloque de origen que cumpla con los requisitos de replicación según se especifica en la configuración de replicación.

      En el ejemplo mostrado anteriormente, se replican los objetos que coincidan con el prefijo "'2020'".

   b. Confirme que el objeto se ha replicado en el bloque de destino.

En el caso de objetos pequeños, la replicación se realiza con rapidez.

Información relacionada

"El servicio de replicación de CloudMirror"

"Use S3"

"Creación de un extremo de servicios de plataforma"

Configuración de notificaciones de eventos

El servicio de notificaciones es uno de los tres servicios de la plataforma StorageGRID. Puede habilitar las notificaciones de un bloque para enviar información acerca de los eventos especificados a un servicio de destino que admita AWS simple Notification Service™ (SNS).

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para que actúe como el origen de las notificaciones.
- Debe haber el extremo que se pretende usar como destino de las notificaciones de eventos y su URN debe estar presente.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar las notificaciones de eventos, cada vez que se produce un evento especificado para un objeto del bloque de origen, se genera una notificación y se envía al tema Servicio de notificación simple (SNS) que se utiliza como extremo de destino. Para habilitar las notificaciones para un bloque, debe crear y aplicar un XML de configuración de notificación válido. El XML de configuración de notificaciones debe usar el URN de un extremo de notificaciones de eventos para cada destino.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la documentación de Amazon. Para obtener más información sobre cómo StorageGRID implementa la API de configuración de notificaciones de bloques de S3, consulte las instrucciones para implementar aplicaciones de cliente S3.

Si habilita las notificaciones de eventos para un bloque que contiene objetos, las notificaciones se envían solo para las acciones que se realizan una vez guardada la configuración de notificación.

Pasos

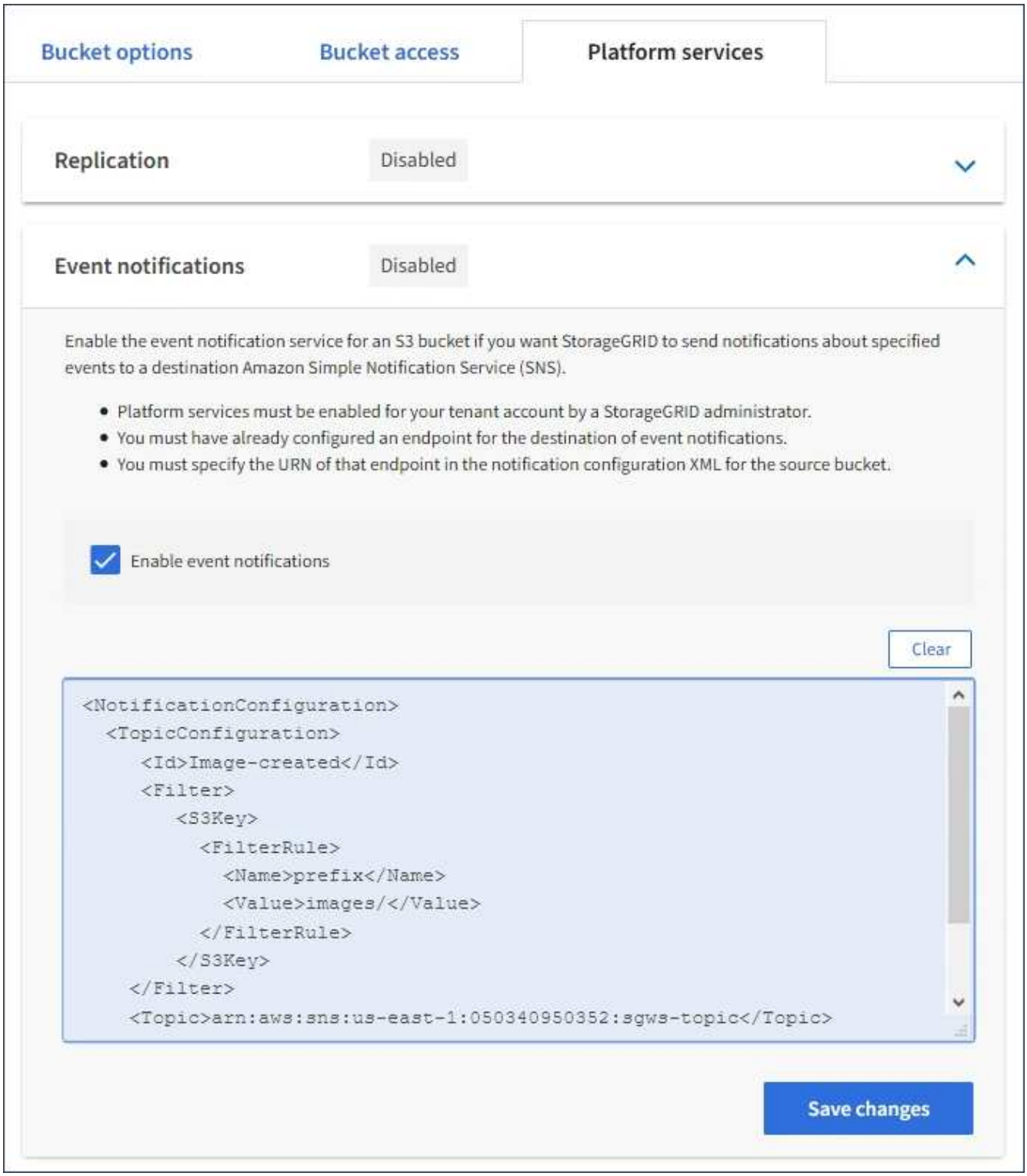
1. Habilite las notificaciones para su bloque de origen:
    - Use un editor de texto para crear el XML de configuración de notificaciones necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación de S3.
    - Al configurar XML, utilice URN de un extremo de notificaciones de eventos como tema de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **Notificaciones de eventos**.
5. Active la casilla de verificación **Activar notificaciones de eventos**.
6. Pegue el XML de configuración de notificación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que las notificaciones de eventos están configuradas correctamente:

   a. Realice una acción en un objeto del bloque de origen que cumpla los requisitos para activar una notificación tal y como se ha configurado en el XML de configuración.

En el ejemplo, se envía una notificación de evento cada vez que se crea un objeto con el `images/` prefijo.

b. Confirme que se ha entregado una notificación al tema SNS de destino.

Por ejemplo, si el tema de destino está alojado en el servicio de notificación simple (SNS) de AWS, puede configurar el servicio para que le envíe un correo electrónico cuando se entrega la notificación.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

Si se recibe la notificación en el tema de destino, ha configurado correctamente el bloque de origen para

las notificaciones StorageGRID.

Información relacionada

"Notificaciones para bloques"

"Use S3"

"Creación de un extremo de servicios de plataforma"

Utilizando el servicio de integración de búsqueda

El servicio de integración de búsqueda es uno de los tres servicios de la plataforma StorageGRID. Este servicio puede habilitar el envío de metadatos de objetos a un índice de búsqueda de destino siempre que se cree, se elimine o actualice los metadatos o las etiquetas de un objeto.

Puede configurar la integración de búsqueda mediante el Administrador de inquilinos para aplicar XML de configuración de StorageGRID personalizado a un bloque.

> Debido a que el servicio de integración de búsqueda hace que los metadatos de objeto se envíen a un destino, su XML de configuración se denomina XML_ de configuración de notificación de metadatos. Este XML de configuración es diferente al *notification Configuration XML* utilizado para habilitar las notificaciones de eventos.

Consulte las instrucciones para implementar aplicaciones cliente de S3 para obtener más detalles sobre las siguientes operaciones personalizadas de la API DE REST de StorageGRID S3:

- DELETE bucket metadata notification Configuration
- OBTENGA la solicitud de configuración de notificación de metadatos del bloque
- PUT bucket metadata notification Configuration

Información relacionada

"XML de configuración para la integración de búsqueda"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configurar el servicio de integración de búsqueda"

"Use S3"

XML de configuración para la integración de búsqueda

El servicio de integración de búsqueda se configura mediante un conjunto de reglas contenidas en `<MetadataNotificationConfiguration>` y.. `</MetadataNotificationConfiguration>` etiquetas. Cada regla especifica los objetos a los que se aplica la regla y el destino al que StorageGRID debe enviar los metadatos de esos objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos de los objetos con el prefijo `/images` en un destino y los metadatos de los objetos con el prefijo `/videos` a otro. Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, una configuración que incluye una regla para objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` no está permitido.

Los destinos deben especificarse mediante el URN de un extremo de StorageGRID que se ha creado para el servicio de integración de búsqueda. Estos extremos se refieren a un índice y tipo definidos en un clúster de Elasticsearch.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

En la tabla se describen los elementos del XML de configuración de notificaciones de metadatos.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No

Nombre	Descripción	Obligatorio
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. El valor de urn se incluye en el elemento Destination.	Sí

Utilice el XML de configuración de notificación de metadatos de ejemplo para aprender a crear su propio XML.

La configuración de notificaciones de metadatos se aplica a todos los objetos

En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configuración de notificaciones de metadatos con dos reglas

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

"Use S3"

"JSON generado por el servicio de integración de búsqueda"

"Configurar el servicio de integración de búsqueda"

Configurar el servicio de integración de búsqueda

El servicio de integración de búsqueda envía metadatos de objetos a un índice de búsqueda de destino cada vez que se crea, se elimina o se actualizan sus metadatos o etiquetas.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque de S3 cuyo contenido desea indexar.
- El extremo que pretende usar como destino del servicio de integración de búsqueda ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino. Si habilita el servicio de integración de búsqueda para un bloque que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Debe actualizar estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

Pasos

1. Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
   - Consulte la información sobre XML de configuración para la integración de búsquedas.
   - Al configurar XML, utilice URN de un extremo de integración de búsqueda como destino.

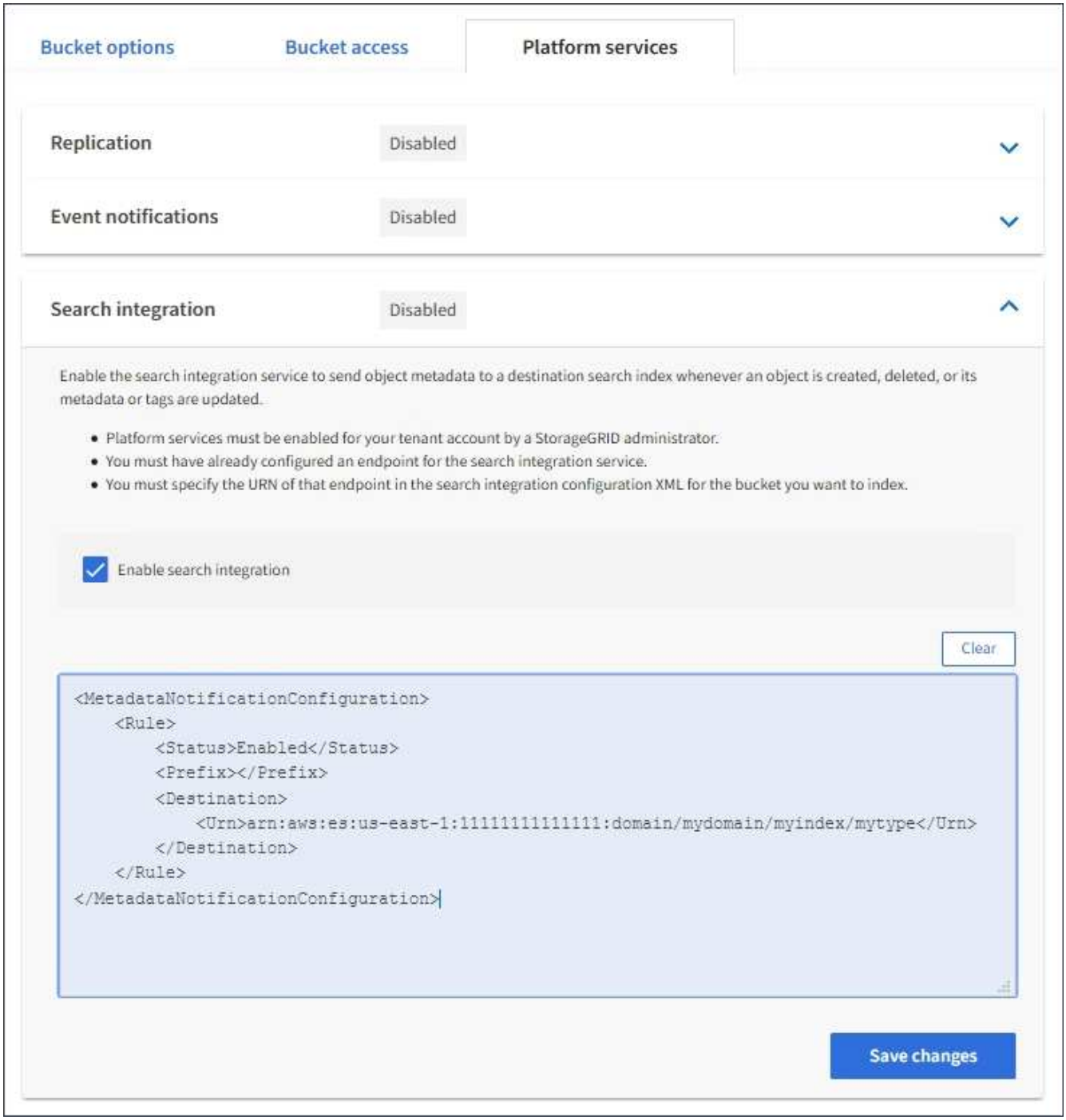
```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **integración de búsqueda**
5. Active la casilla de verificación **Activar integración de búsqueda**.

6. Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.



> Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que el servicio de integración de búsqueda está configurado correctamente:
   a. Añada un objeto al bloque de origen que cumpla los requisitos para activar una notificación de metadatos tal y como se especifica en el XML de configuración.

      En el ejemplo mostrado anteriormente, todos los objetos añadidos al bloque activan una notificación de metadatos.

b. Confirme que se ha agregado un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el extremo.

Después de terminar

Según sea necesario, se puede deshabilitar la integración de búsqueda para un bloque con cualquiera de los siguientes métodos:

- Seleccione **STORAGE (S3)** > **Buckets** y anule la selección de la casilla de verificación **Enable search Integration**.
- Si utiliza la API de S3 directamente, utilice una solicitud de notificación DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente de S3.

Información relacionada

"Descripción del servicio de integración de búsqueda"

"XML de configuración para la integración de búsqueda"

"Use S3"

"Creación de un extremo de servicios de plataforma"

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo de JSON que se podría generar cuando un objeto con la clave `SGWS/Tagging.txt` se crea en un bloque llamado `test`. La `test` el bloque no tiene versiones, por lo que el `versionId` la etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

Tipo	Nombre y descripción del artículo
Información sobre bloques y objetos	`bucket`: Nombre del cubo
`key`: Nombre de clave de objeto	`versionID`: Versión de objeto, para objetos en cubos con versiones
`region`: Región de cucharón, por ejemplo `us-east-1`	Metadatos del sistema
`size`: Tamaño del objeto (en bytes) visible para un cliente HTTP	`md5`: Hash de objeto
Metadatos del usuario	`metadata`: Todos los metadatos de usuario del objeto, como pares clave-valor `key:value`
Etiquetas	`tags`: Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor `key:value`

Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indizado un documento, no se pueden editar los tipos de campo del documento en el índice.

Información de copyright

Información de la marca comercial