Configure los extremos de servicios de la plataforma

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Configure los extremos de servicios de la 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 punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de gestión de puntos finales o acceso raíz, en una cuadrícula cuya red se ha configurado para permitir que los nodos de almacenamiento accedan a recursos de punto final externo. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. 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 bucket de StorageGRID en un bucket de Amazon S3, cree un punto final de servicios de plataforma que incluya la información y las credenciales que necesita StorageGRID para acceder al bucket de destino en Amazon.

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 puede configurar un depósito de origen para que utilice más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de Amazon Simple Notification Service (Amazon SNS) y notificaciones sobre la eliminación de objetos a un segundo tema de Amazon 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 es compatible con los extremos Amazon SNS y Kafka. No se admiten el servicio de cola simple (SQS) ni los extremos de AWS Lambda.

Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si tiene `ssl.client.auth` establezca en `required` En su configuración de Kafka broker, puede causar problemas de configuración de punto final de Kafka.

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 alojados en un cloud de AWS o en otro lugar.

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 punto final. StorageGRID creará el tipo si es necesario al enviar metadatos de objetos al extremo.

Información relacionada

"Administre StorageGRID"

Especifique URN para el extremo de servicios de la plataforma

Al crear un extremo de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará el URN para hacer referencia al punto final cuando cree un 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 Amazon Web Services (AWS), utilice `arn:aws`
- Si el servicio está alojado en Google Cloud Platform (GCP), 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` o. `kafka`
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	`bucket-name`
Notificaciones	`sns-topic-name` o. `kafka-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 y GCP

Para las entidades AWS y GCP, el URN completo es un AWS ARN válido. 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:

  Especifique un punto final de Amazon Simple Notification Service:

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

  Especifique un punto final Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-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.

Cree un extremo de servicios de plataforma

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

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".
- Se ha creado el recurso al que hace referencia el punto final de servicios de plataforma:
  - Replicación de CloudMirror: Bloque de S3
  - Notificación de eventos: Tema de Amazon Simple Notification Service (Amazon SNS) o Kafka
  - Notificación de búsqueda: Índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Tiene 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)

  "Especifique URN para el extremo de servicios de la plataforma"

- Credenciales de autenticación (si es necesario):

  Extremos de integración de búsquedas de AWS

  Para los extremos de integración de búsqueda de AWS, puede usar las siguientes credenciales:

  - Clave de acceso: ID de clave de acceso y clave de acceso secreta
  - Basic HTTP: Nombre de usuario y contraseña
  - CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

  Replicación de CloudMirror y extremos de Amazon SNS

  Para la replicación de CloudMirror y los extremos de Amazon SNS, puede usar las siguientes credenciales:

  - Clave de acceso: ID de clave de acceso y clave de acceso secreta
  - CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

  Puntos finales de Kafka

  Para los puntos finales de Kafka, puede utilizar las siguientes credenciales:

  - SASL/PLAIN: Nombre de usuario y contraseña
  - SASL/SCRAM-SHA-256: Nombre de usuario y contraseña
  - SASL/SCRAM-SHA-512: Nombre de usuario y contraseña

- Certificado de seguridad (si se utiliza un certificado de CA personalizado)

- Si las funciones de seguridad de Elasticsearch están activadas, tiene el privilegio de clúster de supervisión para las pruebas de conectividad y el privilegio WRITE INDEX o los privilegios INDEX y DELETE INDEX para las actualizaciones de documentos.

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 soporta el punto final se muestra junto al nombre del punto final cuando se muestra en la página de puntos finales, 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, se utilizan los siguientes puertos predeterminados:

   - Puerto 443 para URI HTTPS y puerto 80 para URI HTTP (mayoría de extremos)
   - Puerto 9092 para URI HTTPS y HTTP (solo puntos finales Kafka)

   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 el punto final se utiliza para el servicio de replicación de CloudMirror, no incluya el nombre del 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 puede cambiar el URN de un punto final después de crear el punto final.

6. Seleccione **continuar**.
7. Seleccione un valor para **Tipo de autenticación**.

Extremos de integración de búsquedas de AWS

Introduzca o cargue las credenciales para un extremo de integración de búsqueda de AWS.

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
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

Replicación de CloudMirror o extremos de Amazon SNS

Introduzca o cargue las credenciales para una replicación de CloudMirror o un extremo de Amazon SNS.

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

Tipo de autenticación	Descripción	Credenciales
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

Puntos finales de Kafka

Introduzca o cargue las credenciales para un punto final de Kafka.

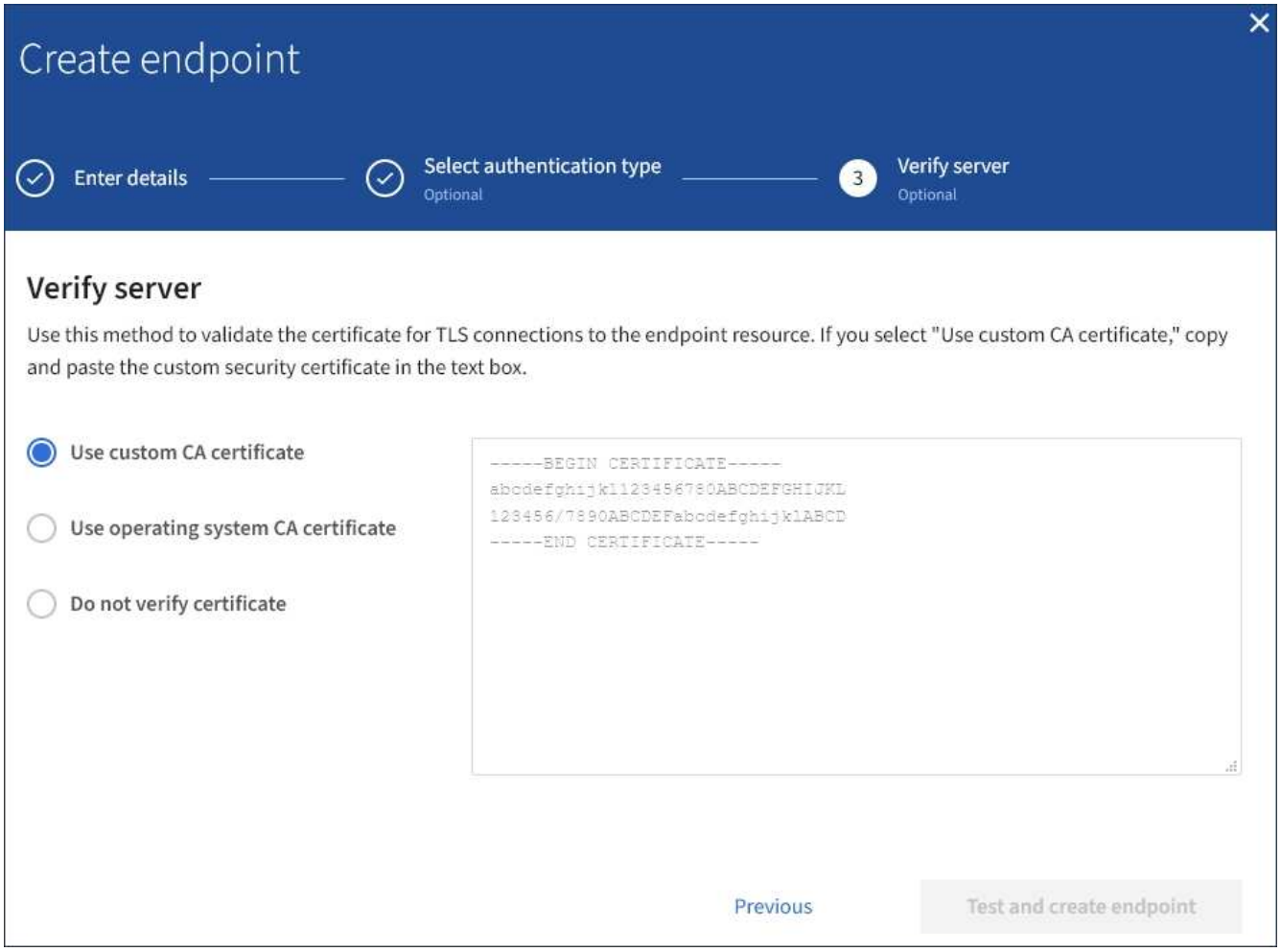
Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
SASL/PLAIN	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-256 para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-512 para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña

Seleccione **Usar la autenticación de delegación tomada** si el nombre de usuario y la contraseña se derivan de un token de delegación que se obtuvo de un clúster de Kafka.

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 de cuadrícula 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**.

La creación de punto final falla si los servicios de plataforma no están activados 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

"Especifique URN para el extremo de servicios de la plataforma"

"Configure la replicación de CloudMirror"

"Configure las notificaciones de eventos"

"Configure el servicio de integración de búsqueda"

Probar la conexión para el extremo de servicios de la 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.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

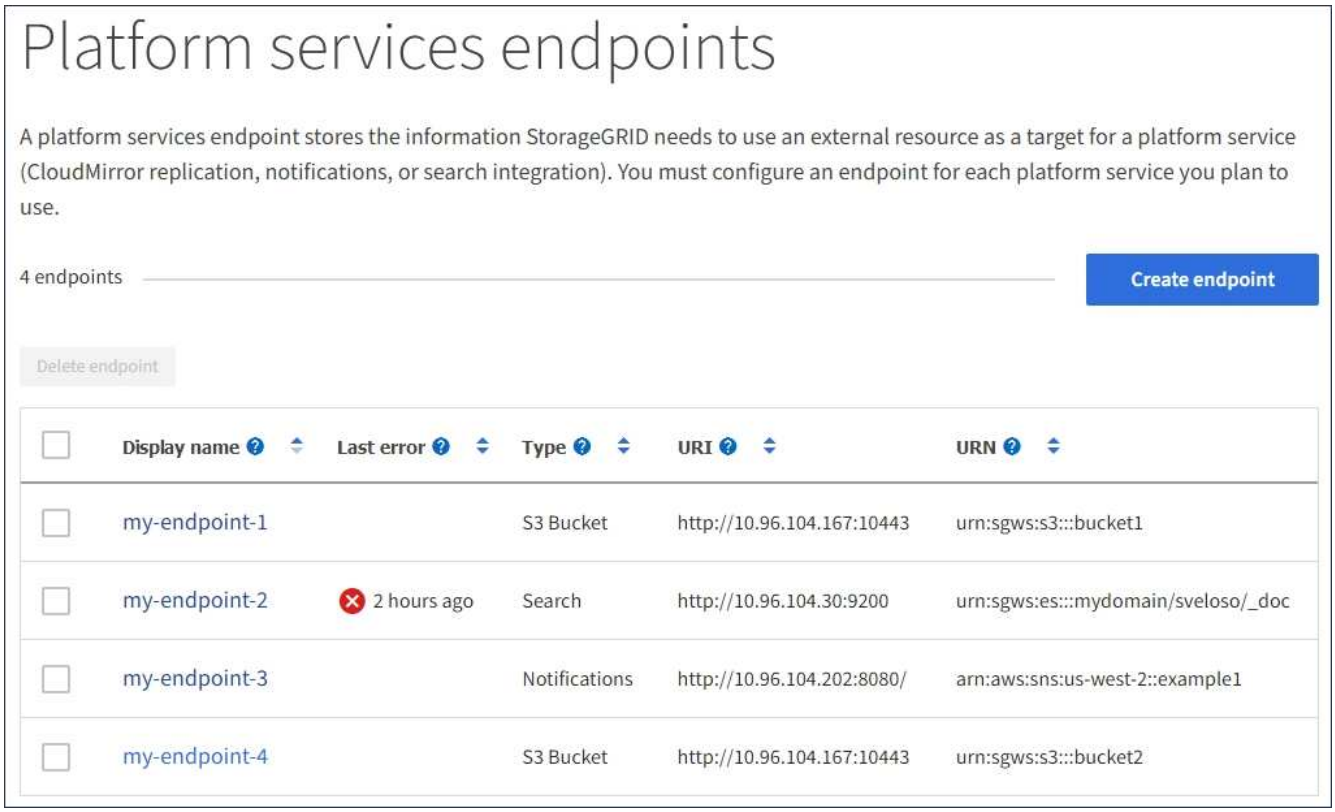
Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

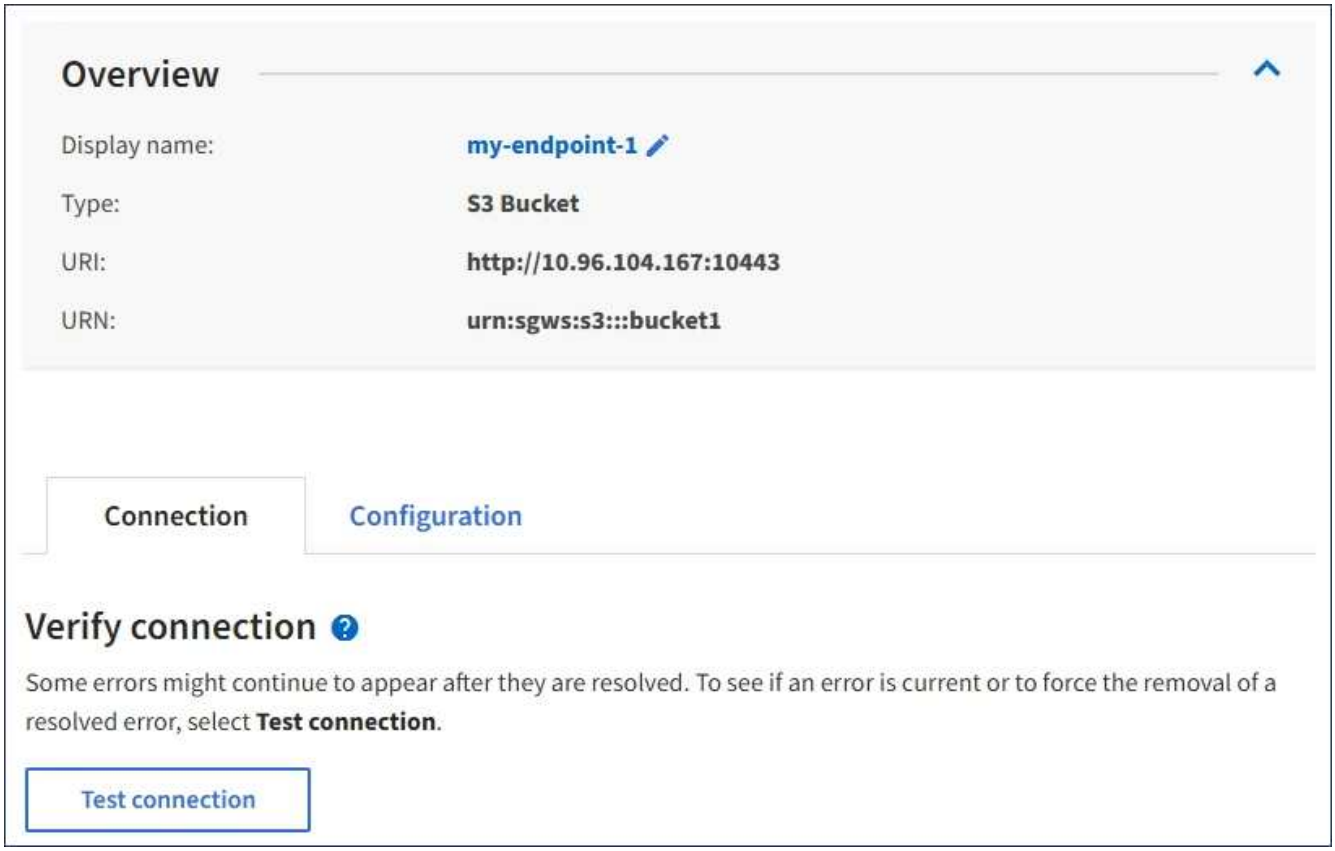
1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   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**.

Editar 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 puede cambiar el URN para un punto final de servicios de plataforma.

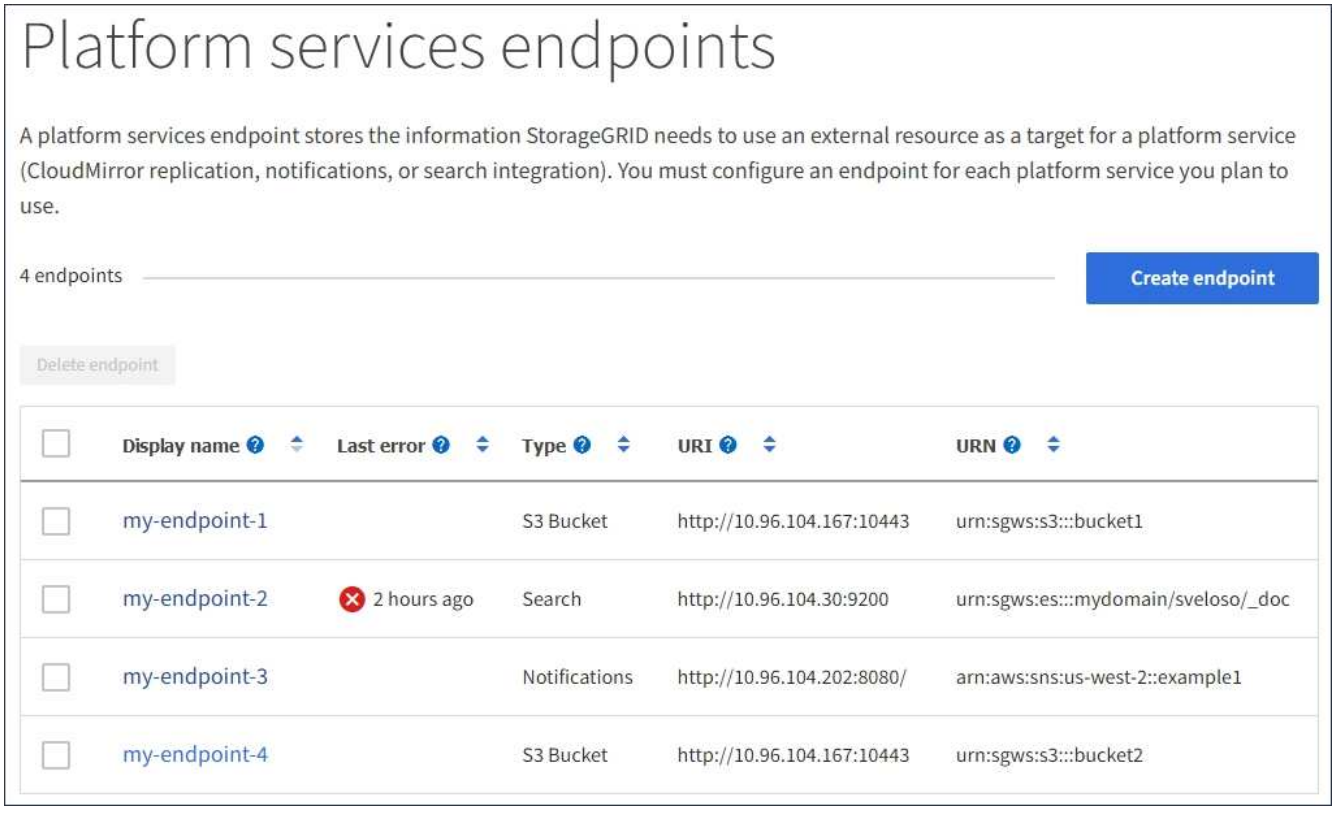
Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

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

   No puede cambiar el URN de un punto final después de crear el punto final.

   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 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**.
      - Para la autenticación CAP (C2S Access Portal), cambie la URL de las credenciales temporales o la frase de contraseña de la clave privada del cliente opcional y cargue nuevos archivos de certificado y claves según sea necesario.

        La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada no cifrada.

   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**.

Eliminar extremo de servicios de plataforma

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

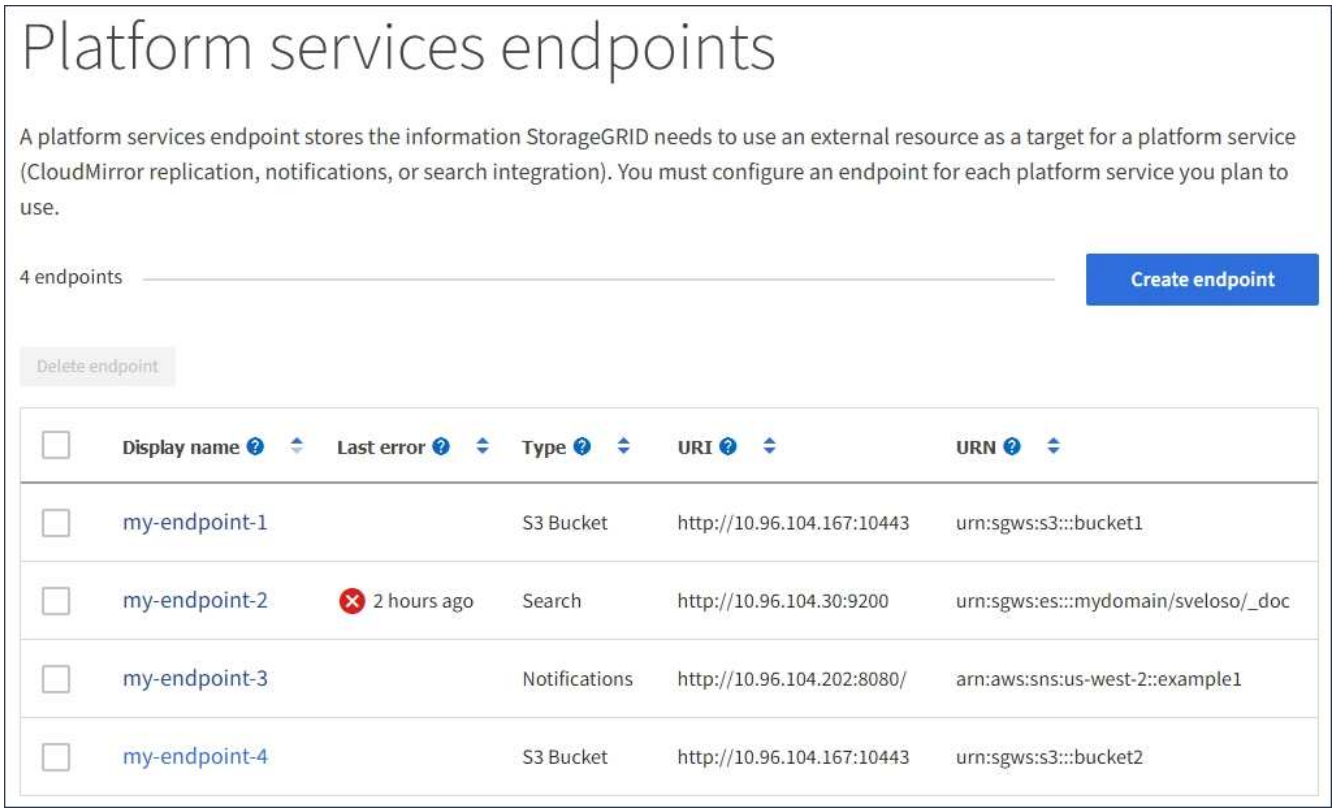
Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

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.

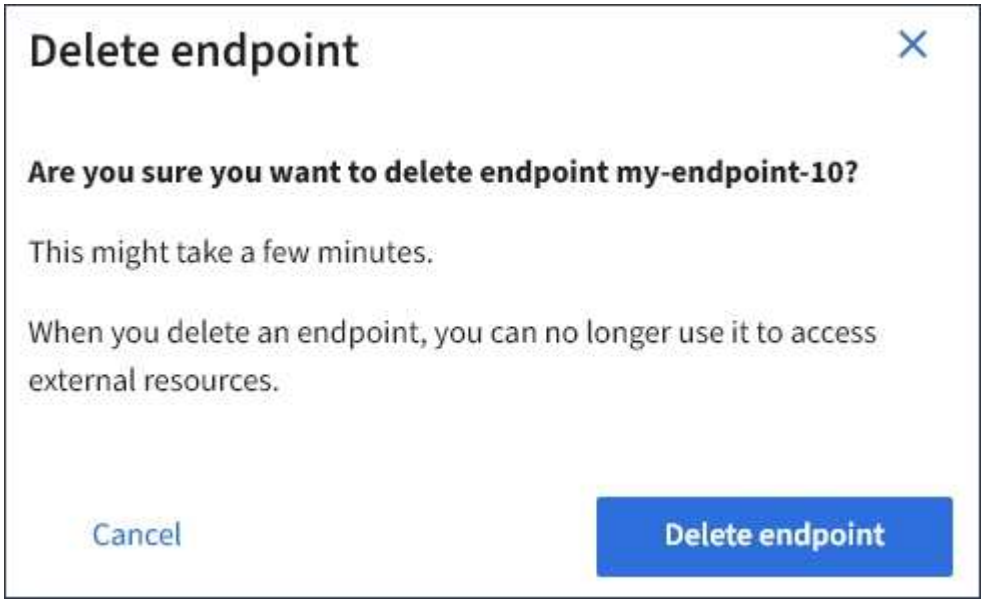


2. Seleccione la casilla de verificación de cada punto final que desee suprimir.

> 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.



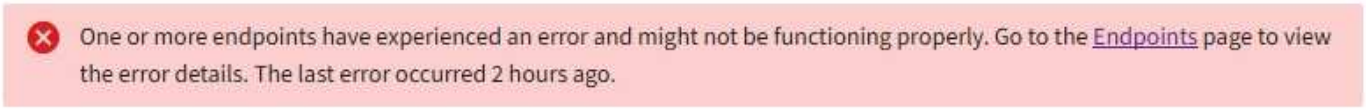
4. Seleccione **Eliminar punto final**.

Solucionar errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final 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.

Determine si se ha producido un error

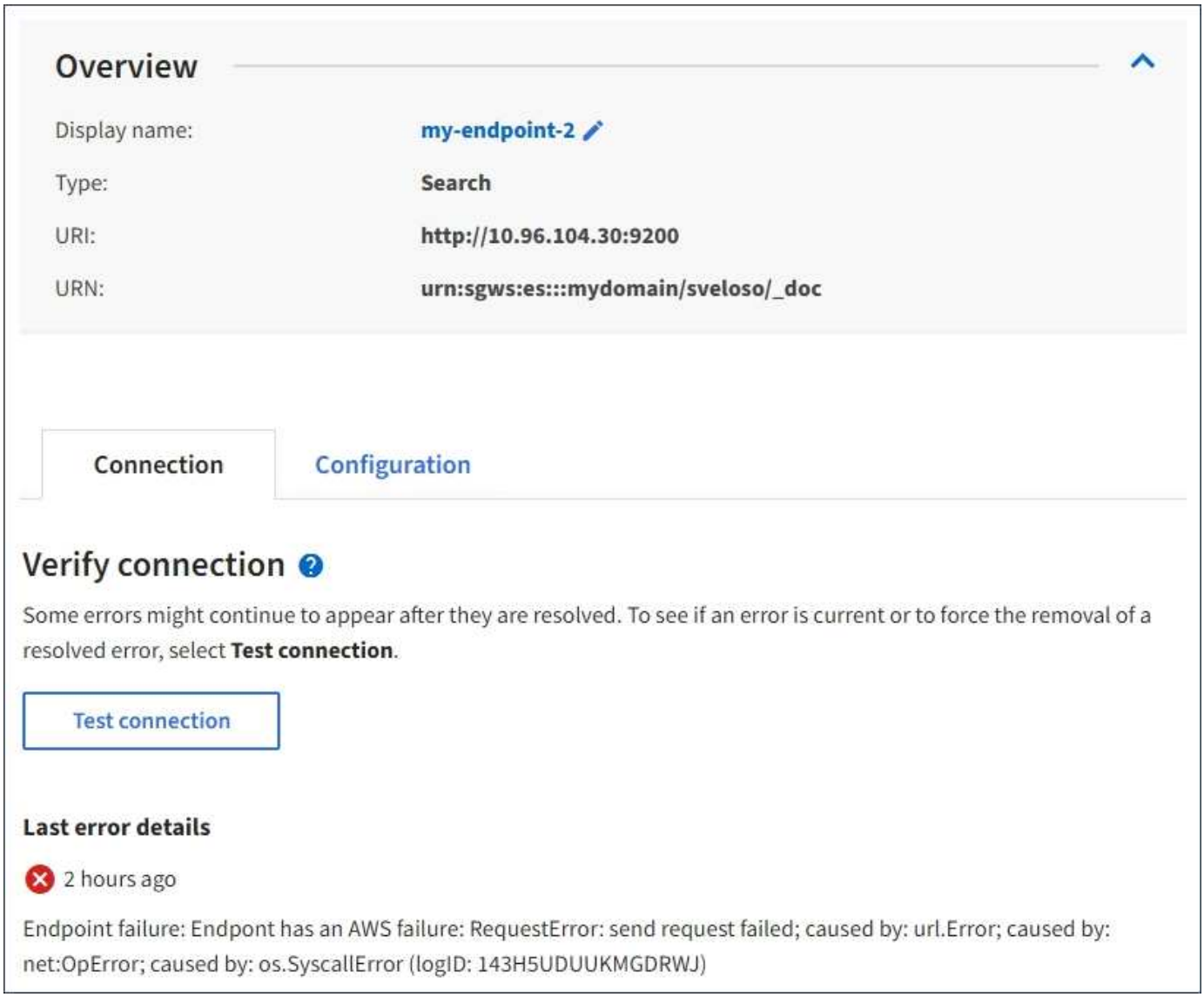
Si se ha producido algún error de punto final de servicios de plataforma en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.



El mismo error que aparece en el panel de control también aparece en la parte superior de la página Puntos Finales 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.



Compruebe si el 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.

Resolver 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 «Las credenciales del punto final o el acceso al destino deben actualizarse» y los detalles son «ACCESSDENIED» o «InvalidAccessKeyId».

Si necesita editar el extremo para resolver un error, al seleccionar **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 Forbidden”), compruebe los permisos asociados con las credenciales del punto final.

Información relacionada

- **Administrar los servicios de plataforma de StorageGRID › Solucionar problemas**
- "Cree un extremo de servicios de plataforma"
- "Probar la conexión para el extremo de servicios de la plataforma"
- "Editar extremo de servicios de plataforma"