Uso de Cloud Storage Pools

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Uso de Cloud Storage Pools

Puede usar los pools de almacenamiento en cloud para mover objetos de StorageGRID a una ubicación de almacenamiento externa, como el almacenamiento S3 Glacier o Microsoft Azure Blob. Mover objetos fuera de la cuadrícula permite aprovechar un nivel de almacenamiento de bajo coste para el archivado a largo plazo.

- "Qué es un pool de almacenamiento cloud"
- "Ciclo de vida de un objeto de Cloud Storage Pool"
- "Cuándo usar Cloud Storage Pools"
- "Consideraciones para Cloud Storage Pools"
- "Comparación de los pools de almacenamiento en cloud y la replicación de CloudMirror"
- "Creación de un pool de almacenamiento en el cloud"
- "Editar un pool de almacenamiento en el cloud"
- "Eliminación de un pool de almacenamiento en el cloud"
- "Solución de problemas de Cloud Storage Pools"

Qué es un pool de almacenamiento cloud

Un pool de almacenamiento en cloud permite utilizar ILM para mover datos de objetos fuera de su sistema StorageGRID. Por ejemplo, es posible que prefiera mover objetos a los que se accede con poca frecuencia a un almacenamiento en cloud de menor coste, como Amazon S3 Glacier, S3 Glacier Deep Archive o el nivel de acceso Archive en el almacenamiento Microsoft Azure Blob. O bien, puede que quiera mantener un backup en cloud de objetos de StorageGRID para mejorar la recuperación ante desastres.

Desde el punto de vista de la gestión del ciclo de vida de la información, un pool de almacenamiento en cloud es similar al de un pool de almacenamiento. Para almacenar objetos en cualquiera de las ubicaciones, debe seleccionar el pool al crear las instrucciones de ubicación para una regla de ILM. Sin embargo, si bien los pools de almacenamiento constan de nodos de almacenamiento o nodos de archivado dentro del sistema StorageGRID, un pool de almacenamiento en cloud consta de un bloque externo (S3) o un contenedor (almacenamiento blob de Azure).

En la siguiente tabla, se comparan los pools de almacenamiento con los pools de almacenamiento en el cloud y se muestran similitudes y diferencias de nivel elevado.

	Del banco de almacenamiento	**Pool de almacenamiento en cloud**
¿Cómo se crea?	Uso de la opción **ILM** > **agrupaciones de almacenamiento** en Grid Manager. Es necesario configurar las calificaciones de almacenamiento para poder crear el pool de almacenamiento.	Uso de la opción **ILM** > **agrupaciones de almacenamiento** en Grid Manager. Debe configurar el bloque o contenedor externo para poder crear el Cloud Storage Pool.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Cuántos pools se pueden crear?	Ilimitada.	Hasta 10.
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento o nodos de archivado dentro de StorageGRID.	En un bloque de Amazon S3 o un contenedor de almacenamiento de Azure Blob que se encuentra externo al sistema StorageGRID. Si Cloud Storage Pool es un bloque de Amazon S3: • Opcionalmente, se puede configurar un ciclo de vida de bloque para pasar los objetos a un almacenamiento a largo plazo de bajo coste, como Amazon S3 Glacier o S3 Glacier Deep Archive. El sistema de almacenamiento externo debe admitir la clase de almacenamiento Glacier y la API DE restauración DE objetos S3. • Puede crear pools de almacenamiento en el cloud para usarlos con los servicios de cloud comercial (C2S) de AWS, compatibles con la región secreta de AWS. Si Cloud Storage Pool es un contenedor de almacenamiento de Azure Blob, StorageGRID realiza la transición del objeto al nivel de archivado. **Nota:** en general, no configure la gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor utilizado para un grupo de almacenamiento en cloud. Las operaciones POSTERIORES a la restauración de objetos en el Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.
¿Qué controla la ubicación de objetos?	Una regla de ILM en la política activa de ILM.	Una regla de ILM en la política activa de ILM.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Cuántas copias de cada objeto se permiten?	Múltiples.	Una copia en el pool de almacenamiento cloud y, opcionalmente, una o varias copias en StorageGRID. **Nota:** no puede almacenar un objeto en más de un grupo de almacenamiento en la nube en un momento dado.
¿Cuáles son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste.

Ciclo de vida de un objeto de Cloud Storage Pool

Antes de implementar Cloud Storage Pools, revise el ciclo de vida de los objetos que se almacenan en cada tipo de pool de almacenamiento en cloud.

Información relacionada

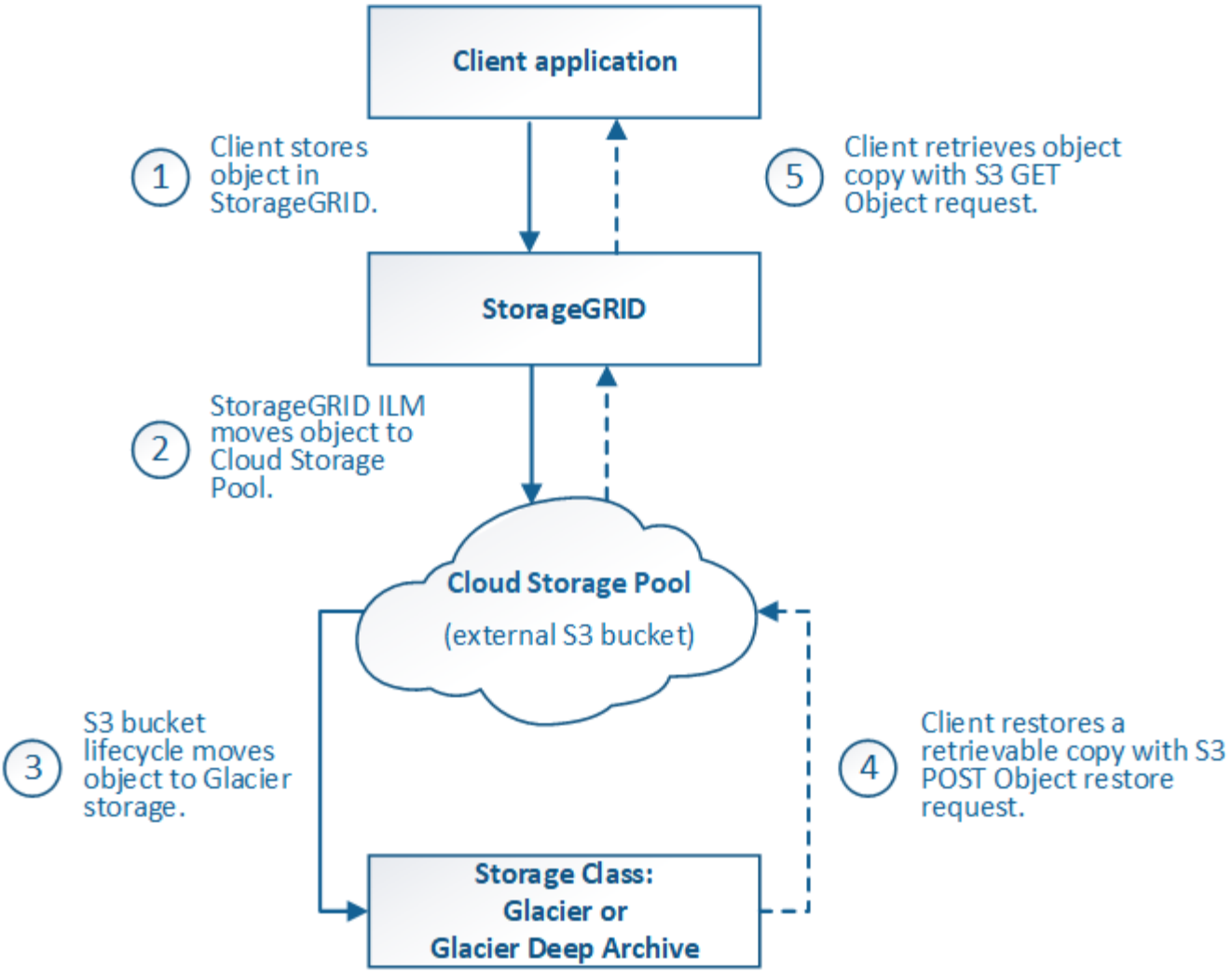
S3: Ciclo de vida de un objeto de Cloud Storage Pool

Azure: Ciclo de vida de un objeto de Cloud Storage Pool]

S3: Ciclo de vida de un objeto de Cloud Storage Pool

En la figura, se muestran las etapas del ciclo de vida de un objeto almacenado en un pool de almacenamiento en cloud de S3.

> En la figura y las explicaciones, "'Glacier'" hace referencia tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: La clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración acelerada. Solo se admite la recuperación masiva o estándar.



1. **Objeto almacenado en StorageGRID**

   Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. **Objeto movido a S3 Cloud Storage Pool**
   - Cuando el objeto coincide con una regla de ILM que utiliza un S3 Cloud Storage Pool como ubicación, StorageGRID mueve el objeto al bloque de S3 externo especificado por el Cloud Storage Pool.
   - Cuando el objeto se haya movido a S3 Cloud Storage Pool, la aplicación cliente puede recuperarlo con una solicitud DE OBJETO GET de S3 de StorageGRID, a menos que el objeto se haya migrado al almacenamiento Glacier.
3. **Objeto que ha pasado a Glacier (estado no recuperable)**
   - Opcionalmente, se puede cambiar el objeto al almacenamiento Glacier. Por ejemplo, el bloque externo de S3 puede utilizar la configuración del ciclo de vida para mover un objeto al almacenamiento Glacier de inmediato o después de varios días.

> Si desea realizar la transición de objetos, debe crear una configuración de ciclo de vida para el bloque de S3 externo y debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API DE restauración DE objetos S3 POSTERIOR.

> No use Cloud Storage Pools para los objetos que han sido procesados por los clientes de Swift. Swift no admite solicitudes DE restauración POSTERIOR de objetos, por lo que StorageGRID no podrá recuperar objetos Swift que se hayan migrado al almacenamiento S3 Glacier. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

- Durante la transición, la aplicación cliente puede usar una solicitud DE objeto HEAD de S3 para supervisar el estado del objeto.

4. **Objeto restaurado desde el almacenamiento Glacier**

   Si se ha realizado la transición de un objeto al almacenamiento Glacier, la aplicación cliente puede emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable al pool de almacenamiento en cloud de S3. La solicitud especifica cuántos días debe estar disponible la copia en el Cloud Storage Pool y en el nivel de acceso a datos que se usará en la operación de restauración (acelerada, estándar o masiva). Cuando se alcanza la fecha de vencimiento de la copia recuperable, la copia se devuelve automáticamente a un estado no recuperable.

   > Si también hay una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier con una solicitud DE restauración POSTERIOR a objeto. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

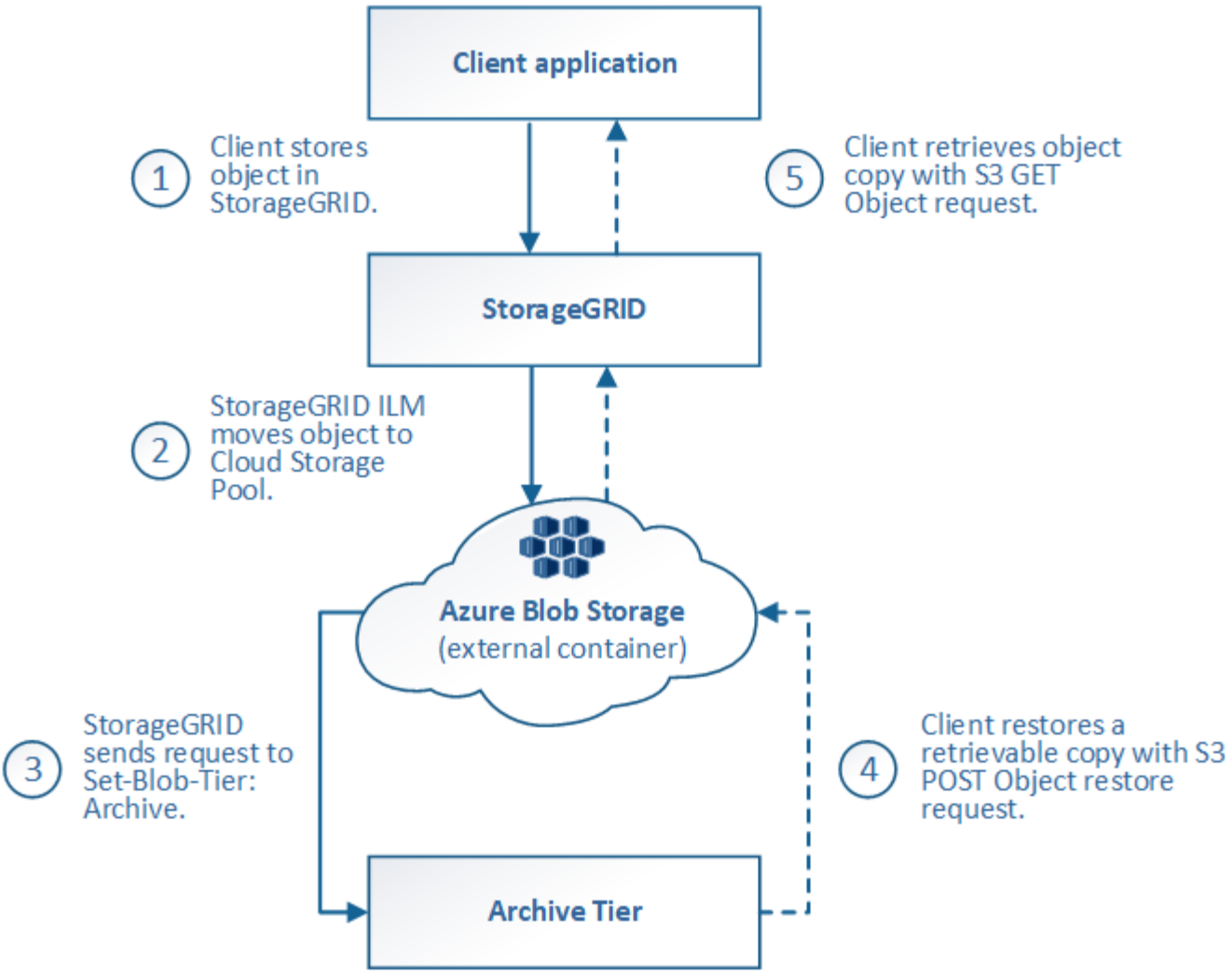
   Una vez restaurado un objeto, la aplicación cliente puede emitir UNA solicitud GET Object para recuperar el objeto restaurado.

Información relacionada

"Use S3"

Azure: Ciclo de vida de un objeto de Cloud Storage Pool

En la figura, se muestran las etapas del ciclo de vida de un objeto almacenado en un pool de almacenamiento en cloud de Azure.



1. **Objeto almacenado en StorageGRID**

   Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. **Objeto movido a Azure Cloud Storage Pool**

   Cuando el objeto coincide con una regla de ILM que utiliza un Azure Cloud Storage Pool como ubicación de ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento externo de Azure Blob especificado por el Cloud Storage Pool

   > No use Cloud Storage Pools para los objetos que han sido procesados por los clientes de Swift. Swift no admite solicitudes POSTERIORES a la restauración de objetos, por lo que StorageGRID no podrá recuperar objetos de Swift que se hayan migrado al nivel de archivado de almacenamiento de Azure Blob. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

3. **Objeto que ha pasado a la capa de archivado (estado no recuperable)**

   Inmediatamente después de mover el objeto a Azure Cloud Storage Pool, StorageGRID realiza una transición automática del objeto al nivel de archivado de almacenamiento de Azure Blob.

4. **Objeto restaurado desde el nivel de archivo**

Si se ha realizado la transición de un objeto al nivel de archivado, la aplicación cliente puede emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable a Azure Cloud Storage Pool.

Cuando StorageGRID recibe LA restauración DE objetos POSTERIOR, este realiza una transición temporal del objeto al nivel de refrigeración del almacenamiento de Azure Blob. Tan pronto como se alcanza la fecha de vencimiento de la solicitud DE restauración DE objeto POSTERIOR, StorageGRID realiza la transición del objeto de nuevo al nivel de archivado.

> Si también existen una o varias copias del objeto en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivado mediante la emisión de una solicitud DE restauración DE objetos POSTERIOR. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

   Una vez que se ha restaurado un objeto en Azure Cloud Storage Pool, la aplicación cliente puede emitir una solicitud GET Object para recuperar el objeto restaurado.

Cuándo usar Cloud Storage Pools

Los pools de almacenamiento en cloud pueden proporcionar ventajas importantes en diversos casos de uso.

Realizar backup de los datos de StorageGRID en una ubicación externa

Puede usar un pool de almacenamiento en cloud para realizar backup de objetos StorageGRID en una ubicación externa.

Si no se puede acceder a las copias en StorageGRID, se pueden utilizar los datos de objetos en el pool de almacenamiento en cloud para atender las solicitudes de los clientes. Sin embargo, es posible que deba emitir la solicitud de restauración DE objetos S3 POST para acceder a la copia de objeto de backup en el Cloud Storage Pool.

Los datos del objeto en un pool de almacenamiento en cloud también se pueden utilizar para recuperar los datos perdidos de StorageGRID debido a un fallo del volumen de almacenamiento o del nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un pool de almacenamiento en el cloud, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Para implantar una solución de backup:

1. Cree un único pool de almacenamiento en el cloud.
2. Configure una regla de ILM que almacene copias de objetos en los nodos de almacenamiento de forma simultánea (como copias replicadas o codificadas por borrado) y una única copia de objetos en el Cloud Storage Pool.
3. Añada la regla a la política de ILM. A continuación, simule y active la directiva.

Organizar en niveles los datos de StorageGRID en ubicaciones externas

Puede utilizar un pool de almacenamiento en cloud para almacenar objetos fuera del sistema StorageGRID. Por ejemplo, supongamos que tiene un gran número de objetos que necesita retener, pero espera tener

acceso a esos objetos rara vez, si es que alguna vez. Puede usar un pool de almacenamiento en cloud para organizar los objetos en niveles para reducir el almacenamiento y liberar espacio en StorageGRID.

Para implementar una solución por niveles:

1. Cree un único pool de almacenamiento en el cloud.
2. Configure una regla de ILM que mueva objetos que no se usen frecuentemente desde nodos de almacenamiento a Cloud Storage Pool.
3. Añada la regla a la política de ILM. A continuación, simule y active la directiva.

Mantenga varios extremos de cloud

Puede configurar varios pools de almacenamiento en cloud si desea organizar en niveles o realizar backups de datos de objetos en más de un cloud. Los filtros de las reglas de ILM permiten especificar los objetos que se almacenan en cada Cloud Storage Pool. Por ejemplo, puede que desee almacenar objetos de algunos inquilinos o bloques en Amazon S3 Glacier y objetos de otros inquilinos o bloques en el almacenamiento de Azure Blob. O bien, es posible que desee mover datos entre el almacenamiento de Amazon S3 Glacier y Azure Blob. Cuando utilice varios pools de almacenamiento en cloud, tenga en cuenta que un objeto se puede almacenar solo en un pool de almacenamiento en cloud cada vez.

Para implementar varios extremos de cloud:

1. Cree hasta 10 pools de almacenamiento en cloud.
2. Configure las reglas de ILM para almacenar los datos de los objetos adecuados en el momento adecuado en cada pool de almacenamiento de cloud. Por ejemplo, almacene objetos del bloque A en el Cloud Storage Pool A y almacene objetos del bloque B en el Cloud Storage Pool B. O bien, almacene objetos en el pool de almacenamiento en cloud A durante cierto tiempo y muévalos a Cloud Storage Pool B.
3. Añada las reglas a la política de ILM. A continuación, simule y active la directiva.

Consideraciones para Cloud Storage Pools

Si planea utilizar un pool de almacenamiento en cloud para mover objetos desde el sistema StorageGRID, debe revisar las consideraciones que hay que tener en cuenta a la hora de configurar y utilizar pools de almacenamiento en cloud.

Consideraciones generales

- En general, el almacenamiento de archivado en cloud, como el almacenamiento de Amazon S3 Glacier o Azure Blob, es un lugar económico para almacenar datos de objetos. No obstante, los costes para recuperar datos del almacenamiento de archivado en el cloud son relativamente altos. Para alcanzar el coste general más bajo, debe tener en cuenta cuándo y con qué frecuencia accederá a los objetos en el pool de almacenamiento en cloud. El uso de un Cloud Storage Pool solo se recomienda para el contenido al que espera acceder con poca frecuencia.
- No use Cloud Storage Pools para los objetos que han sido procesados por los clientes de Swift. Swift no admite solicitudes POSTERIORES a la restauración de objetos, por lo que StorageGRID no podrá recuperar objetos de Swift que se hayan migrado al almacenamiento S3 Glacier ni al nivel de almacenamiento de Azure Blob. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).
- No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.

Información necesaria para crear un pool de almacenamiento en cloud

Antes de poder crear un Cloud Storage Pool, debe crear el bloque de S3 externo o el contenedor de almacenamiento externo de Azure Blob que utilizará para el Cloud Storage Pool. A continuación, cuando cree el pool de almacenamiento en cloud en StorageGRID, debe especificar la siguiente información:

- El tipo de proveedor: Almacenamiento Amazon S3 o Azure Blob.
- Si selecciona Amazon S3, si Cloud Storage Pool va a utilizarse con la región secreta de AWS (**CAP (Portal de acceso C2S)**).
- El nombre exacto del contenedor o contenedor.
- El extremo de servicio necesario para acceder al bloque o contenedor.
- La autenticación necesaria para acceder al bloque o contenedor:
  - **S3**: Opcionalmente, un ID de clave de acceso y una clave de acceso secreta.
  - **C2S**: La dirección URL completa para obtener credenciales temporales del servidor CAP; un certificado de CA del servidor, un certificado de cliente, una clave privada para el certificado de cliente y, si la clave privada está cifrada, la frase de acceso para descifrarla.
  - **Almacenamiento de Azure Blob**: Un nombre de cuenta y una clave de cuenta. Estas credenciales deben tener permiso completo para el contenedor.
- De manera opcional, un certificado de CA personalizado para verificar las conexiones TLS al bloque o contenedor.

Consideraciones sobre los puertos utilizados para Cloud Storage Pools

Para garantizar que las reglas de ILM puedan mover objetos desde y hacia el Cloud Storage Pool especificado, debe configurar la red o las redes que contienen los nodos de almacenamiento del sistema. Debe asegurarse de que los siguientes puertos puedan comunicarse con el pool de almacenamiento en cloud.

De forma predeterminada, los pools de almacenamiento en cloud utilizan los puertos siguientes:

- **80**: Para los URI de punto final que comienzan con http
- **443**: Para los URI de punto final que comienzan con https

Es posible especificar un puerto diferente cuando se crea o se edita un pool de almacenamiento en el cloud.

Si utiliza un servidor proxy no transparente, también debe configurar un proxy de almacenamiento para permitir que los mensajes se envíen a extremos externos, como un extremo de Internet.

Consideraciones sobre los costos

El acceso al almacenamiento en el cloud por medio de un pool de almacenamiento en el cloud requiere conectividad de red al cloud. Debe tener en cuenta el coste de la infraestructura de red que utilizará para acceder al cloud y aprovisionarlo adecuadamente, en función de la cantidad de datos que espera mover entre StorageGRID y el cloud con el pool de almacenamiento en cloud.

Cuando StorageGRID se conecta al extremo externo de Flash Storage Pool, emite distintas solicitudes para supervisar la conectividad y garantizar que puede ejecutar las operaciones requeridas. Aunque se asociarán algunos costes adicionales con estas solicitudes, el coste de supervisar un Cloud Storage Pool solo debería ser una pequeña fracción del coste total de almacenar objetos en S3 o Azure.

Es posible que deba incurrir en costes más significativos si necesita mover objetos desde un extremo de

almacenamiento en cloud externo a StorageGRID. Los objetos pueden moverse de nuevo a StorageGRID en cualquiera de estos casos:

- La única copia del objeto se encuentra en un Pool de almacenamiento en cloud y en su lugar decide almacenar el objeto en StorageGRID. En este caso, sólo tiene que volver a configurar las reglas y la política de ILM. Cuando se produce la evaluación de la gestión de la vida útil de la información, StorageGRID emite varias solicitudes para recuperar el objeto desde el pool de almacenamiento en cloud. A continuación, StorageGRID crea el número especificado de copias replicadas o codificadas de borrado en forma local. Cuando el objeto se mueve de nuevo a StorageGRID, se elimina la copia en el pool de almacenamiento en el cloud.
- Se pierden los objetos debido a un fallo en el nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un pool de almacenamiento en el cloud, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

> Cuando se devuelven objetos a StorageGRID desde un pool de almacenamiento en el cloud, StorageGRID emite varias solicitudes al extremo de pool de almacenamiento en cloud para cada objeto. Antes de mover un gran número de objetos, póngase en contacto con el soporte técnico para obtener ayuda a la hora de calcular el plazo de tiempo y los costes asociados.

S3: Permisos necesarios para el bloque de Cloud Storage Pool

La política de bloque para el bloque externo de S3 usado para un Cloud Storage Pool debe otorgar permiso StorageGRID para mover un objeto al bloque, obtener el estado de un objeto, restaurar un objeto del almacenamiento Glacier cuando sea necesario y más. Lo ideal es que StorageGRID tenga acceso de control total al cucharón (`s3:*`); sin embargo, si esto no es posible, la directiva bucket debe conceder los siguientes permisos S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Consideraciones para el ciclo de vida del bloque externo

El movimiento de objetos entre StorageGRID y el bloque externo S3 especificado en el Cloud Storage Pool está controlado por las reglas de ILM y la política activa de ILM en StorageGRID. Por el contrario, la configuración del ciclo de vida de ese bloque controla la transición de objetos desde el bloque S3 externo especificado en Cloud Storage Pool a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implementa la clase de almacenamiento Glacier).

Si desea realizar la transición de objetos desde Cloud Storage Pool, debe crear la configuración de ciclo de vida adecuada en el bloque externo de S3. Debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible CON la API DE restauración POSTERIOR a objetos de S3.

Por ejemplo, supongamos que desea que se realice inmediatamente la transición de todos los objetos

movidos de StorageGRID al pool de almacenamiento en cloud al almacenamiento Amazon S3 Glacier. Debe crear una configuración de ciclo de vida en el bloque S3 externo que especifique una única acción (**transición**) de la siguiente forma:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Esta regla transitaría todos los objetos de bloques al Amazon S3 Glacier el día en que se crearon (es decir, el día en que se movieron de StorageGRID a la agrupación de almacenamiento en cloud).

> Al configurar el ciclo de vida del cucharón externo, no utilice nunca acciones **Expiración** para definir cuándo caducan los objetos. Las acciones de caducidad hacen que el sistema de almacenamiento externo elimine los objetos caducados. Si más adelante intenta acceder a un objeto caducado de StorageGRID, no se encuentra el objeto eliminado.

Si desea realizar la transición de objetos del Cloud Storage Pool a S3 Glacier Deep Archive (en lugar de Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida de la cuchara. Sin embargo, tenga en cuenta que no puede utilizar el `Expedited` organice en niveles los objetos de S3 Glacier Deep Archive.

Azure: Consideraciones para el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puede configurar el nivel de acceso predeterminado en Hot o Cool. Al crear una cuenta de almacenamiento para usar con un pool de almacenamiento en el cloud, se debe usar el nivel de función como nivel predeterminado. Aunque StorageGRID establece inmediatamente el nivel Archivado cuando se mueven objetos al pool de almacenamiento en el cloud, el uso de una configuración predeterminada de caliente garantiza que no se cobrará una tarifa de eliminación anticipada de los objetos que se quitan del nivel de refrigeración antes del mínimo de 30 días.

Azure: Gestión del ciclo de vida no compatible

No utilice la gestión del ciclo de vida del almacenamiento BLOB de Azure para el contenedor utilizado con un Cloud Storage Pool. Las operaciones de ciclo de vida pueden interferir en las operaciones de Cloud Storage Pool.

Información relacionada

"Creación de un pool de almacenamiento en el cloud"

"S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud"

"C2S S3: Especificar detalles de autenticación de un pool de almacenamiento en el cloud"

"Azure: Especificar detalles de autenticación para un pool de almacenamiento en cloud"

"Administre StorageGRID"

Comparación de los pools de almacenamiento en cloud y la replicación de CloudMirror

Cuando comience a usar pools de almacenamiento en cloud, podría ser útil comprender las similitudes y diferencias entre los pools de almacenamiento en cloud y el servicio de replicación CloudMirror de StorageGRID.

	Pool de almacenamiento en cloud	**Servicio de replicación de CloudMirror**
¿Cuál es el objetivo principal?	Un pool de almacenamiento en cloud actúa como destino de archivado. La copia de objeto del Pool de almacenamiento en cloud puede ser la única copia del objeto, o bien puede ser una copia adicional. Es decir, en lugar de conservar dos copias en las instalaciones, solo puede conservar una copia en StorageGRID y enviar una copia al Cloud Storage Pool.	El servicio de replicación de CloudMirror permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) en un bloque de S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura de S3 independiente.
¿Cómo se configura?	Los pools de almacenamiento en cloud se definen del mismo modo que los pools de almacenamiento, mediante Grid Manager o la API de gestión de grid. Puede seleccionar un Cloud Storage Pool como ubicación en una regla de ILM. Si bien un pool de almacenamiento consta de un grupo de nodos de almacenamiento, un pool de almacenamiento en el cloud se define mediante un extremo remoto de S3 o Azure (dirección IP, credenciales, etc.).	Un usuario de inquilino configura la replicación de CloudMirror definiendo un extremo de CloudMirror (dirección IP, credenciales, etc.) mediante el administrador de inquilinos o la API de S3. Una vez configurado el extremo de CloudMirror, se puede configurar cualquier bloque que sea propiedad de esa cuenta de inquilino para que apunte al extremo de CloudMirror.
¿Quién es responsable de su configuración ?	Normalmente, un administrador de grid	Normalmente, un usuario inquilino
¿Cuál es el destino?	• Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Nivel de Azure Blob Archive	• Cualquier infraestructura compatible de S3 (incluido Amazon S3)

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿Qué hace que los objetos se muevan al destino?	Una o varias reglas de ILM en la política activa de ILM. Las reglas de ILM definen los objetos que StorageGRID se mueve al Cloud Storage Pool y cuándo se mueven los objetos.	La acción de incluir un nuevo objeto en un bloque de origen que se haya configurado con un extremo de CloudMirror.los objetos que existían en el bloque de origen antes de que se configurara el bloque con el extremo de CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se recuperan los objetos?	Las aplicaciones deben solicitar a StorageGRID para recuperar objetos que se hayan movido a un pool de almacenamiento en cloud. Si se transición la única copia de un objeto al almacenamiento de archivado, StorageGRID gestiona el proceso de restauración del objeto para que se pueda recuperar.	Debido a que la copia duplicada en el bloque de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes ya sea a StorageGRID o al destino de S3. Por ejemplo, supongamos que usa la replicación de CloudMirror para reflejar objetos en una organización asociada. El partner puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Puede leer directamente desde el destino?	No StorageGRID gestiona los objetos movidos a un pool de almacenamiento en cloud. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del pool de almacenamiento en cloud).	Sí, porque la copia duplicada es una copia independiente.
¿Qué ocurre si un objeto se elimina del origen?	El objeto también se elimina en el Cloud Storage Pool.	La acción de eliminación no se replica. Un objeto eliminado ya no existe en el bloque StorageGRID, pero sigue existiendo en el bloque de destino. Del mismo modo, los objetos del bloque de destino se pueden eliminar sin que ello afecte al origen.
¿Cómo accede a los objetos tras un desastre (el sistema StorageGRID no está operativo)?	Los nodos StorageGRID con errores deben recuperarse. Durante este proceso, es posible que se restauren copias de los objetos replicados con las copias del Cloud Storage Pool.	Las copias de objetos en el destino de CloudMirror son independientes de la StorageGRID, por lo que se podrá acceder a ellas directamente antes de que se recuperen los nodos StorageGRID.

Información relacionada

"Administre StorageGRID"

Creación de un pool de almacenamiento en el cloud

Cuando crea un Cloud Storage Pool, debe especificar el nombre y la ubicación del

bloque o contenedor externo que StorageGRID utilizará para almacenar objetos, el tipo de proveedor cloud (Amazon S3 o Azure Blob Storage) y la información que StorageGRID necesita para acceder a la bloque o el contenedor externo.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe haber revisado las directrices para la configuración de Cloud Storage Pools.
- Debe haber el bloque o contenedor externo al que hace referencia Cloud Storage Pool.
- Debe tener toda la información de autenticación necesaria para acceder al bloque o contenedor.

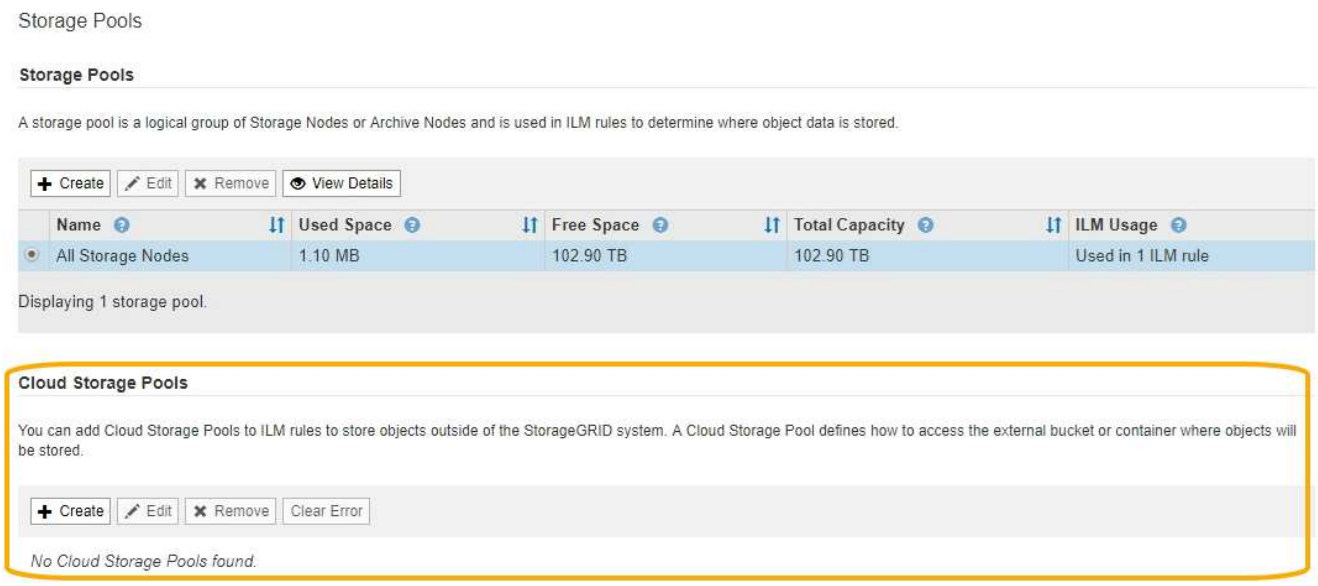
Acerca de esta tarea

Un Cloud Storage Pool especifica un único bloque de almacenamiento S3 externo o Azure Blob. StorageGRID valida el pool de almacenamiento en cloud tan pronto como lo guarde, por lo que debe asegurarse de que existe el bloque o contenedor especificado en el pool de almacenamiento en el cloud y sea posible acceder a él.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools. Esta página incluye dos secciones: Pools de almacenamiento y pools de almacenamiento en cloud.



2. En la sección Cloud Storage Pools de la página, haga clic en **Crear**.

   Se muestra el cuadro de diálogo Crear un pool de almacenamiento en cloud.

3. Introduzca la siguiente información:

Campo	Descripción
Nombre para mostrar	Un nombre que describe brevemente el pool de almacenamiento en el cloud y su propósito. Utilice un nombre que será fácil de identificar al configurar las reglas de ILM.
Tipo de proveedor	Qué proveedor de cloud utilizará para este pool de almacenamiento en cloud: • Amazon S3 (seleccione esta opción para un pool de almacenamiento en cloud S3 o C2S S3) • Almacenamiento de Azure Blob **Nota:** cuando selecciona un Tipo de proveedor, las secciones de extremo de servicio, autenticación y verificación de servidor aparecen en la parte inferior de la página.
Cucharón o contenedor	El nombre del bloque de S3 externo o del contenedor de Azure que se creó para el pool de almacenamiento en cloud. Se producirá un error en el nombre que especifique aquí para que coincida exactamente con el nombre del bloque o contenedor, o bien se producirá un error al crear el pool de almacenamiento en cloud. No se puede cambiar este valor después de guardar el pool de almacenamiento en cloud.

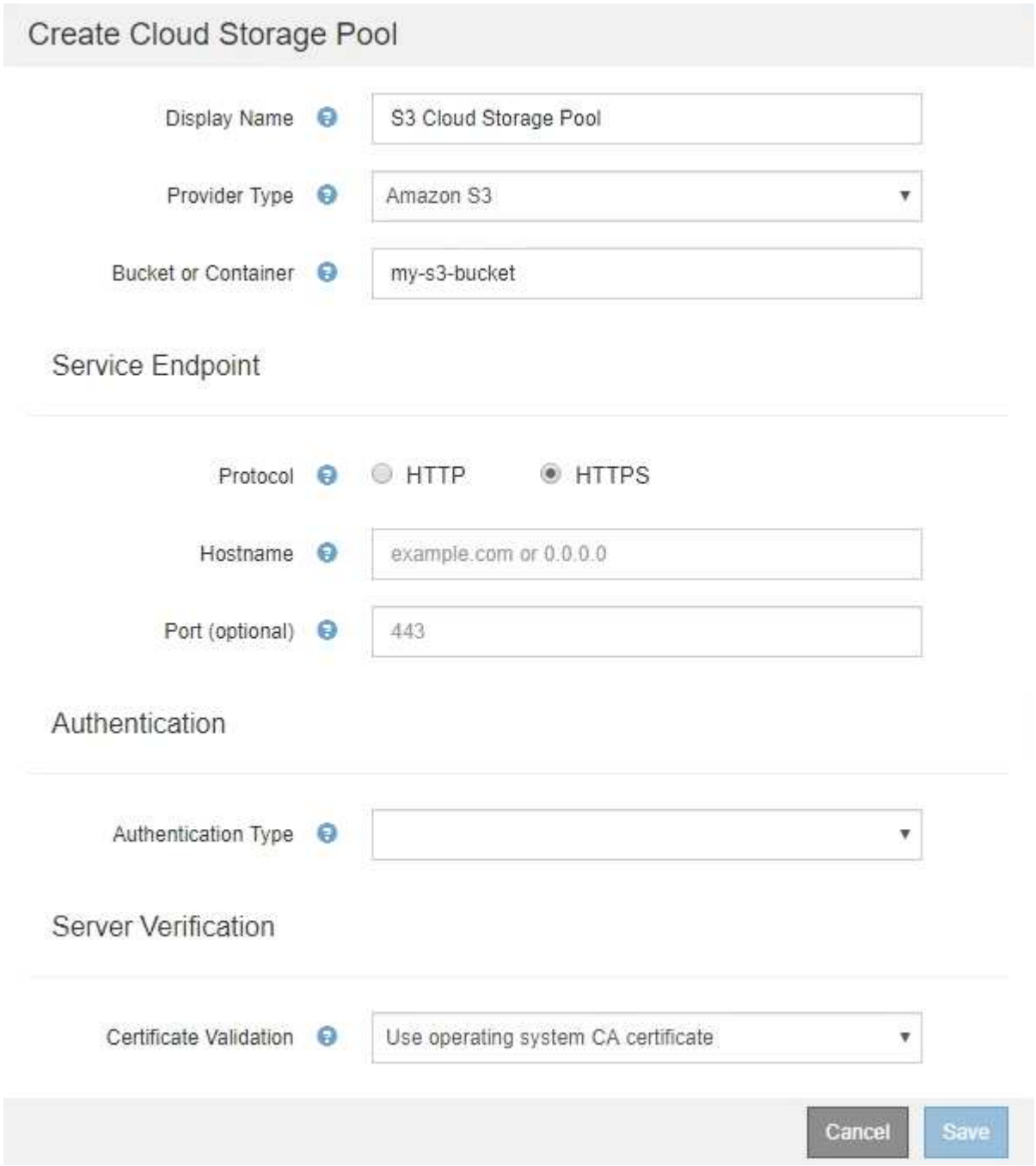
4. Complete las secciones Service Endpoint, Authentication and Server Verification de la página, según el tipo de proveedor seleccionado.
   - "S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud"
   - "C2S S3: Especificar detalles de autenticación de un pool de almacenamiento en el cloud"
   - "Azure: Especificar detalles de autenticación para un pool de almacenamiento en cloud"

S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud

Al crear un Cloud Storage Pool para S3, debe seleccionar el tipo de autenticación requerido para el extremo de Cloud Storage Pool. Puede especificar Anónimo o introducir un ID de clave de acceso y una clave de acceso secreta.

Lo que necesitará

- Debe haber introducido la información básica para Cloud Storage Pool y ha especificado **Amazon S3** como tipo de proveedor.



- Si utiliza la autenticación de clave de acceso, debe conocer el identificador de clave de acceso y la clave de acceso secreta del bloque S3 externo.

Pasos

1. En la sección **Service Endpoint**, proporcione la siguiente información:

   a. Seleccione el protocolo que desea utilizar al conectarse al Cloud Storage Pool.

      El protocolo predeterminado es HTTPS.

   b. Introduzca el nombre de host o la dirección IP del servidor del grupo de almacenamiento en cloud.

      Por ejemplo:

      `s3-aws-region.amazonaws.com`

      > No incluya el nombre del segmento en este campo. Incluye el nombre del segmento en el campo **cucharón o contenedor**.

   a. Opcionalmente, especifique el puerto que se debe utilizar al conectarse al Cloud Storage Pool.

      Deje este campo vacío para utilizar el puerto predeterminado: Puerto 443 para HTTPS o puerto 80 para HTTP.

2. En la sección **autenticación**, seleccione el tipo de autenticación que se requiere para el extremo de Cloud Storage Pool.

Opción	Descripción
Clave de acceso	Se requiere un identificador de clave de acceso y una clave de acceso secreta para acceder al bloque del pool de almacenamiento en cloud.
Anónimo	Todos tienen acceso al bloque de pools de almacenamiento en cloud. No se requieren un identificador de clave de acceso ni una clave de acceso secreta.
CAP (Portal de acceso C2S)	Se utiliza únicamente para C2S S3. Vaya a. "C2S S3: Especificar detalles de autenticación de un pool de almacenamiento en el cloud".

3. Si seleccionó Access Key, introduzca la siguiente información:

Opción	Descripción
ID de clave de acceso	El ID de clave de acceso de la cuenta a la que pertenece el bloque externo.
Clave de acceso secreta	La clave de acceso secreta asociada.

4. En la sección Server Verification, seleccione el método que debe utilizarse para validar el certificado de conexiones TLS con el pool de almacenamiento de cloud:

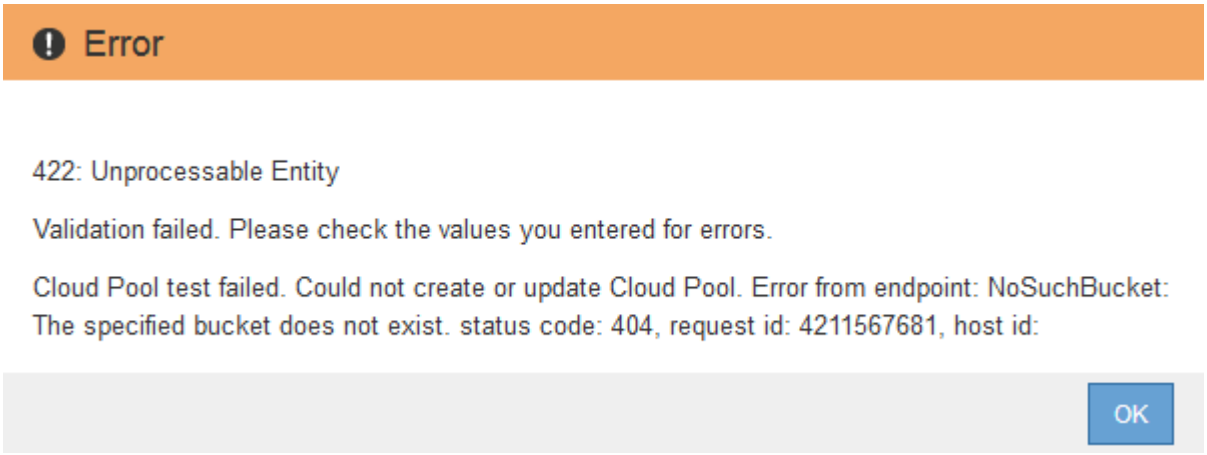
Opción	Descripción
Utilizar certificado de CA del sistema operativo	Utilice los certificados de CA predeterminados instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Haga clic en **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

5. Haga clic en **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el bloque y el extremo de servicio existen y que se pueden alcanzar utilizando las credenciales especificadas.
- Escribe un archivo de marcador en el bloque para identificar el bloque como un pool de almacenamiento en el cloud. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se puede informar un error si existe un error de certificado o si el bloque especificado no existe todavía.



Consulte las instrucciones para solucionar problemas de Cloud Storage Pools, solucionar el problema y vuelva a intentar guardar el pool de almacenamiento en cloud.

Información relacionada

"Solución de problemas de Cloud Storage Pools"

C2S S3: Especificar detalles de autenticación de un pool de almacenamiento en el cloud

Para utilizar el servicio S3 de Commercial Cloud Services (C2S) como un Pool de almacenamiento en cloud, debe configurar C2S Access Portal (CAP) como el tipo de autenticación, de modo que StorageGRID pueda solicitar credenciales temporales para acceder al bloque de S3 de su cuenta C2S.

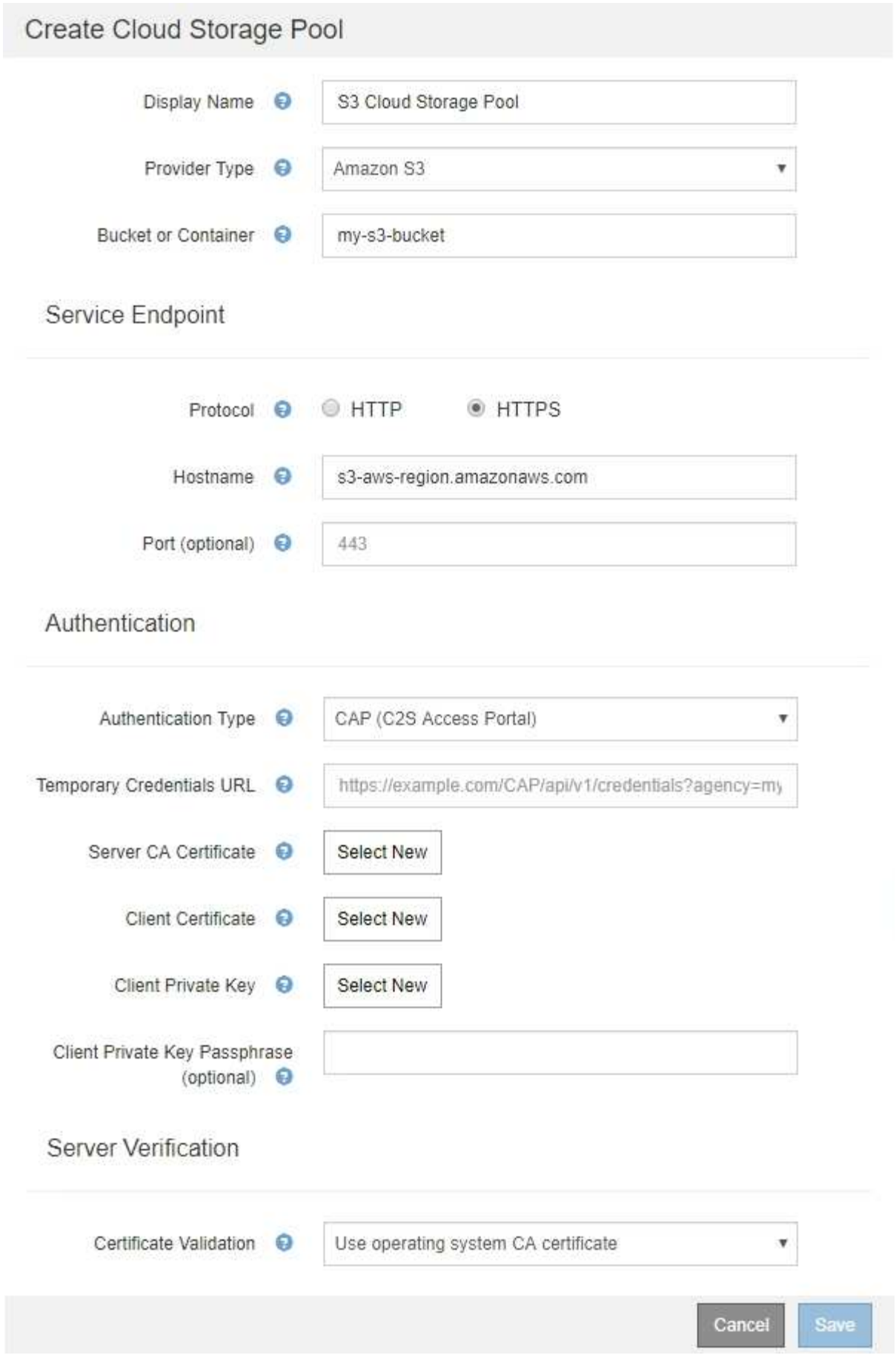
Lo que necesitará

- Introdujo la información básica de un pool de almacenamiento en cloud de Amazon S3, incluido el extremo de servicio.
- Debe conocer la dirección URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
- Debe tener un certificado de CA de servidor emitido por una CA correspondiente. StorageGRID utiliza este certificado para comprobar la identidad del servidor CAP. El certificado de CA del servidor debe utilizar la codificación PEM.
- Debe tener un certificado de cliente emitido por una entidad de certificación gubernamental (CA) correspondiente. StorageGRID utiliza este certificado para identificarse al servidor CAP. El certificado de cliente debe utilizar la codificación PEM y debe tener acceso a su cuenta C2S.
- Debe tener una clave privada codificada en PEM para el certificado de cliente.
- Si la clave privada del certificado de cliente está cifrada, debe tener la frase de contraseña para descifrarla.

Pasos

1. En la sección **autenticación**, seleccione **CAP (Portal de acceso de C2S)** en el menú desplegable **Tipo de autenticación**.

   Aparecen los campos de autenticación CAP C2S.


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. Proporcione la siguiente información:
   a. Para **URL de credenciales temporales**, introduzca la dirección URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
   b. Para **Certificado CA de servidor**, haga clic en **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM que StorageGRID utilizará para verificar el servidor CAP.
   c. Para **Certificado de cliente**, haga clic en **Seleccionar nuevo** y cargue el certificado codificado con PEM que StorageGRID utilizará para identificarse al servidor CAP.
   d. Para **clave privada de cliente**, haga clic en **Seleccionar nuevo** y cargue la clave privada codificada con PEM para el certificado de cliente.

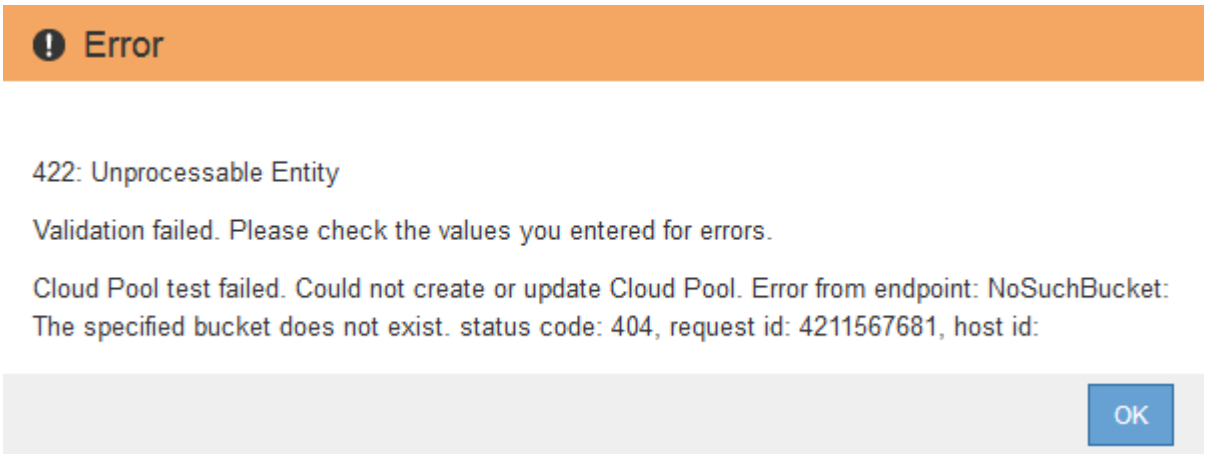
      Si la clave privada está cifrada, se debe utilizar el formato tradicional. (No se admite el formato cifrado PKCS #8).

   e. Si la clave privada del cliente está cifrada, introduzca la frase de acceso para descifrar la clave privada del cliente. De lo contrario, deje en blanco el campo **frase de paso de clave privada cliente**.
3. En la sección Server Verification, introduzca la siguiente información:
   a. Para **validación de certificados**, seleccione **utilizar certificado de CA personalizado**.
   b. Haga clic en **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM.
4. Haga clic en **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el bloque y el extremo de servicio existen y que se pueden alcanzar utilizando las credenciales especificadas.
- Escribe un archivo de marcador en el bloque para identificar el bloque como un pool de almacenamiento en el cloud. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se puede informar un error si existe un error de certificado o si el bloque especificado no existe todavía.



Consulte las instrucciones para solucionar problemas de Cloud Storage Pools, solucionar el problema y vuelva a intentar guardar el pool de almacenamiento en cloud.

Información relacionada

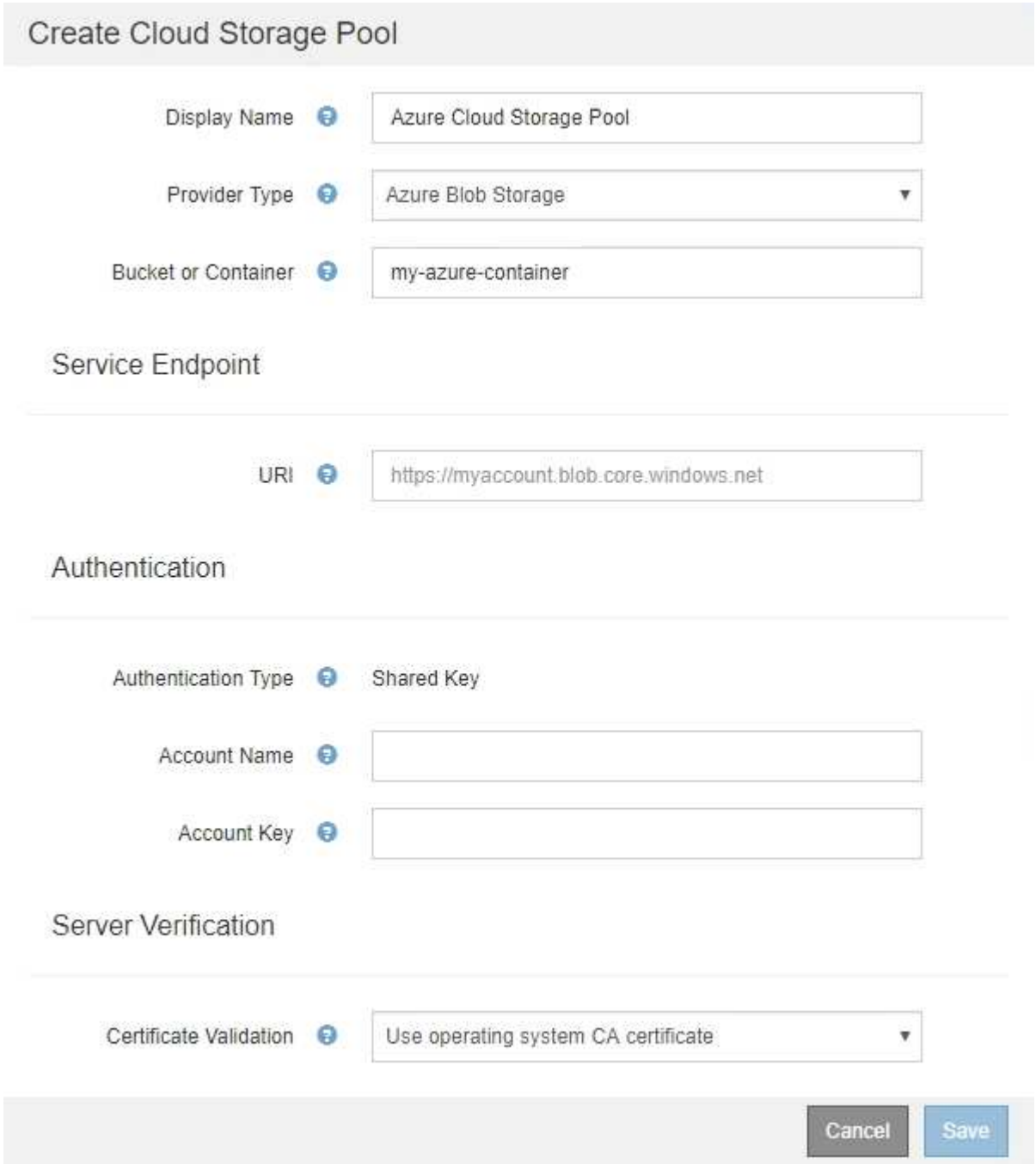
"Solución de problemas de Cloud Storage Pools"

Azure: Especificar detalles de autenticación para un pool de almacenamiento en cloud

Cuando crea un Cloud Storage Pool para el almacenamiento BLOB de Azure, debe especificar un nombre de cuenta y una clave de cuenta para el contenedor externo que StorageGRID utilizará para almacenar objetos.

Lo que necesitará

- Debe haber introducido la información básica para Cloud Storage Pool y ha especificado **Azure Blob Storage** como tipo de proveedor. **Clave compartida** aparece en el campo **Tipo de autenticación**.



- Debe conocer el identificador uniforme de recursos (URI) que se utiliza para acceder al contenedor de almacenamiento BLOB que se utiliza para el pool de almacenamiento de cloud.
- Debe conocer el nombre de la cuenta de almacenamiento y la clave secreta. Puede usar el portal de Azure para encontrar estos valores.

Pasos

1. En la sección **Service Endpoint**, introduzca el Identificador uniforme de recursos (URI) que se utiliza para acceder al contenedor de almacenamiento BLOB utilizado para el Pool de almacenamiento en la nube.

   Especifique el URI en uno de los siguientes formatos:

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

   Si no especifica un puerto, el puerto 443 se utiliza de manera predeterminada para los URI HTTPS y el puerto 80 se utiliza para los URI HTTP. + + **ejemplo URI para el contenedor de almacenamiento Azure Blob**:
   `https://myaccount.blob.core.windows.net`

2. En la sección **autenticación**, proporcione la siguiente información:

   a. Para **Nombre de cuenta**, introduzca el nombre de la cuenta de almacenamiento Blob que posee el contenedor de servicios externo.

   b. Para **clave de cuenta**, introduzca la clave secreta de la cuenta de almacenamiento Blob.

   Para los extremos de Azure, se debe usar la autenticación de clave compartida.

3. En la sección **verificación del servidor**, seleccione el método que debe utilizarse para validar el certificado para las conexiones TLS con el grupo de almacenamiento en la nube:

Opción	Descripción
Utilizar certificado de CA del sistema operativo	Utilice los certificados de CA predeterminados instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Haga clic en **Seleccionar nuevo** y cargue el certificado codificado con PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

4. Haga clic en **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el contenedor y el URI existen y que se puede alcanzar utilizando las credenciales especificadas.
- Escribe un archivo marcador en el contenedor para identificarlo como un pool de almacenamiento en el cloud. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, es posible que se notifique un error si existe un error de certificado o el contenedor

especificado no existe todavía.

Consulte las instrucciones para solucionar problemas de Cloud Storage Pools, solucionar el problema y vuelva a intentar guardar el pool de almacenamiento en cloud.

Información relacionada

"Solución de problemas de Cloud Storage Pools"

Editar un pool de almacenamiento en el cloud

Puede editar un pool de almacenamiento en cloud para cambiar su nombre, extremo de servicio u otros detalles; sin embargo, no puede cambiar el bloque de S3 o el contenedor de Azure para un pool de almacenamiento en cloud.

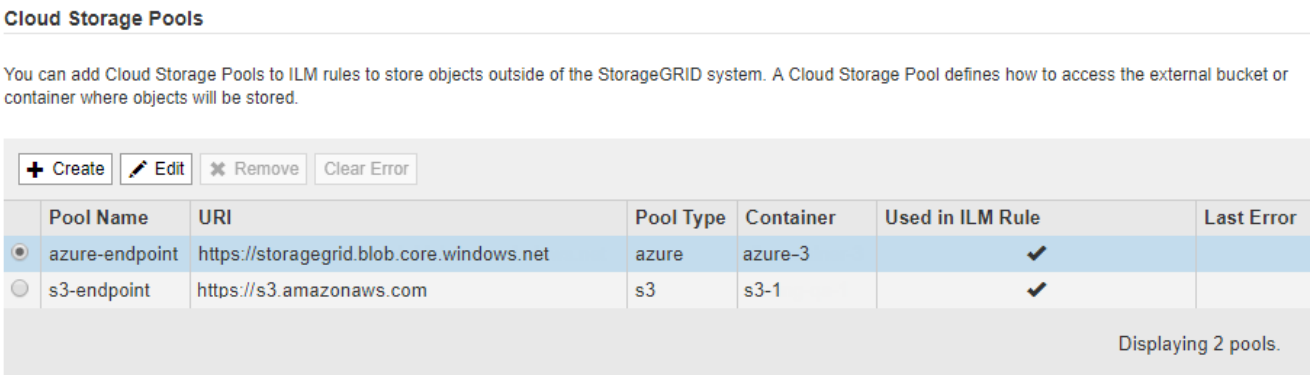
Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe haber revisado las directrices para la configuración de Cloud Storage Pools.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools. En la tabla Cloud Storage Pools, se enumera los pools de almacenamiento en el cloud.



2. Seleccione el botón de opción del pool de almacenamiento en cloud que desea editar.
3. Haga clic en **Editar**.
4. Según sea necesario, cambie el nombre para mostrar, el extremo de servicio, las credenciales de autenticación o el método de validación de certificados.

   > No puede cambiar el tipo de proveedor, ni el bloque de S3 o el contenedor de Azure para un pool de almacenamiento en cloud.

   Si ha cargado previamente un certificado de servidor o cliente, puede seleccionar **Ver actual** para revisar el certificado que se está utilizando actualmente.

5. Haga clic en **Guardar**.

   Cuando guarda un pool de almacenamiento en cloud, StorageGRID valida que el bloque o el contenedor y

el extremo de servicio existen, y que se pueden acceder a ellos con las credenciales especificadas.

Si la validación de Cloud Storage Pool falla, se muestra un mensaje de error. Por ejemplo, es posible que se informe un error si existe un error de certificado.

Consulte las instrucciones para solucionar problemas de Cloud Storage Pools, solucionar el problema y vuelva a intentar guardar el pool de almacenamiento en cloud.

Información relacionada

"Consideraciones para Cloud Storage Pools"

"Solución de problemas de Cloud Storage Pools"

Eliminación de un pool de almacenamiento en el cloud

Puede quitar un pool de almacenamiento en cloud que no se utilice en una regla de ILM y que no contenga datos de objetos.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Ha confirmado que el bloque de S3 o el contenedor de Azure no contienen ningún objeto. Se produce un error si intenta quitar un Pool de almacenamiento en cloud si contiene objetos. Consulte «"resolución de problemas de pools de almacenamiento en cloud".

> Cuando se crea un pool de almacenamiento en el cloud, StorageGRID escribe un archivo marcador en el bloque o contenedor para identificarlo como un pool de almacenamiento en el cloud. No elimine este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

- Ya ha quitado todas las reglas de ILM que pueden haber usado el pool.

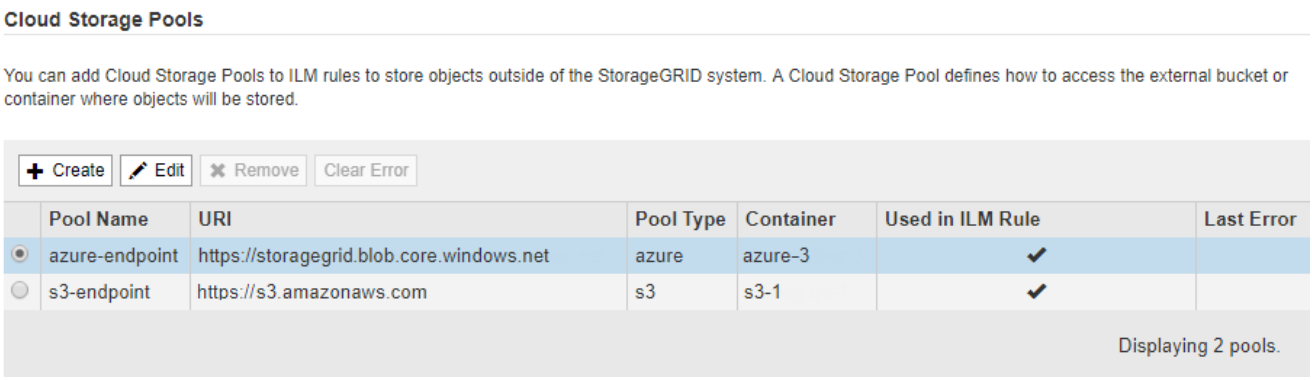
Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools.

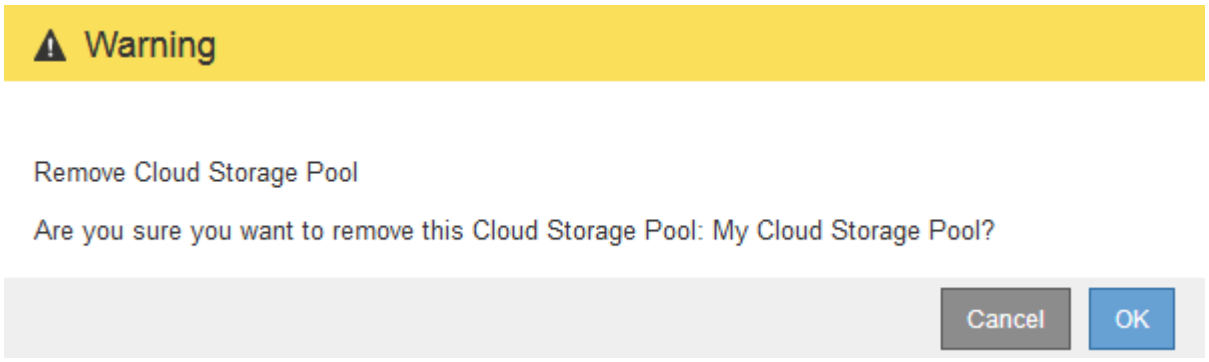
2. Seleccione el botón de opción de un pool de almacenamiento en cloud que no se utilice actualmente en una regla de ILM.

   No puede quitar un pool de almacenamiento en cloud si se utiliza en una regla de ILM. El botón **Quitar** está desactivado.



3. Haga clic en **Quitar**.

   Aparecerá una advertencia de confirmación.



4. Haga clic en **Aceptar**.

   El pool de almacenamiento en cloud se elimina.

Información relacionada

"Solución de problemas de Cloud Storage Pools"

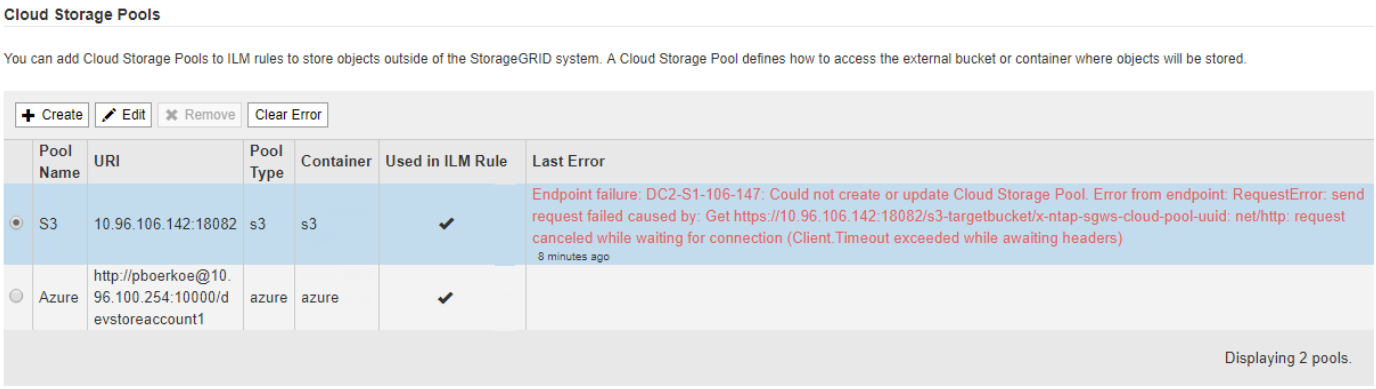
Solución de problemas de Cloud Storage Pools

Si se encuentran errores al crear, editar o eliminar un pool de almacenamiento en el cloud, siga estos pasos para resolver el problema.

Determinar si se ha producido un error

StorageGRID realiza una comprobación simple del estado de cada pool de almacenamiento en cloud una vez por minuto para garantizar que se pueda acceder al pool de almacenamiento en cloud y que funciona correctamente. Si la comprobación del estado detecta un problema, se muestra un mensaje en la columna Last error de la tabla Cloud Storage Pools en la página Storage Pools.

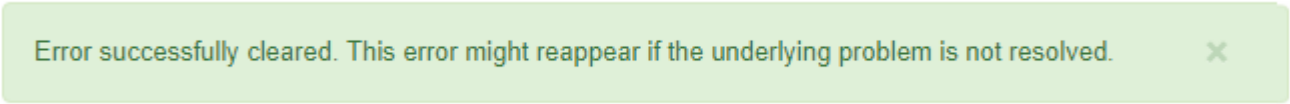
En la tabla, se muestra el error más reciente detectado para cada pool de almacenamiento en cloud e indica cuánto tiempo se produjo el error.



Además, se activa una alerta de error * de conectividad del grupo de almacenamiento en cloud* si la comprobación del estado detecta que se han producido uno o varios errores nuevos de Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya a la página del grupo de almacenamiento (seleccione **ILM** > **agrupaciones de almacenamiento**), revise los mensajes de error en la columna último error y consulte las siguientes directrices para la solución de problemas.

Comprobar si se ha solucionado un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. En la página Cloud Storage Pool, seleccione el botón de opción del extremo y haga clic en **Borrar error**. Un mensaje de confirmación indica que StorageGRID borró el error para el pool de almacenamiento en el cloud.



Si se ha resuelto el problema subyacente, ya no se muestra el mensaje de error. Sin embargo, si el problema subyacente no se ha solucionado (o si se encuentra un error diferente), el mensaje de error aparecerá en la columna último error en unos minutos.

Error: Este pool de almacenamiento en cloud contiene contenido inesperado

Es posible ver este mensaje de error cuando se intenta crear, editar o eliminar un pool de almacenamiento en cloud. Este error se produce si el cucharón o el contenedor incluye `x-ntap-sgws-cloud-pool-uuid` Archivo marcador, pero ese archivo no tiene el UUID esperado.

Por lo general, solo verá este error si crea un nuevo pool de almacenamiento en el cloud y otra instancia de StorageGRID ya utiliza el mismo pool de almacenamiento en el cloud.

Intente realizar estos pasos para corregir el problema:

- Compruebe que nadie de su organización utiliza también este pool de almacenamiento en el cloud.
- Elimine el `x-ntap-sgws-cloud-pool-uuid` Archivo e intente configurar de nuevo el Pool de almacenamiento en la nube.

Error: No se pudo crear o actualizar Cloud Storage Pool. Error desde el punto final

Es posible ver este mensaje de error cuando se intenta crear o editar un pool de almacenamiento en el cloud. Este error indica que algún problema de conectividad o configuración impide que StorageGRID escriba en el pool de almacenamiento en el cloud.

Para corregir el problema, revise el mensaje de error desde el punto final.

- Si el mensaje de error contiene `Get *url*: EOF`, Compruebe que el extremo de servicio utilizado para el grupo de almacenamiento en la nube no utiliza el protocolo HTTP para un contenedor o bloque que requiere HTTPS.
- Si el mensaje de error contiene `Get *url*: net/http: request canceled while waiting for connection`, Compruebe que la configuración de red permite a los nodos de almacenamiento acceder al extremo de servicio utilizado para el grupo de almacenamiento en la nube.
- Para todos los demás mensajes de error de punto final, intente uno o más de los siguientes:
  - Cree un contenedor o bloque externo con el mismo nombre que introdujo para el Cloud Storage Pool e intente guardar de nuevo el nuevo Cloud Storage Pool.
  - Corrija el nombre de contenedor o bloque que especificó para Cloud Storage Pool e intente guardar de nuevo el nuevo pool de almacenamiento en cloud.

Error: No se pudo analizar el certificado de CA

Es posible ver este mensaje de error cuando se intenta crear o editar un pool de almacenamiento en el cloud. El error se produce si StorageGRID no pudo analizar el certificado introducido al configurar el pool de almacenamiento en cloud.

Para corregir el problema, compruebe el certificado de CA que proporcionó para los problemas.

Error: No se encontró un pool de almacenamiento en cloud con este ID

Es posible ver este mensaje de error cuando se intenta editar o eliminar un pool de almacenamiento en el cloud. Este error se produce si el extremo devuelve una respuesta 404, que puede significar cualquiera de las siguientes:

- Las credenciales utilizadas para Cloud Storage Pool no tienen permiso de lectura para el bloque.
- El bloque utilizado para el pool de almacenamiento en cloud no incluye el `x-ntap-sgws-cloud-pool-uuid` archivo de marcador.

Intente uno o más de estos pasos para corregir el problema:

- Compruebe que el usuario asociado a la clave de acceso configurada tenga los permisos necesarios.
- Edite el pool de almacenamiento cloud con credenciales que tengan los permisos necesarios.
- Si los permisos son correctos, póngase en contacto con el servicio de soporte técnico.

Error: No se ha podido comprobar el contenido del pool de almacenamiento en cloud. Error desde el punto final

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. Este error indica que algún problema de conectividad o configuración impide que StorageGRID lea el contenido del bucket de Cloud Storage Pool.

Para corregir el problema, revise el mensaje de error desde el punto final.

Error: Los objetos ya se han colocado en este cucharón

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. No

puede eliminar un pool de almacenamiento en cloud si contiene datos que se movieron a este punto por ILM, datos que estaban en el bloque antes de configurar el Cloud Storage Pool o datos que algún otro origen colocó en el bloque después de crear el Cloud Storage Pool.

Intente uno o más de estos pasos para corregir el problema:

- Siga las instrucciones para devolver objetos a StorageGRID en «"ciclo de vida de un objeto de agrupación de almacenamiento en cloud"».
- Si está seguro de que ILM no colocó los objetos restantes en el Cloud Storage Pool, elimine manualmente los objetos del bloque.

> No elimine nunca manualmente objetos de un pool de almacenamiento en cloud que haya colocado allí ILM. Si más adelante intenta acceder a un objeto eliminado manualmente desde StorageGRID, no se encuentra el objeto eliminado.

Error: El proxy encontró un error externo al intentar acceder al pool de almacenamiento de cloud

Es posible ver este mensaje de error si se configuró un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el extremo externo de S3 utilizado para el pool de almacenamiento en el cloud. Este error ocurre si el servidor proxy externo no puede acceder al extremo de Cloud Storage Pool. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externo.

Intente uno o más de estos pasos para corregir el problema:

- Compruebe la configuración de Cloud Storage Pool (**ILM** > **agrupaciones de almacenamiento**).
- Compruebe la configuración de red del servidor proxy de almacenamiento.

Información relacionada

"Ciclo de vida de un objeto de Cloud Storage Pool"