Utilice grupos de almacenamiento en la nube

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Utilice grupos de almacenamiento en la nube

¿Qué es un pool de almacenamiento en la nube?

Un grupo de almacenamiento en la nube le permite usar ILM para mover datos de objetos fuera de su sistema StorageGRID . Por ejemplo, es posible que desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor costo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivo en el almacenamiento de blobs de Microsoft Azure. O bien, es posible que desee mantener una copia de seguridad en la nube de los objetos StorageGRID para mejorar la recuperación ante desastres.

Desde una perspectiva ILM, un grupo de almacenamiento en la nube es similar a un grupo de almacenamiento. Para almacenar objetos en cualquiera de las ubicaciones, seleccione el grupo al crear las instrucciones de ubicación para una regla ILM. Sin embargo, mientras que los grupos de almacenamiento constan de nodos de almacenamiento dentro del sistema StorageGRID , un grupo de almacenamiento en la nube consta de un depósito externo (S3) o contenedor (almacenamiento de blobs de Azure).

La tabla compara los grupos de almacenamiento con los grupos de almacenamiento en la nube y muestra las similitudes y diferencias de alto nivel.

	Pool de almacenamiento	**Grupo de almacenamiento en la nube**
¿Cómo se crea?	Usando la opción **ILM** > **Grupos de almacenamiento** en el Administrador de Grid.	Usando la opción **ILM** > **Grupos de almacenamiento** > **Grupos de almacenamiento en la nube** en Grid Manager. Debe configurar el contenedor o depósito externo antes de poder crear el grupo de almacenamiento en la nube.
¿Cuántos pools puedes crear?	Ilimitado.	Hasta 10.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento dentro de StorageGRID.	En un bucket de Amazon S3, un contenedor de almacenamiento de blobs de Azure o un Google Cloud externo al sistema StorageGRID . Si el grupo de almacenamiento en la nube es un bucket de Amazon S3: • Opcionalmente, puede configurar un ciclo de vida de depósito para trasladar objetos a un almacenamiento a largo plazo y de bajo costo, como Amazon S3 Glacier o S3 Glacier Deep Archive. El sistema de almacenamiento externo debe ser compatible con la clase de almacenamiento Glacier y la API S3 RestoreObject. • Puede crear grupos de almacenamiento en la nube para usar con AWS Commercial Cloud Services (C2S), que admite la región secreta de AWS. Si el grupo de almacenamiento en la nube es un contenedor de almacenamiento de blobs de Azure, StorageGRID traslada el objeto al nivel de archivo. **Nota:** En general, no configure la administración del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado para un grupo de almacenamiento en la nube. Las operaciones de restauración de objetos en el grupo de almacenamiento en la nube pueden verse afectadas por el ciclo de vida configurado.
¿Qué controla la ubicación de los objetos?	Una regla ILM en las políticas ILM activas.	Una regla ILM en las políticas ILM activas.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.
¿Cuántas copias de cada objeto están permitidas?	Múltiple.	Una copia en el grupo de almacenamiento en la nube y, opcionalmente, una o más copias en StorageGRID. **Nota:** No es posible almacenar un objeto en más de un grupo de almacenamiento en la nube al mismo tiempo.
¿Cuales son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste. **Nota**: Los datos de FabricPool no se pueden agrupar en grupos de almacenamiento en la nube.

Ciclo de vida de un objeto de grupo de almacenamiento en la nube

Antes de implementar grupos de almacenamiento en la nube, revise el ciclo de vida de los objetos que se almacenan en cada tipo de grupo de almacenamiento en la nube.

S3: Ciclo de vida de un objeto de grupo de almacenamiento en la nube

Los pasos describen las etapas del ciclo de vida de un objeto almacenado en un grupo de almacenamiento en la nube S3.

> "Glacier" se refiere tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: la clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración acelerada. Solo se admite la recuperación masiva o estándar.

> Google Cloud Platform (GCP) admite la recuperación de objetos del almacenamiento a largo plazo sin necesidad de una operación de restauración POST.

1. **Objeto almacenado en StorageGRID**

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

2. **Objeto movido al pool de almacenamiento en la nube S3**
   - Cuando el objeto coincide con una regla ILM que utiliza un grupo de almacenamiento en la nube S3 como su ubicación, StorageGRID mueve el objeto al depósito S3 externo especificado por el grupo de almacenamiento en la nube.
   - Cuando el objeto se ha movido al grupo de almacenamiento en la nube S3, la aplicación cliente puede recuperarlo mediante una solicitud GetObject de S3 desde StorageGRID, a menos que el objeto se haya transferido al almacenamiento Glacier.
3. **Objeto en transición a Glaciar (estado no recuperable)**
   - Opcionalmente, el objeto puede trasladarse al almacenamiento de Glaciar. Por ejemplo, el depósito S3 externo podría usar la configuración del ciclo de vida para trasladar un objeto al almacenamiento de Glacier inmediatamente o después de una cierta cantidad de días.

     > Si desea realizar la transición de objetos, debe crear una configuración de ciclo de vida para el depósito S3 externo y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

   - Durante la transición, la aplicación cliente puede utilizar una solicitud S3 HeadObject para monitorear el estado del objeto.
4. **Objeto restaurado del almacenamiento del glaciar**

   Si un objeto se ha transferido al almacenamiento de Glacier, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable al grupo de almacenamiento en la nube S3. La solicitud especifica cuántos días debe estar disponible la copia en el grupo de almacenamiento en la nube y el nivel de acceso a datos que se utilizará para la operación de restauración (acelerada, estándar o masiva). Cuando se alcanza la fecha de vencimiento de la copia recuperable, la copia vuelve automáticamente a un estado no recuperable.

Si también existen una o más copias del objeto en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde Glacier emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

5. **Objeto recuperado**

   Una vez que se ha restaurado un objeto, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Azure: ciclo de vida de un objeto de grupo de almacenamiento en la nube

Los pasos describen las etapas del ciclo de vida de un objeto almacenado en un grupo de almacenamiento en la nube de Azure.

1. **Objeto almacenado en StorageGRID**

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

2. **Objeto movido al grupo de almacenamiento en la nube de Azure**

   Cuando el objeto coincide con una regla ILM que usa un grupo de almacenamiento en la nube de Azure como su ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento de blobs de Azure externo especificado por el grupo de almacenamiento en la nube.

3. **Objeto en transición al nivel de archivo (estado no recuperable)**

   Inmediatamente después de mover el objeto al grupo de almacenamiento en la nube de Azure, StorageGRID transfiere automáticamente el objeto al nivel de archivo de almacenamiento de blobs de Azure.

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

   Si un objeto se ha trasladado al nivel de archivo, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en el grupo de almacenamiento en la nube de Azure.

   Cuando StorageGRID recibe RestoreObject, transfiere temporalmente el objeto al nivel Esporádico de almacenamiento de blobs de Azure. Tan pronto como se alcanza la fecha de vencimiento en la solicitud RestoreObject, StorageGRID transfiere el objeto nuevamente al nivel de archivo.

   Si una o más copias del objeto también existen en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivo emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

5. **Objeto recuperado**

   Una vez que se ha restaurado un objeto en el grupo de almacenamiento en la nube de Azure, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Información relacionada

"Utilice la API REST de S3"

Cuándo utilizar grupos de almacenamiento en la nube

Al utilizar grupos de almacenamiento en la nube, puede realizar copias de seguridad o agrupar datos en niveles en una ubicación externa. Además, puedes realizar copias de seguridad o agrupar datos en más de una nube.

Realizar una copia de seguridad de los datos de StorageGRID en una ubicación externa

Puede utilizar un grupo de almacenamiento en la nube para realizar copias de seguridad de objetos StorageGRID en una ubicación externa.

Si las copias en StorageGRID son inaccesibles, los datos de los objetos en el grupo de almacenamiento en la nube se pueden usar para atender las solicitudes de los clientes. Sin embargo, es posible que necesite emitir una solicitud S3 RestoreObject para acceder a la copia del objeto de respaldo en el grupo de almacenamiento en la nube.

Los datos de objetos en un grupo de almacenamiento en la nube también se pueden usar para recuperar datos perdidos de StorageGRID debido a una falla del volumen de almacenamiento o del nodo de almacenamiento. Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Para implementar una solución de respaldo:

1. Crear un único grupo de almacenamiento en la nube.
2. Configure una regla ILM que almacene simultáneamente copias de objetos en nodos de almacenamiento (como copias replicadas o codificadas por borrado) y una única copia de objeto en el grupo de almacenamiento en la nube.
3. Añade la regla a tu política ILM. Luego, simule y active la política.

Datos de niveles desde StorageGRID a una ubicación externa

Puede utilizar un grupo de almacenamiento en la nube para almacenar objetos fuera del sistema StorageGRID . Por ejemplo, supongamos que tiene una gran cantidad de objetos que necesita conservar, pero espera acceder a ellos en raras ocasiones, o nunca. Puede utilizar un grupo de almacenamiento en la nube para organizar los objetos en un almacenamiento de menor costo y liberar espacio en StorageGRID.

Para implementar una solución de niveles:

1. Crear un único grupo de almacenamiento en la nube.
2. Configure una regla ILM que mueva objetos rara vez utilizados desde los nodos de almacenamiento al grupo de almacenamiento en la nube.
3. Añade la regla a tu política ILM. Luego, simule y active la política.

Mantener múltiples puntos finales en la nube

Puede configurar varios puntos finales de Cloud Storage Pool si desea organizar en niveles o realizar copias de seguridad de datos de objetos en más de una nube. Los filtros en sus reglas ILM le permiten especificar qué objetos se almacenan en cada grupo de almacenamiento en la nube. Por ejemplo, es posible que desee almacenar objetos de algunos inquilinos o buckets en Amazon S3 Glacier y objetos de otros inquilinos o

buckets en Azure Blob Storage. O bien, es posible que desee mover datos entre Amazon S3 Glacier y Azure Blob Storage.

> Al utilizar varios puntos finales de un grupo de almacenamiento en la nube, tenga en cuenta que un objeto solo se puede almacenar en un grupo de almacenamiento en la nube a la vez.

Para implementar múltiples puntos finales en la nube:

1. Crea hasta 10 grupos de almacenamiento en la nube.
2. Configure las reglas de ILM para almacenar los datos de objetos adecuados en el momento adecuado en cada grupo de almacenamiento en la nube. Por ejemplo, almacene objetos del depósito A en el grupo de almacenamiento en la nube A y almacene objetos del depósito B en el grupo de almacenamiento en la nube B. O bien, almacene objetos en el grupo de almacenamiento en la nube A durante un período de tiempo y luego muévalos al grupo de almacenamiento en la nube B.
3. Añade las reglas a tu política de ILM. Luego, simule y active la política.

Consideraciones para los grupos de almacenamiento en la nube

Si planea utilizar un grupo de almacenamiento en la nube para mover objetos fuera del sistema StorageGRID , debe revisar las consideraciones para configurar y usar grupos de almacenamiento en la nube.

Consideraciones generales

- En general, el almacenamiento de archivo en la nube, como Amazon S3 Glacier o Azure Blob Storage, es un lugar económico para almacenar datos de objetos. Sin embargo, los costos de recuperar datos del almacenamiento de archivos en la nube son relativamente altos. Para lograr el costo general más bajo, debe considerar cuándo y con qué frecuencia accederá a los objetos en el grupo de almacenamiento en la nube. Se recomienda utilizar un grupo de almacenamiento en la nube solo para contenido al que se espera acceder con poca frecuencia.
- No se admite el uso de grupos de almacenamiento en la nube con FabricPool debido a la latencia adicional para recuperar un objeto del destino del grupo de almacenamiento en la nube.
- Los objetos que tienen habilitado el bloqueo de objetos S3 no se pueden colocar en grupos de almacenamiento en la nube.
- Si el depósito S3 de destino de un grupo de almacenamiento en la nube tiene habilitado el bloqueo de objetos S3, el intento de configurar la replicación del depósito (PutBucketReplication) fallará con un error AccessDenied.
- Las siguientes combinaciones de plataforma, autenticación y protocolo con bloqueo de objetos S3 no son compatibles con los grupos de almacenamiento en la nube:
  - **Plataformas**: Google Cloud Platform y Azure
  - **Tipos de autenticación**: Roles de IAM en cualquier lugar y acceso anónimo
  - **Protocolo**: HTTP

Consideraciones sobre los puertos utilizados para los grupos de almacenamiento en la nube

Para garantizar que las reglas ILM puedan mover objetos hacia y desde el grupo de almacenamiento en la nube especificado, debe configurar la red o las redes que contienen los nodos de almacenamiento de su sistema. Debe asegurarse de que los siguientes puertos puedan comunicarse con el grupo de almacenamiento en la nube.

De forma predeterminada, los grupos de almacenamiento en la nube utilizan los siguientes puertos:

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

Puede especificar un puerto diferente al crear o editar un grupo de almacenamiento en la nube.

Si utiliza un servidor proxy no transparente, también debe"configurar un proxy de almacenamiento" para permitir que se envíen mensajes a puntos finales externos, como un punto final en Internet.

Consideraciones sobre los costos

El acceso al almacenamiento en la nube mediante un Cloud Storage Pool requiere conectividad de red a la nube. Debe considerar el costo de la infraestructura de red que utilizará para acceder a la nube y aprovisionarla adecuadamente, en función de la cantidad de datos que espera mover entre StorageGRID y la nube mediante el grupo de almacenamiento en la nube.

Cuando StorageGRID se conecta al punto final del grupo de almacenamiento en la nube externo, emite varias solicitudes para monitorear la conectividad y garantizar que pueda realizar las operaciones necesarias. Si bien estas solicitudes implicarán algunos costos adicionales, el costo de monitorear un grupo de almacenamiento en la nube debería ser solo una pequeña fracción del costo total de almacenar objetos en S3 o Azure.

Es posible que se produzcan costos más significativos si necesita mover objetos desde un punto final de un grupo de almacenamiento en la nube externo a StorageGRID. Los objetos se pueden mover nuevamente a StorageGRID en cualquiera de estos casos:

- La única copia del objeto está en un grupo de almacenamiento en la nube y usted decide almacenar el objeto en StorageGRID . En este caso, reconfigura tus reglas y políticas de ILM. Cuando se produce la evaluación de ILM, StorageGRID emite varias solicitudes para recuperar el objeto del grupo de almacenamiento en la nube. Luego, StorageGRID crea localmente la cantidad especificada de copias replicadas o codificadas por borrado. Una vez que el objeto se mueve nuevamente a StorageGRID, se elimina la copia en el grupo de almacenamiento en la nube.
- Los objetos se pierden debido a una falla del nodo de almacenamiento. Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

> ⓘ Cuando los objetos se mueven nuevamente a StorageGRID desde un grupo de almacenamiento en la nube, StorageGRID emite múltiples solicitudes al punto final del grupo de almacenamiento en la nube para cada objeto. Antes de mover grandes cantidades de objetos, comuníquese con el soporte técnico para obtener ayuda para estimar el tiempo y los costos asociados.

S3: Permisos necesarios para el depósito del grupo de almacenamiento en la nube

Las políticas para el depósito S3 externo utilizado para un grupo de almacenamiento en la nube deben otorgarle a StorageGRID permiso para mover un objeto al depósito, obtener el estado de un objeto, restaurar un objeto desde el almacenamiento de Glacier cuando sea necesario, etc. Idealmente, StorageGRID debería tener acceso de control total al depósito.(`s3:*`); sin embargo, si esto no es posible, la política del bucket debe otorgar 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 depósito externo

El movimiento de objetos entre StorageGRID y el depósito S3 externo especificado en el grupo de almacenamiento en la nube está controlado por las reglas de ILM y las políticas de ILM activas en StorageGRID. Por el contrario, la transición de objetos del depósito S3 externo especificado en el grupo de almacenamiento en la nube a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implementa la clase de almacenamiento Glacier) está controlada por la configuración del ciclo de vida de ese depósito.

Si desea realizar la transición de objetos desde el grupo de almacenamiento en la nube, debe crear la configuración de ciclo de vida adecuada en el depósito S3 externo y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

Por ejemplo, supongamos que desea que todos los objetos que se mueven desde StorageGRID al grupo de almacenamiento en la nube se transfieran al almacenamiento de Amazon S3 Glacier de inmediato. Debe crear una configuración de ciclo de vida en el depósito S3 externo que especifique una única acción (**Transición**) de la siguiente manera:

```
<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 trasladaría todos los objetos de bucket a Amazon S3 Glacier el día en que se crearon (es decir, el día en que se trasladaron de StorageGRID al Cloud Storage Pool).

> Al configurar el ciclo de vida del depósito externo, nunca utilice acciones **Expiración** para definir cuándo expiran los objetos. Las acciones de expiración hacen que el sistema de almacenamiento externo elimine los objetos expirados. Si posteriormente intenta acceder a un objeto caducado desde StorageGRID, no se encontrará el objeto eliminado.

Si desea transferir objetos del grupo de almacenamiento en la nube a S3 Glacier Deep Archive (en lugar de a Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida del bucket. Sin embargo, tenga en cuenta que no puede utilizar el `Expedited` Nivel para restaurar objetos del Archivo S3 Glacier Deep.

Azure: Consideraciones para el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puede establecer el nivel de acceso predeterminado en Activo o Esporádico. Al crear una cuenta de almacenamiento para usarla con un grupo de almacenamiento en la nube, debe utilizar el nivel Activo como nivel predeterminado. Si bien StorageGRID establece inmediatamente el nivel en Archivo cuando mueve objetos al grupo de almacenamiento en la nube, el uso de una configuración predeterminada de Activo garantiza que no se le cobrará una tarifa de eliminación anticipada por los objetos eliminados del nivel Fresco antes del mínimo de 30 días.

Azure: No se admite la gestión del ciclo de vida

No utilice la administración del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado con un grupo de almacenamiento en la nube. Las operaciones del ciclo de vida podrían interferir con las operaciones del grupo de almacenamiento en la nube.

Información relacionada

"Crear un grupo de almacenamiento en la nube"

Comparar los grupos de almacenamiento en la nube y la replicación de CloudMirror

A medida que comience a utilizar los grupos de almacenamiento en la nube, puede resultar útil comprender las similitudes y diferencias entre los grupos de almacenamiento en la nube y el servicio de replicación StorageGRID CloudMirror.

	Grupo de almacenamiento en la nube	Servicio de replicación CloudMirror
¿Cuál es el propósito principal?	Actúa como un objetivo de archivo. La copia del objeto en el grupo de almacenamiento en la nube puede ser la única copia del objeto o puede ser una copia adicional. Es decir, en lugar de mantener dos copias en el sitio, puede mantener una copia dentro de StorageGRID y enviar una copia al grupo de almacenamiento en la nube.	Permite que un inquilino replique automáticamente objetos desde un depósito en StorageGRID (origen) a un depósito S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente.
¿Cómo está configurado?	Se define de la misma manera que los grupos de almacenamiento, utilizando Grid Manager o la API de administración de Grid. Se puede seleccionar como ubicación de colocación en una regla ILM. Mientras que un grupo de almacenamiento consta de un grupo de nodos de almacenamiento, un grupo de almacenamiento en la nube se define mediante un punto final remoto de S3 o Azure (dirección IP, credenciales, etc.).	Un usuario inquilino"configura la replicación de CloudMirror" definiendo un punto final de CloudMirror (dirección IP, credenciales, etc.) mediante el Administrador de inquilinos o la API S3. Una vez configurado el punto final de CloudMirror, cualquier depósito propiedad de esa cuenta de inquilino se puede configurar para apuntar al punto final de CloudMirror.
¿Quién es responsable de configurarlo?	Por lo general, un administrador de red	Normalmente, un usuario inquilino
¿Cual es el destino?	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Nivel de archivo de blobs de Azure • Plataforma de Google Cloud (GCP)	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Plataforma de Google Cloud (GCP)
¿Qué hace que los objetos se muevan al destino?	Una o más reglas ILM en las políticas ILM activas. Las reglas de ILM definen qué objetos StorageGRID mueve al grupo de almacenamiento en la nube y cuándo se mueven los objetos.	El acto de ingerir un nuevo objeto en un depósito de origen que se ha configurado con un punto final de CloudMirror. Los objetos que existían en el depósito de origen antes de que este se configurara con el punto final de CloudMirror no se replican, a menos que se modifiquen.

	Grupo de almacenamiento en la nube	Servicio de replicación CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones deben realizar solicitudes a StorageGRID para recuperar objetos que se han movido a un grupo de almacenamiento en la nube. Si la única copia de un objeto se ha transferido al almacenamiento de archivo, StorageGRID administra el proceso de restauración del objeto para que pueda recuperarse.	Dado que la copia reflejada en el depósito de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes a StorageGRID o al destino S3. Por ejemplo, supongamos que utiliza la replicación de CloudMirror para reflejar objetos en una organización asociada. El socio puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario utilizar StorageGRID .
¿Puedes leer desde el destino directamente?	No. Los objetos trasladados a un grupo de almacenamiento en la nube son administrados por StorageGRID. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del grupo de almacenamiento en la nube).	Sí, porque la copia reflejada es una copia independiente.
¿Qué sucede si se elimina un objeto de la fuente?	El objeto también se elimina del grupo de almacenamiento en la nube.	La acción de eliminar no se replica. Un objeto eliminado ya no existe en el depósito StorageGRID , pero continúa existiendo en el depósito de destino. De manera similar, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.
¿Cómo acceder a los objetos después de un desastre (el sistema StorageGRID no está operativo)?	Los nodos StorageGRID fallidos deben recuperarse. Durante este proceso, se pueden restaurar copias de objetos replicados utilizando las copias en el grupo de almacenamiento en la nube.	Las copias de objetos en el destino CloudMirror son independientes de StorageGRID, por lo que se puede acceder a ellas directamente antes de que se recuperen los nodos de StorageGRID .

Crear un grupo de almacenamiento en la nube

Un grupo de almacenamiento en la nube especifica un único depósito externo de Amazon S3 u otro proveedor compatible con S3 o un contenedor de almacenamiento de blobs de Azure.

Cuando se crea un grupo de almacenamiento en la nube, se especifica el nombre y la ubicación del contenedor o depósito externo que StorageGRID usará para almacenar objetos, el tipo de proveedor de nube (Amazon S3/GCP o Azure Blob Storage) y la información que StorageGRID necesita para acceder al contenedor o depósito externo.

StorageGRID valida el grupo de almacenamiento en la nube tan pronto como lo guarda, por lo que debe

asegurarse de que el depósito o contenedor especificado en el grupo de almacenamiento en la nube exista y sea accesible.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"permisos de acceso necesarios" .
- Usted ha revisado el"Consideraciones para los grupos de almacenamiento en la nube" .
- El contenedor o depósito externo al que hace referencia el grupo de almacenamiento en la nube ya existe y usted tiene lainformación del punto final del servicio .
- Para acceder al cubo o contenedor, tienes elInformación de la cuenta para el tipo de autenticación Tú elegirás.

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento** > **Grupos de almacenamiento en la nube**.
2. Seleccione **Crear**, luego ingrese la siguiente información:

Campo	Descripción
Nombre del grupo de almacenamiento en la nube	Un nombre que describe brevemente el grupo de almacenamiento en la nube y su propósito. Utilice un nombre que sea fácil de identificar cuando configure las reglas de ILM.
Tipo de proveedor	¿Qué proveedor de nube utilizará para este grupo de almacenamiento en la nube? • **Amazon S3/GCP**: seleccione esta opción para un proveedor de Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • **Almacenamiento de blobs de Azure**
Cubo o contenedor	El nombre del depósito S3 externo o del contenedor de Azure. No es posible cambiar este valor una vez guardado el grupo de almacenamiento en la nube.

3. Según su selección del tipo de proveedor, ingrese la información del punto final del servicio.

Amazon S3/GCP

a. Para el protocolo, seleccione HTTPS o HTTP.

> No utilice conexiones HTTP para datos confidenciales.

b. Introduzca el nombre del host. Ejemplo:

`s3-aws-region.amazonaws.com`

c. Seleccione el estilo de URL:

Opción	Descripción
Detección automática	Intente detectar automáticamente qué estilo de URL utilizar, según la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una URL de estilo ruta. Seleccione esta opción solo si no sabe qué estilo específico usar.
Estilo alojado virtualmente	Utilice una URL de estilo alojado virtualmente para acceder al depósito. Las URL de estilo alojado virtualmente incluyen el nombre del depósito como parte del nombre de dominio. Ejemplo: `https://bucket-name.s3.company.com/key-name`
Estilo de ruta	Utilice una URL de estilo de ruta para acceder al depósito. Las URL de estilo de ruta incluyen el nombre del depósito al final. Ejemplo: `https://s3.company.com/bucket-name/key-name` **Nota:** La opción de URL de estilo de ruta no se recomienda y quedará obsoleta en una versión futura de StorageGRID.

d. Opcionalmente, ingrese el número de puerto o utilice el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de blobs de Azure

a. Utilice uno de los siguientes formatos para ingresar el URI del punto final del servicio.

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

Ejemplo: `https://myaccount.blob.core.windows.net:443`

Si no especifica un puerto, de manera predeterminada se utiliza el puerto 443 para HTTPS y el puerto 80 para HTTP.

4. Seleccione **Continuar**. Luego, seleccione el tipo de autenticación e ingrese la información requerida para el punto final del grupo de almacenamiento en la nube:

Tecla de acceso

Para Amazon S3/GCP u otro proveedor compatible con S3

a. **ID de clave de acceso**: Ingrese el ID de clave de acceso para la cuenta que posee el depósito externo.
b. **Clave de acceso secreta**: Ingrese la clave de acceso secreta.

Roles de IAM en cualquier lugar

Para el servicio AWS IAM Roles Anywhere

StorageGRID utiliza el Servicio de token de seguridad de AWS (STS) para generar dinámicamente un token de corta duración para acceder a los recursos de AWS.

a. **Región de AWS IAM Roles Anywhere**: seleccione la región para el grupo de almacenamiento en la nube. Por ejemplo, `us-east-1` .
b. **URN de ancla de confianza**: ingrese la URN del ancla de confianza que valida las solicitudes de credenciales STS de corta duración. Puede ser una CA raíz o intermedia.
c. **URN de perfil**: ingrese la URN del perfil de IAM Roles Anywhere que enumera los roles que pueden asumirse para cualquier persona de confianza.
d. **URN de rol**: Ingrese el URN del rol de IAM que puede asumir cualquier persona de confianza.
e. **Duración de la sesión**: Ingrese la duración de las credenciales de seguridad temporales y la sesión del rol. Ingrese al menos 15 minutos y no más de 12 horas.
f. **Certificado de CA del servidor** (opcional): Uno o más certificados de CA confiables, en formato PEM, para verificar el servidor de IAM Roles Anywhere. Si se omite, el servidor no se verificará.
g. **Certificado de entidad final**: La clave pública, en formato PEM, del certificado X509 firmado por el ancla de confianza. AWS IAM Roles Anywhere utiliza esta clave para emitir un token STS.
h. **Clave privada de entidad final**: la clave privada para el certificado de entidad final.

CAP (portal de acceso C2S)

Para el servicio S3 de Servicios de Nube Comercial (C2S)

a. **URL de credenciales temporales**: ingrese la URL completa que StorageGRID utilizará para obtener las credenciales temporales del servidor CAP, incluidos todos los parámetros de API obligatorios y opcionales asignados a su cuenta C2S.
b. **Certificado CA del servidor**: seleccione **Explorar** y cargue el certificado CA que StorageGRID utilizará para verificar el servidor CAP. El certificado debe estar codificado en PEM y ser emitido por una autoridad de certificación gubernamental (CA) apropiada.
c. **Certificado de cliente**: seleccione **Explorar** y cargue el certificado que StorageGRID utilizará para identificarse en el servidor CAP. El certificado del cliente debe estar codificado en PEM, emitido por una autoridad de certificación gubernamental (CA) apropiada y tener acceso a su cuenta C2S.
d. **Clave privada del cliente**: seleccione **Explorar** y cargue la clave privada codificada en PEM para el certificado del cliente.
e. Si la clave privada del cliente está cifrada, ingrese la contraseña para descifrarla. De lo contrario, deje el campo **Frase de contraseña de clave privada del cliente** en blanco.

Si se va a cifrar el certificado del cliente, utilice el formato tradicional para el cifrado. El formato cifrado PKCS #8 no es compatible.

Almacenamiento de blobs de Azure

Para Azure Blob Storage, solo clave compartida

a. **Nombre de la cuenta**: Ingrese el nombre de la cuenta de almacenamiento que posee el contenedor externo
b. **Clave de cuenta**: Ingrese la clave secreta para la cuenta de almacenamiento

Puede utilizar el portal de Azure para encontrar estos valores.

Anónimo

No se requiere información adicional

5. Seleccione **Continuar**. A continuación, elija el tipo de verificación de servidor que desea utilizar:

Opción	Descripción
Usar certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utilice los certificados CA de Grid instalados en el sistema operativo para proteger las conexiones.
Utilice un certificado CA personalizado	Utilice un certificado CA personalizado. Seleccione **Explorar** y cargue el certificado codificado en PEM.
No verificar el certificado	Seleccionar esta opción significa que las conexiones TLS al grupo de almacenamiento en la nube no son seguras.

6. Seleccione **Guardar**.

   Cuando guarda un grupo de almacenamiento en la nube, StorageGRID hace lo siguiente:

   - Valida que el depósito o contenedor y el punto final del servicio existan y que se pueda acceder a ellos utilizando las credenciales que usted especificó.
   - Escribe un archivo de marcador en el depósito o contenedor para identificarlo como un grupo de almacenamiento en la nube. Nunca elimine este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

     Si falla la validación del grupo de almacenamiento en la nube, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se podría informar un error si hay un error de certificado o si el depósito o contenedor especificado aún no existe.

7. Si se produce un error, consulte la"Instrucciones para solucionar problemas de grupos de almacenamiento en la nube" , resuelva cualquier problema y luego intente guardar el grupo de almacenamiento en la nube nuevamente.

Ver detalles del grupo de almacenamiento en la nube

Puede ver los detalles de un grupo de almacenamiento en la nube para determinar dónde se utiliza y ver qué nodos y grados de almacenamiento están incluidos.

Antes de empezar

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

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento** > **Grupos de almacenamiento en la nube**.

   La tabla de grupos de almacenamiento en la nube incluye la siguiente información para cada grupo de almacenamiento en la nube que incluye nodos de almacenamiento:

   - **Nombre**: el nombre para mostrar único del grupo.
   - **URI**: El identificador uniforme de recursos del grupo de almacenamiento en la nube.
   - **Tipo de proveedor**: ¿Qué proveedor de nube se utiliza para este grupo de almacenamiento en la nube?
   - **Contenedor**: el nombre del depósito utilizado para el grupo de almacenamiento en la nube.
   - **Uso de ILM**: cómo se utiliza actualmente el pool. Es posible que un grupo de almacenamiento en la nube no se utilice o que se utilice en una o más reglas ILM, perfiles de codificación de borrado o ambos.
   - **Último error**: el último error detectado durante una verificación del estado de este grupo de almacenamiento en la nube.
2. Para ver los detalles de un grupo de almacenamiento en la nube específico, seleccione su nombre.

   Aparece la página de detalles del grupo.
3. Consulte la pestaña **Autenticación** para obtener información sobre el tipo de autenticación para este grupo de almacenamiento en la nube y para editar los detalles de autenticación.
4. Vea la pestaña **Verificación del servidor** para obtener información sobre los detalles de verificación, editar la verificación, descargar un nuevo certificado o copiar el certificado PEM.
5. Vea la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento en la nube se está utilizando actualmente en alguna regla de ILM o perfil de codificación de borrado.
6. Opcionalmente, vaya a la **página de reglas de ILM** para"Conozca y administre cualquier regla" que utilizan el grupo de almacenamiento en la nube.

Editar un grupo de almacenamiento en la nube

Puede editar un grupo de almacenamiento en la nube para cambiar su nombre, punto final de servicio u otros detalles; sin embargo, no puede cambiar el depósito S3 ni el contenedor de Azure de un grupo de almacenamiento en la nube.

Antes de empezar

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

- Tienes"permisos de acceso específicos" .
- Usted ha revisado el"Consideraciones para los grupos de almacenamiento en la nube" .

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento** > **Grupos de almacenamiento en la nube**.

   La tabla Grupos de almacenamiento en la nube enumera los grupos de almacenamiento en la nube existentes.

2. Seleccione la casilla de verificación del grupo de almacenamiento en la nube que desea editar y luego seleccione **Acciones** > **Editar**.

   Alternativamente, seleccione el nombre del grupo de almacenamiento en la nube y luego seleccione **Editar**.

3. Según sea necesario, cambie el nombre del grupo de almacenamiento en la nube, el punto final del servicio, las credenciales de autenticación o el método de verificación del certificado.

   > No se puede cambiar el tipo de proveedor ni el bucket S3 ni el contenedor de Azure para un grupo de almacenamiento en la nube.

   Si anteriormente cargó un certificado de servidor o cliente, puede expandir el acordeón **Detalles del certificado** para revisar el certificado que está actualmente en uso.

4. Seleccione **Guardar**.

   Cuando guarda un grupo de almacenamiento en la nube, StorageGRID valida que el depósito o contenedor y el punto final del servicio existan y que se pueda acceder a ellos mediante las credenciales que usted especificó.

   Si falla la validación del grupo de almacenamiento en la nube, se muestra un mensaje de error. Por ejemplo, se podría informar un error si hay un error de certificado.

   Vea las instrucciones para"Solución de problemas de grupos de almacenamiento en la nube" , resuelva el problema y luego intente guardar el grupo de almacenamiento en la nube nuevamente.

Eliminar un grupo de almacenamiento en la nube

Puede eliminar un grupo de almacenamiento en la nube si no se utiliza en una regla ILM y no contiene datos de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"permisos de acceso necesarios" .

Si es necesario, utilice ILM para mover datos de objetos

Si el grupo de almacenamiento en la nube que desea eliminar contiene datos de objetos, debe usar ILM para mover los datos a una ubicación diferente. Por ejemplo, puede mover los datos a nodos de almacenamiento en su red o a un grupo de almacenamiento en la nube diferente.

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento** > **Grupos de almacenamiento en la nube**.
2. Mire la columna de uso de ILM en la tabla para determinar si puede eliminar el grupo de almacenamiento en la nube.

   No se puede eliminar un grupo de almacenamiento en la nube si se está utilizando en una regla ILM o en un perfil de codificación de borrado.

3. Si se está utilizando el grupo de almacenamiento en la nube, seleccione ***nombre del grupo de almacenamiento en la nube*** > **uso de ILM**.
4. "Clonar cada regla ILM"que actualmente coloca objetos en el grupo de almacenamiento en la nube que desea eliminar.
5. Determina dónde quieres mover los objetos existentes administrados por cada regla que clonaste.

   Puede utilizar uno o más grupos de almacenamiento o un grupo de almacenamiento en la nube diferente.

6. Edite cada una de las reglas que clonó.

   Para el paso 2 del asistente para crear reglas de ILM, seleccione la nueva ubicación en el campo **copias en**.

7. "Crear una nueva política de ILM"y reemplazar cada una de las reglas antiguas con una regla clonada.
8. Activar la nueva política.
9. Espere a que ILM elimine objetos del grupo de almacenamiento en la nube y los coloque en la nueva ubicación.

Eliminar grupo de almacenamiento en la nube

Cuando el grupo de almacenamiento en la nube esté vacío y no se utilice en ninguna regla de ILM, puedes eliminarlo.

Antes de empezar

- Ha eliminado todas las reglas ILM que podrían haber utilizado el grupo.
- Ha confirmado que el bucket S3 o el contenedor de Azure no contiene ningún objeto.

  Se produce un error si intenta eliminar un grupo de almacenamiento en la nube si contiene objetos. Ver "Solucionar problemas de grupos de almacenamiento en la nube" .

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

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento** > **Grupos de almacenamiento en la nube**.
2. Si la columna de uso de ILM indica que no se está utilizando el grupo de almacenamiento en la nube, seleccione la casilla de verificación.
3. Seleccione **Acciones** > **Eliminar**.
4. Seleccione **Aceptar**.

Solucionar problemas de grupos de almacenamiento en la nube

Utilice estos pasos de solución de problemas para ayudar a resolver errores que pueda encontrar al crear, editar o eliminar un grupo de almacenamiento en la nube.

Determinar si se ha producido un error

StorageGRID realiza una comprobación de estado simple en cada grupo de almacenamiento en la nube leyendo el objeto conocido `x-ntap-sgws-cloud-pool-uuid` para garantizar que se pueda acceder al grupo de almacenamiento en la nube y que funcione correctamente. Cuando StorageGRID detecta un error en el punto final, realiza una comprobación del estado cada minuto desde cada nodo de almacenamiento. Cuando se resuelve el error, las comprobaciones de estado se detienen. Si una verificación de estado detecta un problema, se muestra un mensaje en la columna Último error de la tabla Grupos de almacenamiento en la nube en la página Grupos de almacenamiento.

La tabla muestra el error más reciente detectado para cada grupo de almacenamiento en la nube e indica cuánto tiempo hace que ocurrió el error.

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

Comprobar si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. Desde la página Grupo de almacenamiento en la nube, seleccione el punto final y seleccione **Borrar error**. Un mensaje de confirmación indica que StorageGRID ha solucionado el error del grupo de almacenamiento en la nube.

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

Error: Error en la comprobación de salud. Error del punto final

Es posible que encuentre este error cuando habilite el bloqueo de objetos S3 con retención predeterminada para su depósito de Amazon S3 después de comenzar a usar este depósito para un grupo de almacenamiento en la nube. Este error ocurre cuando la operación PUT no tiene un encabezado HTTP con un valor de suma de comprobación de carga útil como `Content-MD5` . AWS requiere este valor de encabezado para operaciones PUT en buckets con el bloqueo de objetos S3 habilitado.

Para corregir este problema, siga los pasos que se indican en"Editar un grupo de almacenamiento en la nube" sin realizar ningún cambio. Esta acción activa la validación de la configuración del grupo de almacenamiento en la nube que detecta y actualiza automáticamente el indicador de bloqueo de objetos S3 en una configuración de punto final del grupo de almacenamiento en la nube.

Error: Este grupo de almacenamiento en la nube contiene contenido inesperado

Es posible que encuentre este error cuando intente crear, editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el depósito o contenedor incluye el `x-ntap-sgws-cloud-pool-uuid` archivo

marcador, pero ese archivo no tiene el campo de metadatos con el UUID esperado.

Por lo general, solo verá este error si está creando un nuevo grupo de almacenamiento en la nube y otra instancia de StorageGRID ya está usando el mismo grupo de almacenamiento en la nube.

Pruebe uno de estos pasos para corregir el problema:

- Si está configurando un nuevo grupo de almacenamiento en la nube y el depósito contiene el `x-ntap-sgws-cloud-pool-uuid` archivo y claves de objeto adicionales similares al siguiente ejemplo, cree un nuevo depósito y use este nuevo depósito en su lugar.

  Ejemplo de una clave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si el `x-ntap-sgws-cloud-pool-uuid` el archivo es el único objeto en el depósito, elimine este archivo.

Si estos pasos no se aplican a su situación, comuníquese con el soporte técnico.

Error: No se pudo crear o actualizar el grupo de almacenamiento en la nube. Error del punto final

Es posible que encuentre este error en las siguientes circunstancias:

- Cuando intenta crear o editar un grupo de almacenamiento en la nube.
- Cuando selecciona una plataforma, autenticación o combinación de protocolo no compatible con S3 Object Lock durante la configuración de un nuevo grupo de almacenamiento en la nube. Ver "Consideraciones para los grupos de almacenamiento en la nube" .

Este error indica que un problema de conectividad o configuración impide que StorageGRID escriba en el grupo de almacenamiento en la nube.

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

- Si el mensaje de error contiene `Get *url*: EOF` Verifique que el punto final del servicio utilizado para el grupo de almacenamiento en la nube no utilice HTTP para un contenedor o depósito que requiera HTTPS.
- Si el mensaje de error contiene `Get *url*: net/http: request canceled while waiting for connection` , verifique que la configuración de la red permita que los nodos de almacenamiento accedan al punto final de servicio utilizado para el grupo de almacenamiento en la nube.
- Si el error se debe a una plataforma, autenticación o protocolo no compatible, cambie a una configuración compatible con S3 Object Lock e intente guardar nuevamente el nuevo grupo de almacenamiento en la nube.
- Para todos los demás mensajes de error de punto final, pruebe una o más de las siguientes opciones:
  - Cree un contenedor o depósito externo con el mismo nombre que ingresó para el grupo de almacenamiento en la nube e intente guardar el nuevo grupo de almacenamiento en la nube nuevamente.
  - Corrija el nombre del contenedor o depósito que especificó para el grupo de almacenamiento en la nube e intente guardar el nuevo grupo de almacenamiento en la nube nuevamente.

Error: No se pudo analizar el certificado de CA

Es posible que encuentre este error cuando intente crear o editar un grupo de almacenamiento en la nube. El

error ocurre si StorageGRID no pudo analizar el certificado ingresado al configurar el grupo de almacenamiento en la nube.

Para corregir el problema, verifique el certificado CA que proporcionó para ver si hay problemas.

Error: No se encontró un grupo de almacenamiento en la nube con este ID

Es posible que encuentre este error cuando intente editar o eliminar un grupo de almacenamiento en la nube. Este error ocurre si el punto final devuelve una respuesta 404, que puede significar cualquiera de las siguientes cosas:

- Las credenciales utilizadas para el grupo de almacenamiento en la nube no tienen permiso de lectura para el depósito.
- El depósito utilizado para el grupo de almacenamiento en la nube no incluye el `x-ntap-sgws-cloud-pool-uuid` archivo de marcador.

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

- Verifique que el usuario asociado a la clave de acceso configurada tenga los permisos necesarios.
- Edite el grupo de almacenamiento en la nube con credenciales que tengan los permisos necesarios.
- Si los permisos son correctos, comuníquese con el soporte.

Error: No se pudo comprobar el contenido del grupo de almacenamiento en la nube. Error del punto final

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. Este error indica que algún tipo de problema de conectividad o configuración impide que StorageGRID lea el contenido del depósito de Cloud Storage Pool.

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

Error: Ya se han colocado objetos en este depósito

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. No puedes eliminar un grupo de almacenamiento en la nube si contiene datos que ILM movió allí, datos que estaban en el depósito antes de configurar el grupo de almacenamiento en la nube o datos que alguna otra fuente colocó en el depósito después de que se creó el grupo de almacenamiento en la nube.

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

- Siga las instrucciones para mover objetos nuevamente a StorageGRID en "Ciclo de vida de un objeto de grupo de almacenamiento en la nube".
- Si está seguro de que ILM no colocó los objetos restantes en el grupo de almacenamiento en la nube, elimine manualmente los objetos del depósito.

> ⓘ Nunca elimine manualmente objetos de un grupo de almacenamiento en la nube que ILM pueda haber colocado allí. Si posteriormente intenta acceder a un objeto eliminado manualmente desde StorageGRID, no se encontrará el objeto eliminado.

Error: el proxy encontró un error externo al intentar acceder al grupo de almacenamiento en la nube

Es posible que encuentre este error si ha configurado un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el punto final S3 externo utilizado para el grupo de almacenamiento en la nube. Este error se produce si el servidor proxy externo no puede acceder al punto final del grupo de almacenamiento en la nube. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externa.

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

- Verifique la configuración del grupo de almacenamiento en la nube (**ILM** > **Grupos de almacenamiento**).
- Verifique la configuración de red del servidor proxy de almacenamiento.

Error: el certificado X.509 está fuera del período de validez

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. Este error ocurre cuando la autenticación requiere un certificado X.509 para garantizar que se valide el grupo de almacenamiento en la nube externo correcto y el grupo externo está vacío antes de que se elimine la configuración del grupo de almacenamiento en la nube.

Pruebe estos pasos para corregir el problema:

- Actualice el certificado configurado para la autenticación en el grupo de almacenamiento en la nube.
- Asegúrese de que se haya resuelto cualquier alerta de vencimiento de certificado en este grupo de almacenamiento en la nube.

Información relacionada

"Ciclo de vida de un objeto de grupo de almacenamiento en la nube"