Gestiona objetos con ILM

StorageGRID software

NetApp
July 23, 2026

Tabla de contenidos

Gestiona objetos con ILM

Administra objetos con ILM en StorageGRID

Las reglas de gestión del ciclo de vida de la información (ILM) en una política de ILM le indican a StorageGRID cómo crear y distribuir copias de los datos de los objetos y cómo gestionar esas copias a lo largo del tiempo.

${post_edited_translations.segment}

El diseño y la implementación de reglas y políticas de ILM requieren una planificación minuciosa. Debes conocer tus requisitos operativos, la topología de tu sistema StorageGRID, tus necesidades de protección de objetos y los tipos de almacenamiento disponibles. Luego, debes determinar cómo quieres que se copien, distribuyan y almacenen los diferentes tipos de objetos.

Sigue estas instrucciones para:

- Descubre más sobre StorageGRID ILM, incluida "cómo funciona ILM a lo largo de la vida de un objeto".
- Descubre cómo configurar "grupos de almacenamiento", "Grupos de almacenamiento en la nube" y "Reglas de ILM".
- Descubre cómo "crear, simular y activar una política de ILM" que protegerá los datos de objetos en uno o varios sitios.
- Descubre cómo "gestionar objetos con S3 Object Lock" , lo que ayuda a garantizar que los objetos en buckets específicos de S3 no se eliminen ni se sobrescriban durante un periodo de tiempo determinado.

Más información

Para obtener más información, echa un vistazo a estos vídeos:

Resumen de las reglas de ILM

Resumen de las políticas de ILM

ILM y el ciclo de vida de los objetos

Cómo funciona ILM a lo largo de la vida de un objeto en StorageGRID

Comprender cómo StorageGRID utiliza ILM para gestionar los objetos en cada etapa de su ciclo de vida puede ayudarte a diseñar una política más eficaz.

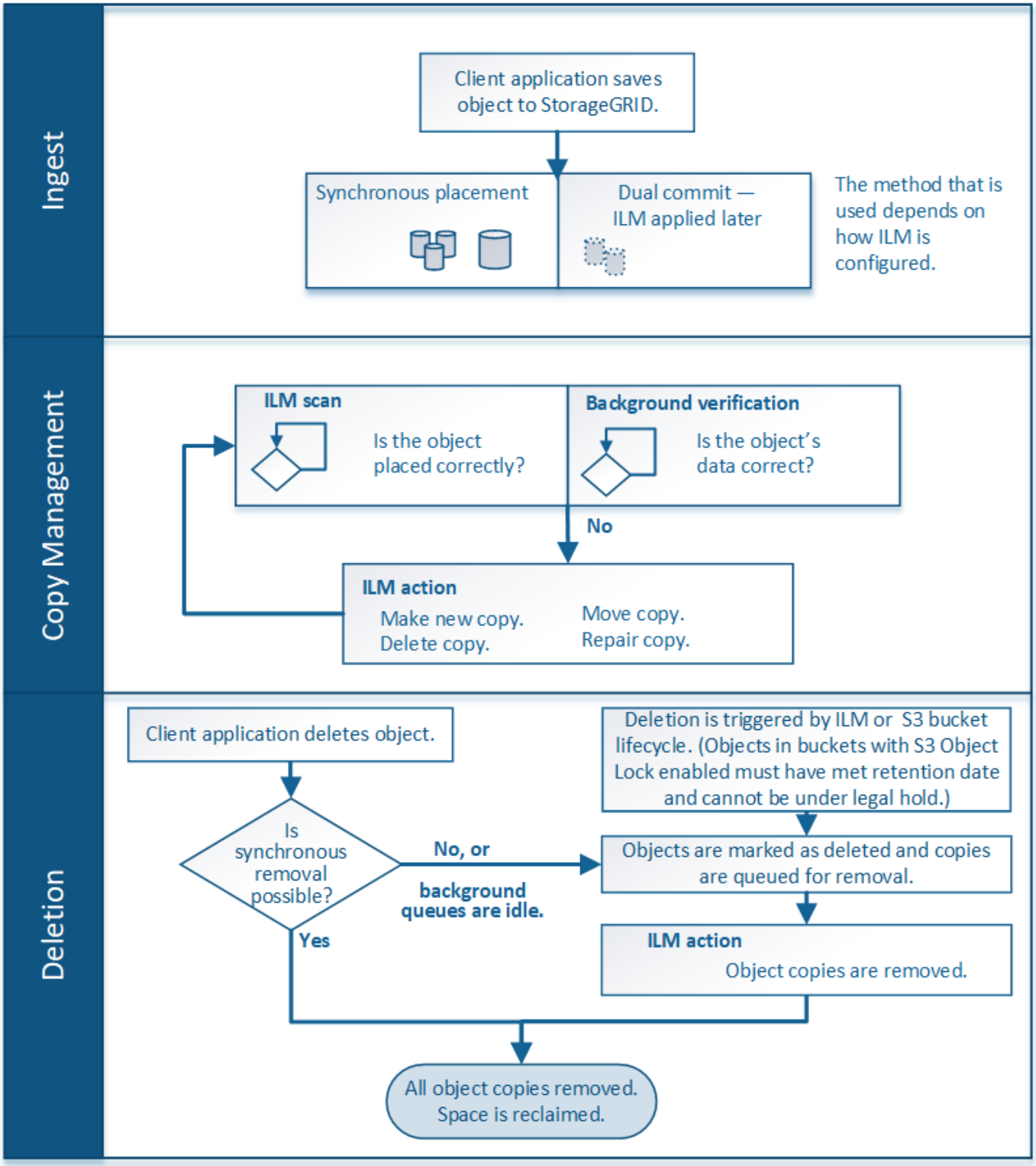
- **Ingesta**: La ingesta comienza cuando una aplicación cliente de S3 establece una conexión para guardar un objeto en el sistema StorageGRID, y finaliza cuando StorageGRID devuelve al cliente un mensaje de «ingesta realizada con éxito». Los datos de los objetos quedan protegidos durante la ingesta, ya sea aplicando inmediatamente las instrucciones de ILM (colocación síncrona) o creando copias provisionales y aplicando ILM posteriormente (confirmación dual), en función de cómo se hayan especificado los requisitos de ILM.
- **Gestión de copias**: Después de crear el número y tipo de copias de objetos que se especifican en las instrucciones de ubicación del ILM, StorageGRID gestiona las ubicaciones de los objetos y los protege contra la pérdida.

- **Análisis y evaluación de ILM**: StorageGRID analiza continuamente la lista de objetos almacenados en la red y comprueba si las copias actuales cumplen los requisitos de ILM. Cuando se requieren diferentes tipos, cantidades o ubicaciones de copias de los objetos, StorageGRID crea, elimina o desplaza copias según sea necesario.
- **Verificación en segundo plano**: StorageGRID realiza continuamente verificaciones en segundo plano para comprobar la integridad de los datos de los objetos. Si se detecta algún problema, StorageGRID crea automáticamente una nueva copia del objeto o un fragmento de objeto sustitutivo con código de borrado en una ubicación que cumpla con los requisitos actuales de ILM. Consulta "Verifica la integridad del objeto".

- **Eliminación de objetos**: La gestión de un objeto finaliza cuando se eliminan todas sus copias del sistema StorageGRID. Los objetos pueden eliminarse como resultado de una solicitud de eliminación por parte de un cliente, de una eliminación realizada por ILM o de una eliminación causada por la expiración del ciclo de vida de un bucket de S3.

  > Los objetos de un bucket en el que se haya habilitado S3 Object Lock no se pueden eliminar si están sujetos a una retención legal o si se ha especificado una fecha límite de retención que aún no se haya alcanzado.

El diagrama resume cómo funciona ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

Opciones de ingestión de ILM en StorageGRID

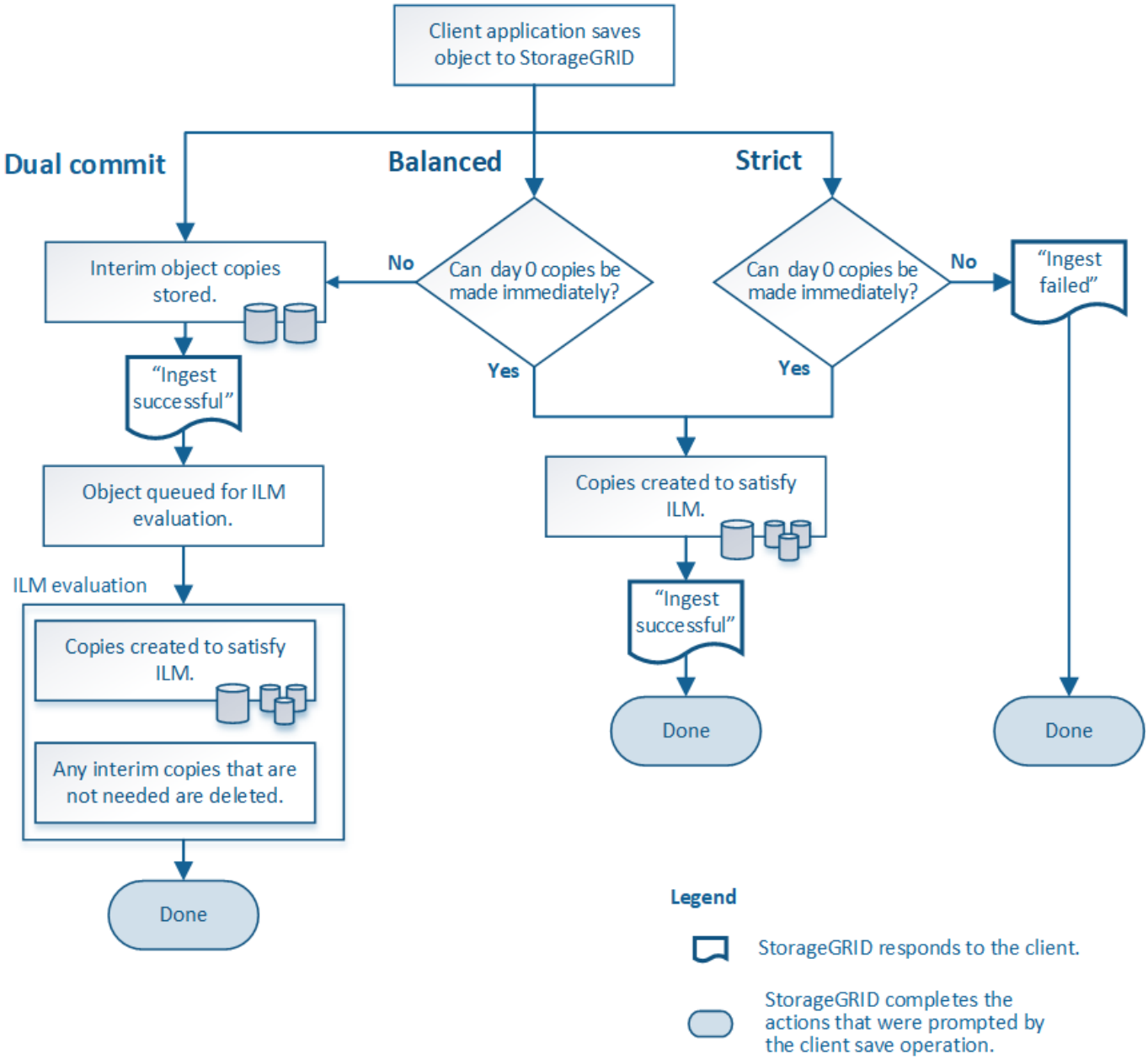
Cuando creas una regla de ILM, especificas una de tres opciones para proteger los objetos al momento de la ingesta: Dual commit, Strict o Balanced.

En función de la opción que elijas, StorageGRID crea copias provisionales y pone los objetos en cola para su

posterior evaluación ILM, o bien utiliza la colocación sincrónica y crea copias de inmediato para cumplir los requisitos ILM.

Diagrama de flujo de las opciones de ingestión

El diagrama de flujo muestra lo que ocurre cuando los objetos coinciden con una regla de ILM que utiliza cada una de las tres opciones de ingesta.



Confirmación doble

Al seleccionar la opción «Dual commit», StorageGRID crea inmediatamente copias provisionales del objeto en dos nodos de almacenamiento diferentes y devuelve al cliente un mensaje de «ingesta realizada con éxito». El objeto se pone en cola para su evaluación por parte de ILM, y las copias que cumplen con las instrucciones de ubicación de la regla se crean después. Si la política de ILM no se puede procesar inmediatamente después del dual commit, la protección contra la pérdida de un sitio podría tardar en lograrse.

Utiliza la opción Dual commit en cualquiera de estos casos:

- Estás utilizando reglas de ILM multisitio y la latencia en la ingesta de los clientes es tu principal consideración. Al utilizar Dual commit, debes asegurarte de que tu grid pueda realizar el trabajo adicional de crear y eliminar las copias de dual commit si no cumplen con ILM. En concreto:
  - La carga en la grid debe ser lo suficientemente baja como para evitar un retraso de ILM.
  - La red debe disponer de recursos de hardware de sobra (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Estás utilizando reglas de ILM multisitio y la conexión WAN entre los sitios suele presentar una latencia elevada o un ancho de banda limitado. En este caso, usar la opción Dual commit puede ayudar a evitar los tiempos de espera de los clientes. Antes de elegir la opción Dual commit, deberías probar la aplicación cliente con cargas de trabajo realistas.

Equilibrado (predeterminado)

Al seleccionar la opción «Equilibrada», StorageGRID también utiliza la colocación sincrónica durante la ingesta y crea inmediatamente todas las copias especificadas en las instrucciones de colocación de la regla. A diferencia de la opción «Estricta», si StorageGRID no puede crear todas las copias de forma inmediata, utiliza en su lugar la confirmación dual. Si la política de ILM utiliza ubicaciones en varios sitios y no se puede lograr una protección inmediata contra la pérdida de un sitio, se activa la alerta **ILM placement unachievable**.

Utiliza la opción «Equilibrada» para conseguir la mejor combinación de protección de datos, rendimiento del grid y éxito en la ingesta. «Equilibrada» es la opción predeterminada en el asistente para crear reglas de ILM.

Estricto

Al seleccionar la opción Strict, StorageGRID utiliza la colocación sincrónica durante la ingesta y crea inmediatamente todas las copias del objeto especificadas en las instrucciones de colocación de la regla. La ingesta falla si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento necesaria no está disponible temporalmente. El cliente debe volver a intentar la operación.

Utiliza la opción Strict si tienes un requisito operativo o normativo que te obligue a almacenar inmediatamente los objetos únicamente en las ubicaciones especificadas en la regla de ILM. Por ejemplo, para cumplir un requisito normativo, es posible que tengas que utilizar la opción Strict y un filtro avanzado de Location Constraint para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Consulta "Ejemplo 5: normas y política de ILM para un comportamiento de ingesta estricto".

Ventajas, desventajas y limitaciones de las opciones de ingesta de ILM en StorageGRID

Conocer las ventajas y desventajas de cada una de las tres opciones para proteger los datos en el momento de la ingesta (Balanced, Strict o Dual commit) puede ayudarte a decidir cuál elegir para una regla de ILM.

Para obtener una visión general de las opciones de ingestión, consulta "Opciones de ingesta".

Ventajas de las opciones Equilibrada y Estricta

En comparación con Dual commit, que crea copias provisionales durante la importación, las dos opciones de colocación sincrónica pueden ofrecer las siguientes ventajas:

- **Mayor seguridad de los datos**: Los datos de los objetos quedan protegidos de inmediato según lo especificado en las instrucciones de ubicación de la regla ILM, que pueden configurarse para proteger contra una amplia variedad de situaciones de fallo, incluido el fallo de más de una ubicación de almacenamiento. El dual commit solo puede proteger contra la pérdida de una única copia local.

- **Funcionamiento más eficiente de la red**: Cada objeto se procesa una sola vez, en el momento de su incorporación. Dado que el sistema StorageGRID no necesita realizar un seguimiento ni eliminar copias provisionales, la carga de procesamiento es menor y se consume menos espacio en la base de datos.
- **(Equilibrado) Recomendado**: La opción «Equilibrado» ofrece una eficiencia óptima de ILM. Se recomienda utilizar la opción «Equilibrado» salvo que se requiera un comportamiento de ingesta estricto o que la grid cumpla todos los criterios para utilizar Dual commit.
- **(Estricta) Certeza sobre la ubicación de los objetos**: La opción Estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de ubicación establecidas en la regla ILM.

Desventajas de las opciones «Balanced» y «Strict»

En comparación con Dual commit, las opciones Balanced y Strict presentan algunas desventajas:

- **Ingestas más largas por parte del cliente**: Las latencias de ingesta del cliente pueden ser mayores. Cuando usas las opciones "Balanced" o "Strict", no se devuelve al cliente un mensaje de "ingesta realizada con éxito" hasta que se hayan creado y almacenado todos los fragmentos con código de borrado o todas las copias replicadas. Sin embargo, es muy probable que los datos del objeto alcancen su ubicación definitiva mucho más rápido.
- **(Estricto) Mayores índices de fallos en la importación**: Con la opción «Estricto», la importación falla siempre que StorageGRID no pueda crear inmediatamente todas las copias especificadas en la regla de ILM. Es posible que veas altos índices de fallos en la importación si una ubicación de almacenamiento necesaria está temporalmente fuera de línea o si los problemas de red provocan retrasos en la copia de objetos entre sitios.
- **(Estricto) En algunas circunstancias, la ubicación de las subidas multiparte a S3 podría no ser la esperada**: con el modo «Estricto», esperas que los objetos se coloquen tal y como describe la regla de ILM o que la ingesta falle. Sin embargo, en una carga multiparte de S3, ILM se evalúa para cada parte del objeto a medida que se ingiere, y para el objeto en su conjunto cuando finaliza la carga multiparte. En las siguientes circunstancias, esto podría dar lugar a ubicaciones diferentes a las que esperas:
  - **Si el ILM cambia mientras se está realizando una subida multiparte a S3**: porque cada parte se almacena según la regla vigente en el momento de su ingesta, es posible que algunas partes del objeto no cumplan los requisitos actuales del ILM cuando finalice la subida multiparte. En estos casos, la ingesta del objeto no falla. En su lugar, cualquier parte que no se haya ubicado correctamente se pone en cola para una reevaluación de ILM y se traslada posteriormente a la ubicación correcta.
  - **Cuando las reglas de ILM filtran por tamaño**: Al evaluar ILM para una parte, StorageGRID filtra en función del tamaño de la parte, no del tamaño del objeto. Esto significa que las partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su conjunto. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir, cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto, todas las partes del objeto se trasladan a DC1.
- **(Estricto) La ingesta no falla cuando se actualizan las etiquetas o los metadatos de un objeto y no es posible realizar las nuevas ubicaciones requeridas**: Con Strict, esperas que los objetos se coloquen tal como lo describe la regla de ILM o que la ingesta falle. Sin embargo, cuando actualizas los metadatos o las etiquetas de un objeto que ya está almacenado en el grid, el objeto no se vuelve a ingerir. Esto significa que cualquier cambio en la ubicación del objeto provocado por la actualización no se realiza de inmediato. Los cambios de ubicación se realizan cuando ILM se vuelve a evaluar mediante los procesos normales de ILM en segundo plano. Si no es posible realizar los cambios de ubicación requeridos (por ejemplo, porque una ubicación recién requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que sea posible realizar los cambios de ubicación.

Limitaciones en la colocación de objetos con las opciones Balanced y Strict

Las opciones Equilibrada o Estricta no se pueden usar para las reglas de ILM que tengan cualquiera de estas instrucciones de ubicación:

- Ubicación en un Cloud Storage Pool el día 0.
- Asignaciones en un grupo de almacenamiento en la nube cuando la regla tiene como hora de referencia una hora de creación definida por el usuario.

Estas restricciones existen porque StorageGRID no puede realizar copias de forma sincrónica en un Cloud Storage Pool, y una hora de creación definida por el usuario podría corresponder al momento actual.

Cómo interactúan las reglas de ILM y la coherencia para afectar la protección de datos

Tanto la regla de ILM como la opción de consistencia que elijas influyen en la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta la ubicación inicial de las copias de los objetos, mientras que la consistencia utilizada al almacenar un objeto afecta la ubicación inicial de los metadatos del objeto. Porque StorageGRID requiere acceso tanto a los datos como a los metadatos de un objeto para cumplir con las solicitudes de los clientes, seleccionar niveles de protección coincidentes para la consistencia y el comportamiento de ingesta puede ofrecer una mejor protección inicial de los datos y respuestas del sistema más predecibles.

Aquí tienes un breve resumen de los valores de consistencia que están disponibles en StorageGRID:

- ${post_edited_translations.segment}
- **Strong-global**: garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes en todos los sitios. Cuando configuras la semántica de Quorum, se aplican los siguientes comportamientos:
  - Permite la tolerancia a fallos del sitio para las solicitudes de los clientes cuando los grids tienen tres o más sitios. Los grids de dos sitios no tendrán tolerancia a fallos del sitio.
  - Las siguientes operaciones de S3 no se podrán realizar si uno de los sitios está inactivo:
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryption
    - PutBucketVersioning
    - PutObjectLegalHold
    - PutObjectLockConfiguration
    - PutObjectRetention

  Si lo necesitas, puedes "Configura la semántica de quórum de StorageGRID para una consistencia global fuerte".
- **Sitio fuerte**: Los metadatos de los objetos se distribuyen inmediatamente a los demás nodos del sitio. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes dentro de un sitio.
- **Read-after-new-write**: proporciona coherencia de lectura tras escritura para objetos nuevos y coherencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.

- **Disponible**: Proporciona consistencia eventual tanto para los objetos nuevos como para las actualizaciones de objetos. Para los buckets de S3, utilízalo solo cuando sea necesario (por ejemplo, para un bucket que contenga valores de registro que rara vez se leen, o para operaciones HEAD o GET sobre claves que no existen). No es compatible con los buckets de S3 FabricPool.

> Antes de seleccionar un valor de consistencia, "Lee la descripción completa sobre la consistencia". Debes entender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo la coherencia y las reglas de ILM pueden interactuar

${post_edited_translations.segment}

- **Regla de ILM**: crea tres copias de objeto, una en el sitio local y otra en cada sitio remoto. Usa el comportamiento de ingesta Strict.
- **Consistencia**: Global fuerte (los metadatos de los objetos se distribuyen inmediatamente a varios sitios).

${post_edited_translations.segment}

El objeto queda totalmente protegido contra la pérdida en el momento en que se recibe el mensaje de ingesta correcta. Por ejemplo, si el sitio local se pierde poco después de la ingesta, siguen existiendo copias tanto de los datos del objeto como de los metadatos del objeto en los sitios remotos. El objeto se puede recuperar íntegramente desde los demás sitios.

Si, por el contrario, usaste la misma regla de ILM y la consistencia de sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se replican en los sitios remotos, pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos del objeto no coincide con el nivel de protección de los datos del objeto. Si el sitio local se pierde poco después de la ingesta, se pierden los metadatos del objeto. El objeto no se puede recuperar.

La interrelación entre la coherencia y las reglas de ILM puede ser compleja. Ponte en contacto con NetApp si necesitas ayuda.

Información relacionada

"Ejemplo 5: normas y política de ILM para un comportamiento de ingesta estricto"

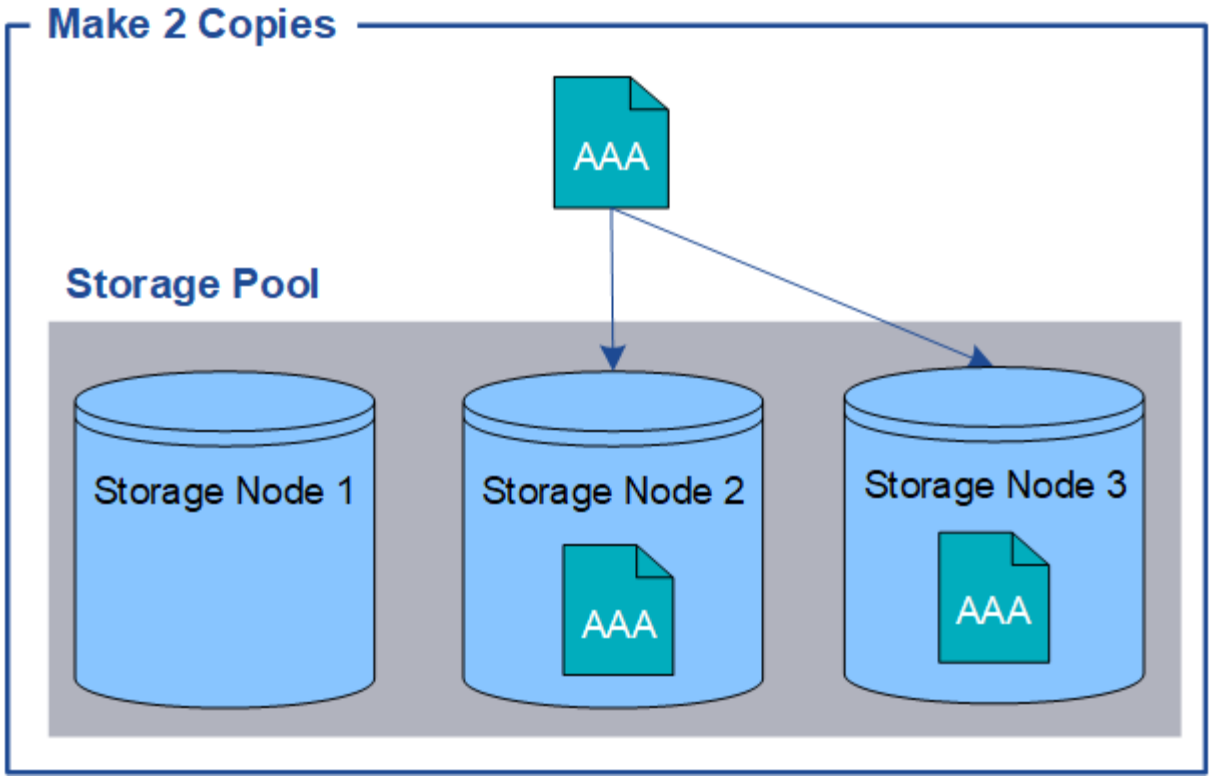
Cómo se almacenan los objetos (replicación o código de borrado)

Conoce la replicación en StorageGRID

La replicación es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos (el otro método es el código de borrado). Cuando los objetos cumplen una regla de ILM que utiliza la replicación, el sistema crea copias exactas de los datos de los objetos y las almacena en Storage Nodes.

Al configurar una regla de ILM para crear copias replicadas, especificas cuántas copias deben crearse, dónde deben ubicarse y durante cuánto tiempo deben almacenarse en cada ubicación.

En el siguiente ejemplo, la regla ILM especifica que se coloquen dos copias replicadas de cada objeto en un grupo de almacenamiento que contiene tres Storage Nodes.



Cuando StorageGRID aplica esta regla a los objetos, crea dos copias del objeto y las almacena en dos nodos de almacenamiento distintos del grupo de almacenamiento. Las dos copias pueden ubicarse en cualquiera de los tres nodos de almacenamiento disponibles. En este caso, la regla ha ubicado las copias del objeto en los nodos de almacenamiento 2 y 3. Al haber dos copias, el objeto puede recuperarse si falla cualquiera de los nodos del grupo de almacenamiento.

> StorageGRID solo puede almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento. Si tu grid incluye tres nodos de almacenamiento y creas una regla ILM de 4 copias, solo se harán tres copias: una por cada nodo de almacenamiento. La alerta **ILM placement unachievable** se activa para indicar que la regla ILM no se pudo aplicar completamente.

Información relacionada

- "¿Qué es el erasure coding?"
- "¿Qué es un storage pool?"
- "Activar la protección contra la pérdida de sitios mediante la replicación y el código de borrado"

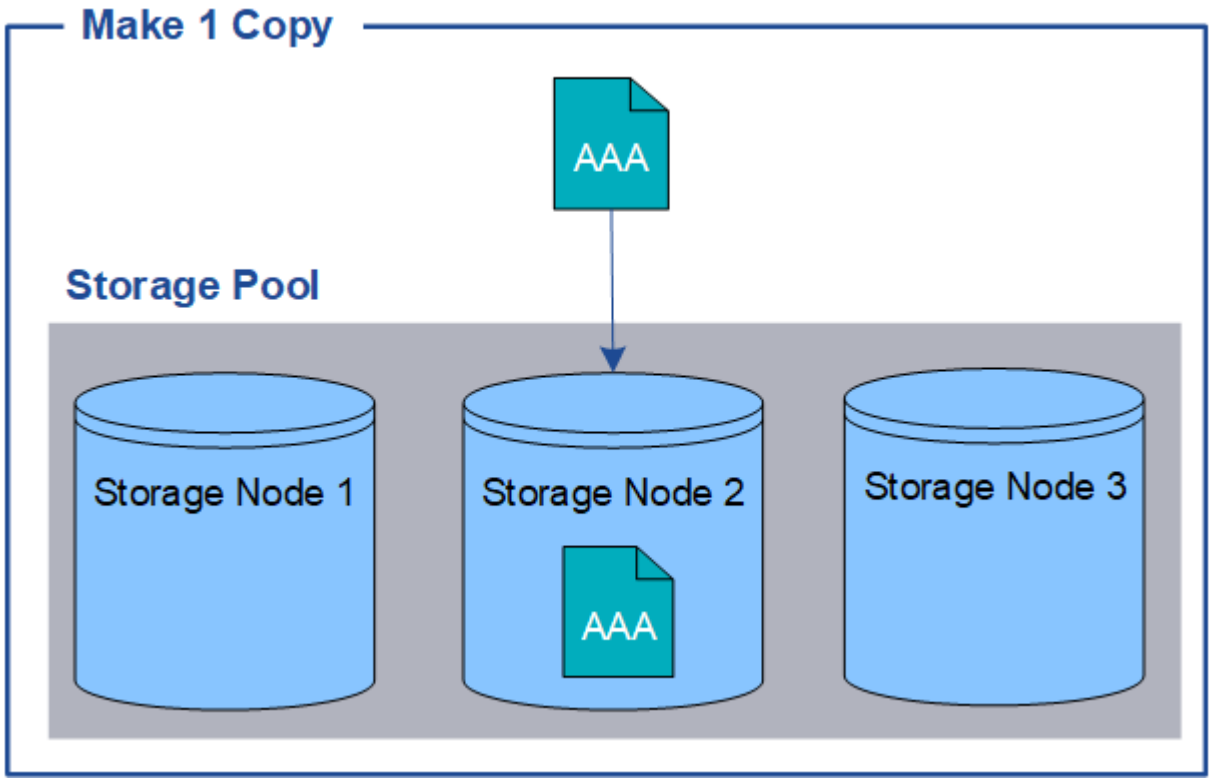
Riesgos de la replicación de una sola copia en StorageGRID

Al crear una regla de ILM para generar copias replicadas, siempre debes especificar al menos dos copias para cualquier periodo de tiempo en las instrucciones de ubicación.

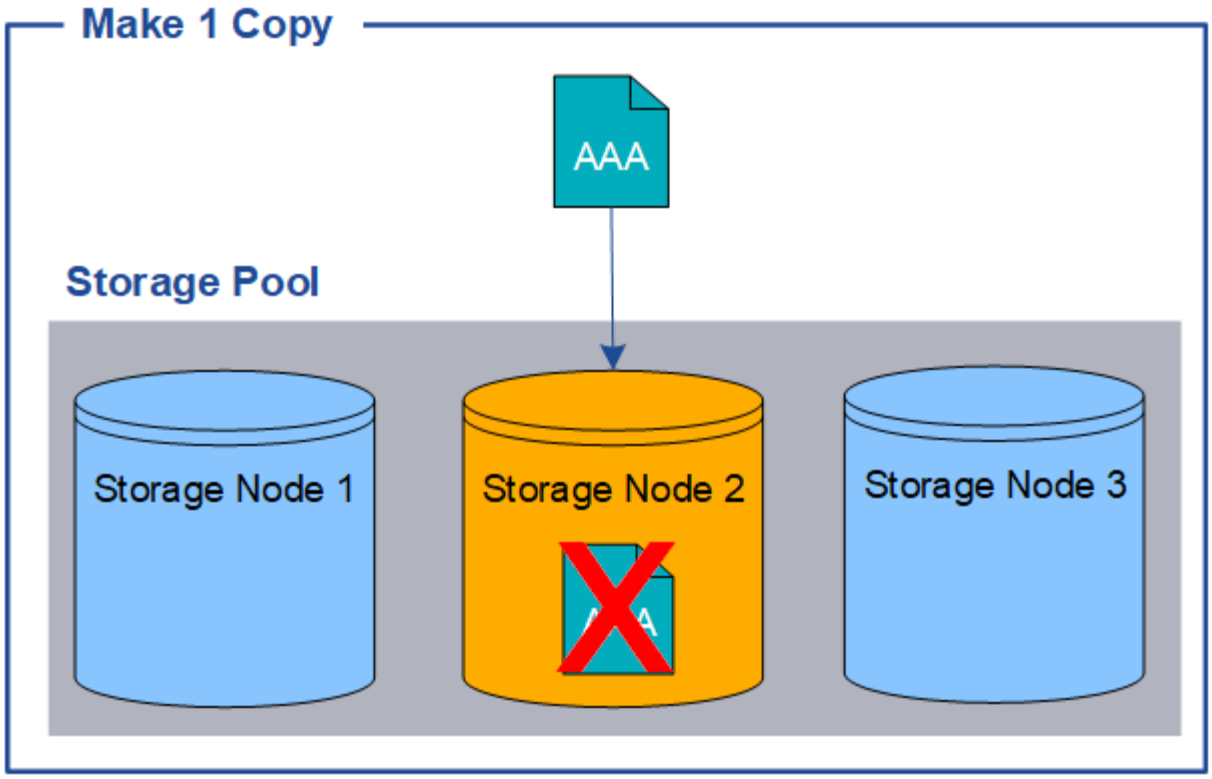
> No utilices una regla de ILM que cree una sola copia replicada durante cualquier periodo de tiempo. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un Storage Node falla o tiene un error importante. También perderás temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.

En el siguiente ejemplo, la regla ILM «Make 1 Copy» especifica que se coloque una copia replicada de un

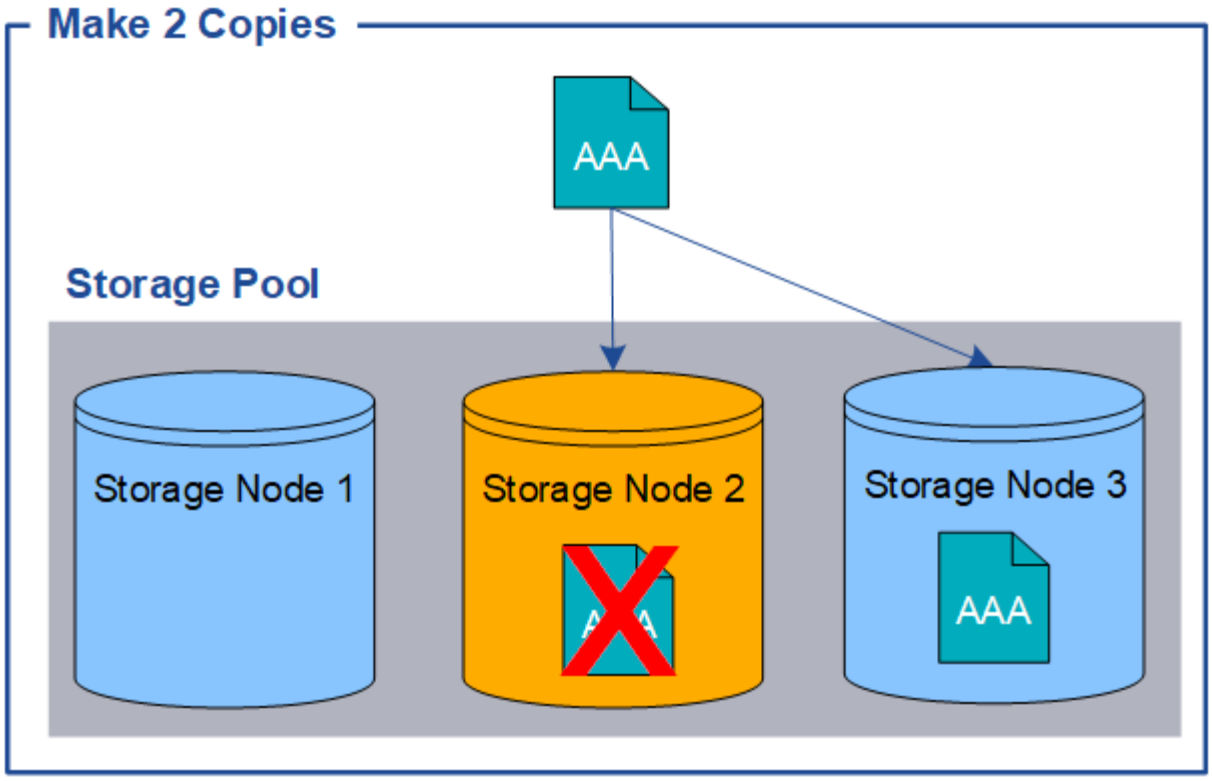
objeto en un grupo de almacenamiento que contiene tres Storage Nodes. Cuando se ingiere un objeto que coincide con esta regla, StorageGRID coloca una sola copia en solo un Storage Node.



Cuando una regla de ILM crea solo una copia replicada de un objeto, el objeto se vuelve inaccesible cuando el nodo de almacenamiento no está disponible. En este ejemplo, perderás temporalmente el acceso al objeto AAA cada vez que el nodo de almacenamiento 2 esté fuera de línea, como durante una actualización u otro procedimiento de mantenimiento. Perderás por completo el objeto AAA si el nodo de almacenamiento 2 falla.



Para evitar la pérdida de datos de los objetos, debes crear siempre al menos dos copias de todos los objetos que desees proteger mediante replicación. Si existen dos o más copias, puedes seguir accediendo al objeto si uno de los Storage Node falla o queda fuera de línea.



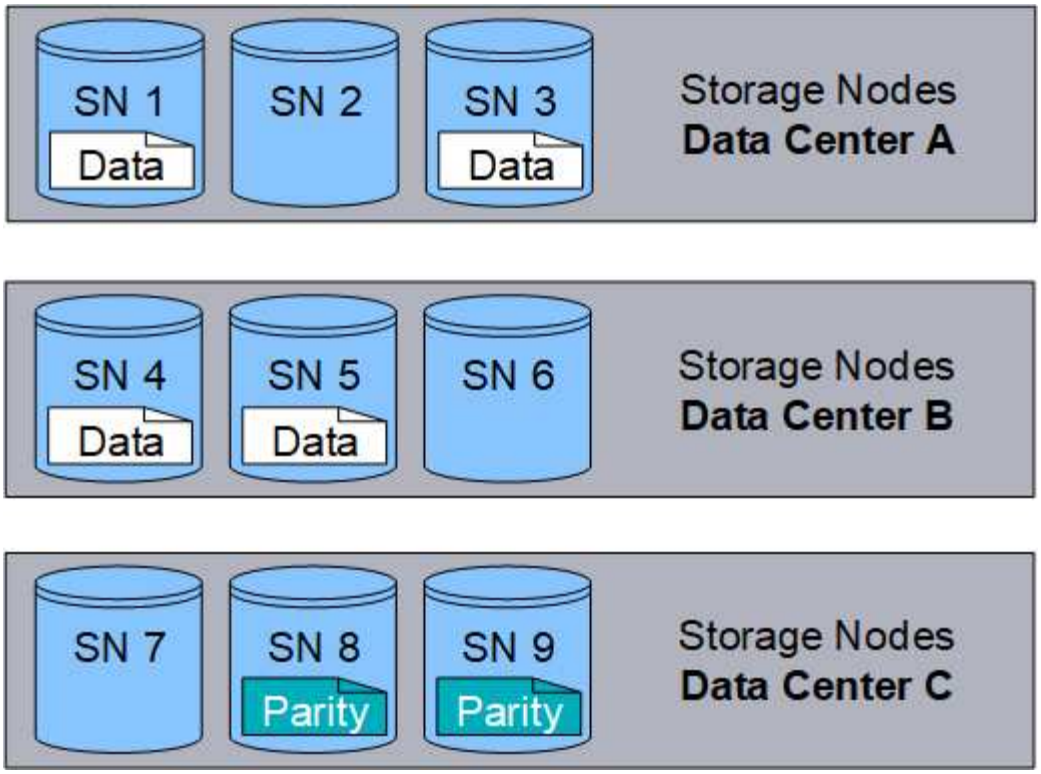
Aprende sobre el código de borrado en StorageGRID

El código de borrado es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos (la replicación es el otro método). Cuando los objetos cumplen una regla de ILM que utiliza el código de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

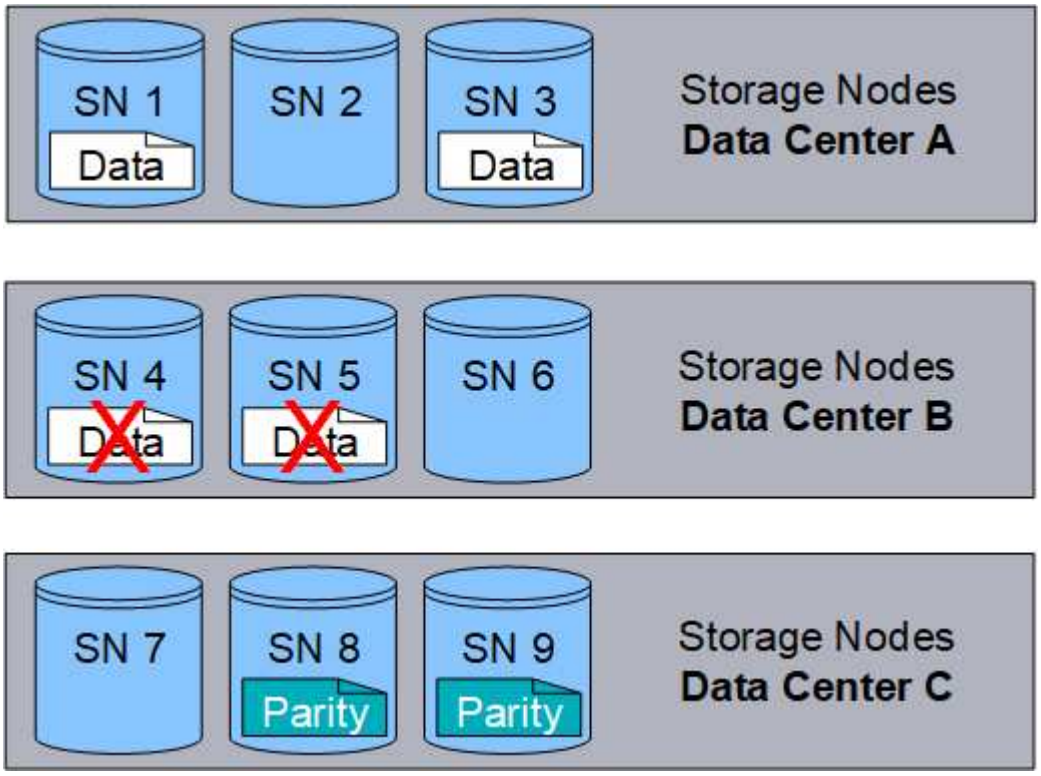
Cuando se accede a un objeto, este se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o de paridad se daña o se pierde, el algoritmo de código de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes.

A medida que creas reglas de ILM, StorageGRID crea perfiles de código de borrado compatibles con dichas reglas. Puedes consultar una lista de perfiles de código de borrado, "cambiar el nombre de un perfil de código de borrado", o "desactivar un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM".

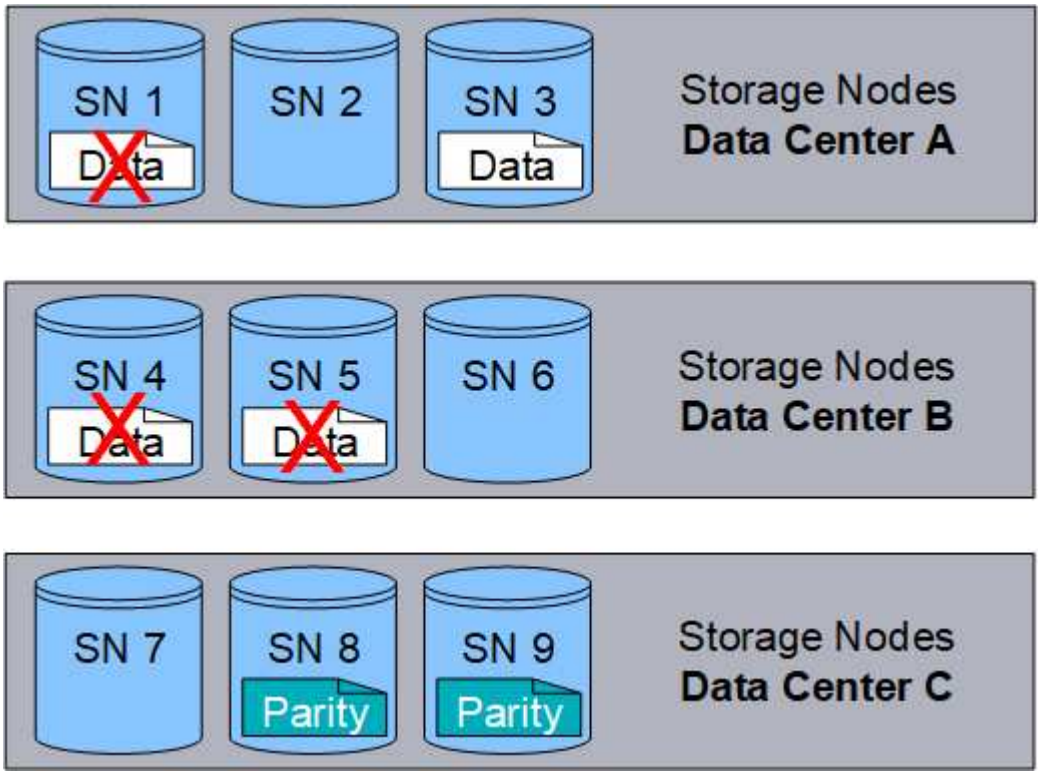
El siguiente ejemplo ilustra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los datos del objeto. Cada uno de los seis fragmentos se almacena en un nodo diferente en tres centros de datos para proporcionar protección de datos ante fallos de nodo o pérdida de sitio.



El esquema de código de borrado 4+2 se puede configurar de diversas formas. Por ejemplo, puedes configurar un grupo de almacenamiento de un solo sitio que contenga seis nodos de almacenamiento. Para "protección contra la pérdida del sitio", puedes usar un grupo de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Puedes recuperar un objeto siempre que cualquiera de los cuatro de los seis fragmentos (de datos o de paridad) sigan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio completo, aún puedes recuperar o reparar el objeto, siempre que los demás fragmentos sigan siendo accesibles.



Si se pierden más de dos nodos de almacenamiento, el objeto no se puede recuperar.



Información relacionada

- "${post_edited_translations.segment}"
- "¿Qué es un storage pool?"
- "${post_edited_translations.segment}"
- "Cambiar el nombre de un perfil de código de borrado"
- "Desactivar un perfil de código de borrado"

Conoce los esquemas de codificación de borrado en StorageGRID

Los esquemas de código de borrado controlan cuántos fragmentos de datos y cuántos fragmentos de paridad se crean para cada objeto.

Al crear o editar una regla de ILM, debes seleccionar un esquema de código de borrado disponible. StorageGRID crea automáticamente esquemas de código de borrado en función de cuántos nodos de almacenamiento y sitios forman el grupo de almacenamiento que planeas usar.

Protección de datos

El sistema StorageGRID utiliza el algoritmo de código de borrado Reed-Solomon. El algoritmo divide un objeto en `k` fragmentos de datos y calcula `m` fragmentos de paridad.

Los `k + m = n` fragmentos se distribuyen entre `n` los nodos de almacenamiento para proporcionar protección de datos de la siguiente manera:

- Para recuperar o reparar un objeto, se necesitan fragmentos. `k`
- Un objeto puede soportar hasta `m` fragmentos perdidos o dañados. Cuanto mayor sea el valor de `m`, mayor

será la tolerancia a los fallos.

La mejor protección de datos la ofrece el esquema de código de borrado con mayor tolerancia a fallos de nodos o volúmenes dentro de un storage pool.

Sobrecarga de almacenamiento

La sobrecarga de almacenamiento de un esquema de codificación de borrado se calcula dividiendo el número de fragmentos de paridad (`m` entre el número de fragmentos de datos (`k`. Puedes utilizar la sobrecarga de almacenamiento para calcular cuánto espacio en disco requiere cada objeto codificado mediante código de borrado:

```
disk space = object size + (object size * storage overhead)
```

Por ejemplo, si almacenas un objeto de 10 MB utilizando el esquema 4+2 (que tiene una sobrecarga de almacenamiento del 50 %), el objeto ocupa 15 MB de almacenamiento en grid. Si almacenas el mismo objeto de 10 MB utilizando el esquema 6+2 (que tiene una sobrecarga de almacenamiento del 33 %), el objeto ocupa aproximadamente 13,3 MB.

Selecciona el esquema de código de borrado con el valor total más bajo de `k+m` que se adapte a tus necesidades. Los esquemas de código de borrado con un número menor de fragmentos son más eficientes desde el punto de vista computacional porque:

- Se crean y distribuyen (o recuperan) menos fragmentos por objeto
- Ofrecen un mejor rendimiento porque el tamaño de los fragmentos es mayor
- Pueden requerir que se añadan menos nodos en un "ampliación cuando se requiere más almacenamiento"

Directrices para los grupos de almacenamiento

Al seleccionar el grupo de almacenamiento que se va a utilizar para una regla que creará una copia con código de borrado, sigue estas directrices relativas a los grupos de almacenamiento:

- El grupo de almacenamiento debe incluir tres o más emplazamientos, o exactamente un emplazamiento.

  > No puedes usar el código de borrado si el grupo de almacenamiento incluye dos sitios.

  - Esquemas de código de borrado para grupos de almacenamiento que contienen tres o más emplazamientos
  - Esquemas de código de borrado para grupos de almacenamiento de un solo sitio
- No utilices un grupo de almacenamiento que incluya el sitio All Sites.
- El grupo de almacenamiento debe incluir al menos `k+m +1` nodos de almacenamiento capaces de almacenar datos de objetos.

  > Los nodos de almacenamiento pueden configurarse durante la instalación para que contengan datos de objetos y metadatos (nodo de almacenamiento «combinado»), solo metadatos de objetos o solo datos de objetos. Para obtener más información, consulta "Tipos de nodos de almacenamiento".

  El número mínimo de nodos de almacenamiento necesarios es `k+m`. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a evitar fallos en la ingesta o retrasos en el ILM si un nodo de

almacenamiento necesario no está disponible temporalmente.

Esquemas de código de borrado para grupos de almacenamiento que contienen tres o más emplazamientos

La siguiente tabla describe los esquemas de código de borrado que admite actualmente StorageGRID para los grupos de almacenamiento que incluyen tres o más emplazamientos. Todos estos esquemas ofrecen protección frente a la pérdida de un emplazamiento. Se puede perder un emplazamiento y el objeto seguirá siendo accesible.

Para los esquemas de código de borrado que ofrecen protección frente a la pérdida de un sitio, el número recomendado de Storage Nodes en el storage pool supera `k+m +1` porque cada sitio requiere un mínimo de tres Storage Nodes.

Esquema de código de borrado (*k*+*m*)	Número mínimo de sitios implementados	Número recomendado de nodos de almacenamiento en cada sitio	Número total recomendado de nodos de almacenamiento	¿Protección contra la pérdida del sitio?	Sobrecarga de almacenamiento
4+2	3	3	9	Sí	50%
6+2	4	3	12	Sí	33%
8+2	5	3	15	Sí	25%
6+3	3	4	12	Sí	50%
9+3	4	4	16	Sí	33%
2+1	3	3	9	Sí	50%
4+1	5	3	15	Sí	25%
6+1	7	3	21	Sí	17%
7+5	3	5	15	Sí	71%

> StorageGRID requiere un mínimo de tres nodos de almacenamiento por sitio. Para usar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda usar cinco nodos de almacenamiento por sitio.

A la hora de seleccionar un esquema de código de borrado que ofrezca protección de sitio, hay que sopesar la importancia relativa de los siguientes factores:

- **Número de fragmentos**: Por lo general, el rendimiento y la flexibilidad de expansión son mejores cuando el número total de fragmentos es menor.
- **Tolerancia a fallos**: La tolerancia a fallos aumenta al disponer de más segmentos de paridad (es decir, cuando `m` tiene un valor más alto).

- **Tráfico de red**: Al recuperarse de fallos, usar un esquema con más fragmentos (es decir, un valor total más alto para `k+m`) genera más tráfico de red.
- **Sobrecarga de almacenamiento**: los esquemas con mayor sobrecarga requieren más espacio de almacenamiento por objeto.

Por ejemplo, a la hora de decidir entre un esquema 4+2 y uno 6+3 (ambos con una sobrecarga de almacenamiento del 50 %), elige el esquema 6+3 si se requiere una mayor tolerancia a fallos. Elige el esquema 4+2 si los recursos de red son limitados. Si todos los demás factores son iguales, elige el 4+2 porque tiene un número total de fragmentos menor.

Si no estás seguro de qué esquema debes utilizar, selecciona 4+2 o 6+3, o ponte en contacto con soporte técnico.

Esquemas de código de borrado para grupos de almacenamiento de un solo sitio

Un grupo de almacenamiento de un solo sitio es compatible con todos los esquemas de código de borrado definidos para tres o más sitios, siempre que dicho sitio cuente con suficientes nodos de almacenamiento.

El número mínimo de nodos de almacenamiento necesarios es `k+m`, pero se recomienda un grupo de almacenamiento con `k+m +1` nodos de almacenamiento. Por ejemplo, el esquema de código de borrado 2+1 requiere un grupo de almacenamiento con un mínimo de tres nodos de almacenamiento, pero se recomienda un grupo de cuatro nodos de almacenamiento.

Esquema de código de borrado (*k+m*)	Número mínimo de nodos de almacenamiento	Número recomendado de nodos de almacenamiento	Sobrecarga de almacenamiento
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Ventajas, desventajas y requisitos para la codificación de borrado en StorageGRID

Antes de decidir si utilizar la replicación o el código de borrado para proteger los datos de objetos contra pérdidas, debes entender las ventajas, desventajas y los requisitos del

código de borrado.

Ventajas del código de borrado

En comparación con la replicación, el código de borrado ofrece una mayor fiabilidad, disponibilidad y eficiencia de almacenamiento.

- **Fiabilidad**: Se mide por el número de fallos simultáneos que se pueden soportar sin pérdida de datos.
  - Replicación: se almacenan varias copias idénticas de un objeto en distintos nodos y en diferentes emplazamientos.
  - Codificación de borrado: un objeto se codifica en fragmentos de datos y de paridad y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección tanto frente a fallos de sitio como de nodo.
- **Disponibilidad**: La capacidad de obtener objetos si los nodos de almacenamiento fallan o se vuelven inaccesibles. En comparación con la replicación, el código de borrado ofrece una mayor disponibilidad con costes de almacenamiento similares.
- **Eficiencia de almacenamiento**: Para un nivel similar de disponibilidad y fiabilidad, los objetos con código de borrado ocupan menos espacio en disco que los objetos replicados. Por ejemplo, un objeto de 10 MB replicado en dos sitios ocupa 20 MB de espacio en disco (dos copias), mientras que un objeto codificado con código de borrado en tres sitios mediante un esquema 6+3 solo ocupa 15 MB de espacio en disco.

> El espacio en disco para los objetos con código de borrado se calcula como el tamaño del objeto más la sobrecarga de almacenamiento. El porcentaje de sobrecarga de almacenamiento es el número de fragmentos de paridad dividido por el número de fragmentos de datos.

Desventajas del código de borrado

En comparación con la replicación, el código de borrado presenta las siguientes desventajas:

- Se recomienda aumentar el número de nodos de almacenamiento y de sitios, dependiendo del esquema de código de borrado. En cambio, si replicas datos de objetos, solo necesitas un nodo de almacenamiento por cada copia. Consulta "Esquemas de código de borrado para grupos de almacenamiento que contienen tres o más emplazamientos" y "Esquemas de código de borrado para grupos de almacenamiento de un solo sitio".
- Aumento del coste y la complejidad de las ampliaciones de almacenamiento. Para ampliar una implementación que utiliza replicación, tienes que añadir capacidad de almacenamiento en cada ubicación donde se crean copias de los objetos. Para ampliar una implementación que utiliza código de borrado, debes tener en cuenta tanto el esquema de código de borrado utilizado como el nivel de ocupación de los nodos de almacenamiento existentes. Por ejemplo, si esperas hasta que los nodos existentes estén al 100% de su capacidad, tienes que añadir al menos `k+m` nodos de almacenamiento, pero si amplías cuando los nodos existentes están al 70% de su capacidad, puedes añadir dos nodos por sitio y seguir maximizando la capacidad de almacenamiento utilizable. Para más información, consulta "Agrega capacidad de almacenamiento para objetos con código de borrado".
- El uso del código de borrado en sitios distribuidos geográficamente conlleva un aumento de la latencia en la recuperación. Los fragmentos de un objeto codificado mediante código de borrado y distribuido entre sitios remotos tardan más en recuperarse a través de conexiones WAN que un objeto replicado y disponible localmente (en el mismo sitio al que se conecta el cliente).
- Cuando usas el código de borrado en sitios distribuidos geográficamente, hay un mayor uso de tráfico de red WAN para las recuperaciones y reparaciones, especialmente para los objetos que se recuperan con

frecuencia o para las reparaciones de objetos a través de conexiones de red WAN.

- Cuando se utiliza el código de borrado entre sitios, el rendimiento máximo de los objetos disminuye drásticamente a medida que aumenta la latencia de red entre los sitios. Esta disminución se debe a una reducción del rendimiento de la red TCP, lo que afecta a la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objetos.
- Mayor uso de los recursos de computación.

Cuándo utilizar el código de borrado

Utiliza el código de borrado para los siguientes requisitos:

- Objetos de más de 1 MB de tamaño.

> El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

- Almacenamiento a largo plazo o en frío para contenido al que se accede con poca frecuencia.
- Alta disponibilidad y fiabilidad de los datos.
- Protección frente a fallos totales del sitio y de los nodos.
- Eficiencia de almacenamiento.
- Implementaciones en un único sitio que requieren una protección de datos eficaz con una sola copia codificada con código de borrado en lugar de múltiples copias replicadas.
- Implementaciones en varios sitios donde la latencia entre sitios es inferior a 100 ms.

Cómo StorageGRID determina la retención de objetos

StorageGRID ofrece opciones tanto a los administradores de grid como a los usuarios individuales de tenant para especificar durante cuánto tiempo almacenar los objetos. En general, cualquier instrucción de retención proporcionada por un usuario de tenant tiene prioridad sobre las instrucciones de retención proporcionadas por el administrador de grid.

Cómo los usuarios del inquilino controlan la retención de objetos

Los usuarios de Tenant pueden usar estos métodos para controlar cuánto tiempo se almacenan sus objetos en StorageGRID:

- Si la configuración global de S3 Object Lock está habilitada para la grid, los usuarios del tenant de S3 pueden crear buckets con S3 Object Lock habilitado y luego seleccionar un **período de retención predeterminado** para cada bucket.
- Si la configuración global de S3 Object Lock está habilitada para el grid, los usuarios de S3 tenant pueden crear buckets con S3 Object Lock habilitado y luego usar la API de REST de S3 para especificar retain-until-date y legal hold para cada versión de objeto añadida a ese bucket.
  - Una versión de objeto que está bajo retención legal no puede eliminarse por ningún método.
  - Antes de que se alcance la fecha límite de retención de una versión de un objeto, esa versión no puede eliminarse por ningún método.

    - Los objetos de los buckets en los que se ha habilitado S3 Object Lock se conservan «para siempre» mediante ILM. Sin embargo, después de que se alcance la fecha de retención, una versión del objeto puede eliminarse mediante una solicitud del cliente o al expirar el ciclo de vida del bucket. Consulta "Gestiona objetos con S3 Object Lock".
- Los usuarios de un tenant de S3 pueden añadir una configuración de ciclo de vida a sus buckets en la que se especifique una acción de Expiration. Si existe un ciclo de vida para el bucket, StorageGRID almacena un objeto hasta que se alcance la fecha o el número de días especificados en la acción de Expiration, a menos que el cliente elimine el objeto antes. Consulta "Crear configuración del ciclo de vida de S3".
- Un cliente S3 puede enviar una solicitud de eliminación de un objeto. StorageGRID siempre da prioridad a las solicitudes de eliminación del cliente frente al ciclo de vida del bucket S3 o ILM al determinar si se debe eliminar o conservar un objeto.

Cómo controlan los administradores de grid la retención de objetos

Los administradores de la grid pueden utilizar estos métodos para controlar la retención de objetos:

- Establece un periodo máximo de retención de S3 Object Lock para cada tenant. Luego, los usuarios del tenant pueden establecer un periodo de retención predeterminado para cada uno de sus buckets. El periodo máximo de retención también se aplica a cualquier objeto nuevo que se incorpore a ese bucket (retain-until-date del objeto).
- Crea instrucciones de ubicación de ILM para controlar el tiempo que se almacenan los objetos. Cuando los objetos coinciden con una regla de ILM, StorageGRID almacena esos objetos hasta que haya transcurrido el último periodo de tiempo en la regla de ILM. Los objetos se conservan indefinidamente si se especifica "para siempre" en las instrucciones de ubicación.
- Independientemente de quién controle el tiempo de retención de los objetos, la configuración de ILM determina qué tipos de copias de los objetos (replicadas o con código de borrado) se almacenan y dónde se ubican dichas copias (Storage Nodes o Cloud Storage Pools).

Cómo interactúan el ciclo de vida de los buckets de S3 y la ILM

Cuando se configura el ciclo de vida de un bucket de S3, las acciones de caducidad del ciclo de vida prevalecen sobre la política de ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría mantenerse en el grid incluso después de que hayan expirado las instrucciones de ILM para ubicar el objeto.

Ejemplos de retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, la configuración del ciclo de vida de los buckets, las solicitudes de eliminación de los clientes y ILM, fíjate en los siguientes ejemplos.

Ejemplo 1: el ciclo de vida de un bucket de S3 conserva los objetos durante más tiempo que el ILM

ILM

Conservar dos copias durante 1 año (365 días)

Ciclo de vida de bucket

Los objetos caducan en 2 años (730 días)

Resultado

StorageGRID almacena el objeto durante 730 días. StorageGRID utiliza la configuración del ciclo de vida del bucket para determinar si se debe eliminar o conservar un objeto.

Si el ciclo de vida del bucket especifica que los objetos deben conservarse durante más tiempo del indicado por el ILM, StorageGRID sigue utilizando las instrucciones de ubicación del ILM al determinar el número y tipo de copias que se deben almacenar. En este ejemplo, dos copias del objeto seguirán almacenándose en StorageGRID desde el día 366 hasta el 730.

Ejemplo 2: el ciclo de vida del bucket de S3 expira los objetos antes que ILM

ILM

Conservar dos copias durante 2 años (730 días)

Ciclo de vida de bucket

Los objetos caducan en 1 año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: la eliminación por parte del cliente anula el ciclo de vida del bucket y el ILM

ILM

Almacena dos copias en los Storage Nodes "para siempre"

Ciclo de vida de bucket

Los objetos caducan en 2 años (730 días)

Solicitud de eliminación de cliente

Publicado el día 400

Resultado

StorageGRID elimina ambas copias del objeto el día 400 en respuesta a la solicitud de eliminación del cliente.

Ejemplo 4: El bloqueo de objetos de S3 anula la solicitud de eliminación del cliente

Bloqueo de objetos de S3

La fecha límite de conservación de una versión del objeto es el 31 de marzo de 2026. No hay ninguna retención legal en vigor.

Regla de ILM conforme

Almacena dos copias en los Storage Nodes "para siempre"

Solicitud de eliminación de cliente

Publicado el 31 de marzo de 2024

Resultado

StorageGRID no eliminará la versión del objeto porque aún faltan 2 años para la fecha límite de conservación.

Cómo StorageGRID borra objetos

StorageGRID puede eliminar objetos ya sea en respuesta directa a una solicitud del cliente o automáticamente como resultado de la expiración del ciclo de vida de un bucket

de S3 o de los requisitos de la política de ILM. Entender las diferentes formas en que se pueden eliminar los objetos y cómo StorageGRID maneja las solicitudes de eliminación puede ayudarte a gestionar los objetos de manera más eficaz.

StorageGRID puede utilizar uno de estos dos métodos para eliminar objetos:

- Eliminación sincrónica: Cuando StorageGRID recibe una solicitud de eliminación de un cliente, todas las copias del objeto se eliminan de inmediato. El cliente es informado de que la eliminación fue exitosa después de que se hayan eliminado las copias.
- Los objetos se colocan en cola para su eliminación: cuando StorageGRID recibe una solicitud de eliminación, el objeto se coloca en cola para su eliminación y se informa inmediatamente al cliente que la eliminación fue exitosa. Las copias de los objetos se eliminan más tarde mediante el procesamiento de ILM en segundo plano.

Al eliminar objetos, StorageGRID utiliza el método que optimiza el rendimiento de la eliminación, minimiza los posibles retrasos en la eliminación y libera espacio libre con mayor rapidez.

La tabla resume en qué casos StorageGRID utiliza cada método.

Método para realizar una eliminación	**Cuando se utiliza**
Los objetos se colocan en cola para su eliminación	Cuando **cualquiera** de las siguientes condiciones sea verdadera: • La eliminación automática de objetos se activó por uno de los siguientes eventos: ◦ Se ha alcanzado la fecha de caducidad o el número de días en la configuración del ciclo de vida de un bucket de S3. ◦ Vence el último plazo especificado en una regla de ILM. **Nota:** Los objetos de un bucket en el que esté activada la función S3 Object Lock no se pueden eliminar si están sujetos a una retención legal o si se ha especificado una fecha límite de conservación que aún no se ha alcanzado. • Un cliente de S3 solicita una eliminación y se cumple una o varias de estas condiciones: ◦ Las copias no se pueden eliminar en los primeros 30 segundos porque, por ejemplo, la ubicación de un objeto no está disponible temporalmente. ◦ Las colas de eliminación en segundo plano están inactivas.
Los objetos se eliminan de inmediato (eliminación sincrónica)	Cuando un cliente de S3 realiza una solicitud de eliminación y se cumplen **todas** las condiciones siguientes: • Todas las copias se pueden eliminar en 30 segundos. • Las colas de eliminación en segundo plano contienen objetos para procesar.

Cuando los clientes de S3 realizan solicitudes de eliminación, StorageGRID comienza añadiendo objetos a la cola de eliminación. Luego pasa a realizar la eliminación sincrónica. Asegurarse de que la cola de eliminación en segundo plano tenga objetos para procesar permite a StorageGRID procesar las eliminaciones de manera más eficiente, especialmente para clientes con baja concurrencia, y ayuda a evitar acumulaciones de

solicitudes de eliminación de los clientes.

Tiempo necesario para eliminar objetos

La forma en que StorageGRID elimina los objetos puede influir en el rendimiento aparente del sistema:

- Cuando StorageGRID lleva a cabo una eliminación sincrónica, puede tardar hasta 30 segundos en devolver un resultado al cliente. Esto significa que la eliminación puede parecer más lenta, aunque en realidad las copias se eliminan más rápidamente que cuando StorageGRID pone los objetos en cola para su eliminación.
- Si estás supervisando de cerca el rendimiento de la eliminación durante una eliminación masiva, es posible que observes que la velocidad de eliminación parece reducirse una vez que se ha eliminado un determinado número de objetos. Este cambio se produce cuando StorageGRID pasa de poner los objetos en cola para su eliminación a realizar una eliminación sincrónica. La aparente reducción de la velocidad de eliminación no significa que las copias de los objetos se estén eliminando más lentamente. Al contrario, indica que, de media, ahora se libera espacio más rápidamente.

Si vas a eliminar un gran número de objetos y tu prioridad es obtener espacio libre rápidamente, plantéate utilizar una solicitud del cliente para eliminarlos en lugar de hacerlo mediante ILM u otros métodos. En general, el espacio libre se obtiene más rápidamente cuando la eliminación la realizan los clientes porque StorageGRID puede utilizar la eliminación sincrónica.

La cantidad de tiempo que se necesita para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de los objetos se eliminan de forma sincrónica o se ponen en cola para su eliminación posterior (para las solicitudes de eliminación de los clientes).
- Otros factores, como el número de objetos en el grid o la disponibilidad de recursos del grid cuando las copias de los objetos se ponen en cola para su eliminación (tanto en el caso de las eliminaciones realizadas por el cliente como en el de otros métodos).

Cómo se eliminan los objetos versionados de S3

Cuando se habilita el control de versiones para un bucket de S3, StorageGRID sigue el comportamiento de Amazon S3 cuando responde a las solicitudes de eliminación, ya sea que esas solicitudes provengan de un cliente de S3, del vencimiento del ciclo de vida de un bucket de S3 o de los requisitos de la política de ILM.

Cuando los objetos están versionados, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto ni liberan espacio. En su lugar, una solicitud de eliminación de objetos crea un marcador de eliminación de cero bytes como versión actual del objeto, lo que hace que la versión anterior del objeto pase a ser "no actual". Un marcador de eliminación de objeto se convierte en un marcador de eliminación de objeto caducado cuando es la versión actual y no hay versiones no actuales.

Aunque el objeto no se haya eliminado, StorageGRID se comporta como si la versión actual del objeto ya no estuviera disponible. Las solicitudes a ese objeto devuelven 404 NotFound. Sin embargo, como los datos del objeto no actual no se han eliminado, las solicitudes que especifiquen una versión no actual del objeto pueden tener éxito.

Si un cliente elimina una versión de un objeto con un identificador de versión de un "bucket de rama", StorageGRID oculta la existencia de la versión del objeto pero no crea un marcador de eliminación en el branch bucket. Si un cliente elimina un objeto sin identificador de versión de un branch bucket, StorageGRID crea un marcador de eliminación en el branch bucket según el comportamiento estándar de S3.

Para liberar espacio al eliminar objetos versionados o para eliminar los marcadores de eliminación, usa una de

las siguientes opciones:

- **Solicitud del cliente S3**: Especifica el ID de versión del objeto en la solicitud S3 DELETE Object (`DELETE /object?versionId=ID`). Ten en cuenta que esta solicitud solo elimina las copias del objeto correspondientes a la versión especificada (las demás versiones siguen ocupando espacio).
- **Ciclo de vida del bucket**: Usa la acción `NoncurrentVersionExpiration` en la configuración del ciclo de vida del bucket. Cuando se cumple el número de NoncurrentDays especificado, StorageGRID elimina permanentemente todas las copias de las versiones de objetos que ya no están vigentes. Estas versiones de objetos no se pueden recuperar.

  La `NewerNoncurrentVersions` acción en la configuración del ciclo de vida del bucket especifica el número de versiones no actuales que se conservan en un bucket de S3 con control de versiones. Si hay más versiones no actuales de las que `NewerNoncurrentVersions` especifica, StorageGRID elimina las versiones más antiguas cuando ha transcurrido el valor de NoncurrentDays. El umbral de `NewerNoncurrentVersions` reemplaza las reglas del ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del umbral de `NewerNoncurrentVersions` se conserva si ILM solicita su eliminación.

  Para eliminar los marcadores de eliminación de objetos caducados, usa la acción `Expiration` con una de las siguientes etiquetas: `ExpiredObjectDeleteMarker`, `Days` o `Date`.

- **ILM**: "Clonar una política activa" y añade dos reglas de ILM a la nueva política:
  - Primera regla: utiliza «Tiempo no actual» como tiempo de referencia para hacer coincidir las versiones no actuales del objeto. En "Paso 1 (Introducir datos) del asistente para crear una regla de ILM", selecciona **Sí** para la pregunta, «¿Aplicar esta regla solo a las versiones anteriores del objeto (en S3 buckets con control de versiones activado)?»
  - Segunda regla: Utiliza **Hora de ingesta** para hacer coincidir la versión actual. La regla «Hora no actual» debe aparecer en la política por encima de la regla **Hora de ingesta**.

    Para eliminar los marcadores de eliminación de objetos caducados, utiliza una regla de **Hora de ingesta** que coincida con los marcadores de eliminación actuales. Los marcadores de eliminación solo se eliminan cuando ha transcurrido un **Periodo de tiempo** de **Días** y el marcador de eliminación actual ha caducado (no hay versiones que no sean actuales).

- **Eliminar objetos de un depósito**: Usa el tenant manager para "Eliminar todas las versiones de los objetos", incluidos los marcadores de eliminación, de un depósito.

Cuando se elimina un objeto versionado, StorageGRID crea un marcador de eliminación de cero bytes como la versión actual del objeto. Todos los objetos y marcadores de eliminación deben eliminarse antes de que se pueda eliminar un bucket versionado.

- Los marcadores de eliminación creados en StorageGRID 11.7 o versiones anteriores solo pueden eliminarse mediante solicitudes del cliente S3, no se eliminan mediante ILM, las reglas de ciclo de vida del bucket ni las operaciones de eliminación de objetos del bucket.
- Los marcadores de eliminación de un bucket creado en StorageGRID 11.8 o una versión posterior pueden eliminarse mediante ILM, las reglas del ciclo de vida del bucket, las operaciones de eliminación de objetos en el bucket o una eliminación explícita realizada por un cliente S3.

Información relacionada

- "Usa la API de REST de S3"
- "Ejemplo 4: reglas y política de ILM para objetos versionados de S3"

Crea y asigna grados de almacenamiento en StorageGRID

Los niveles de almacenamiento identifican el tipo de almacenamiento que utiliza un nodo de almacenamiento. Puedes crear niveles de almacenamiento si deseas que las reglas de ILM coloquen determinados objetos en determinados nodos de almacenamiento.

Antes de empezar

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

Acerca de esta tarea

Al instalar StorageGRID por primera vez, se asigna automáticamente el nivel de almacenamiento **Predeterminado** a todos los nodos de almacenamiento del sistema. Si es necesario, puedes definir opcionalmente niveles de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

El uso de niveles de almacenamiento personalizados te permite crear grupos de almacenamiento ILM que contengan únicamente un tipo específico de nodo de almacenamiento. Por ejemplo, es posible que desees que determinados objetos se almacenen en tus nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash de StorageGRID.

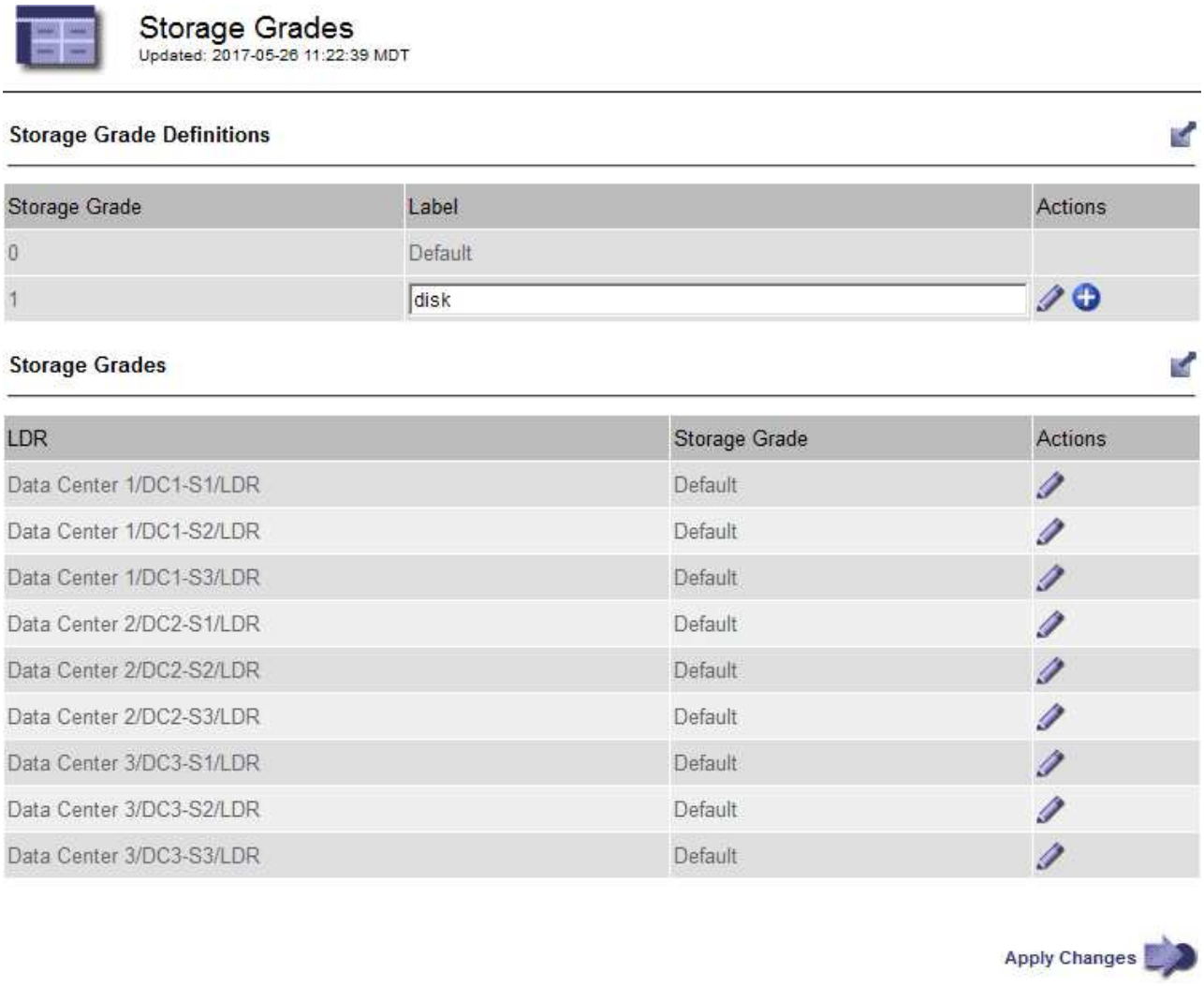
> ⓘ A los nodos de almacenamiento «solo metadatos» no se les puede asignar un nivel de almacenamiento. Para obtener más información, consulta "Tipos de nodos de almacenamiento".

Si el nivel de almacenamiento no es un factor relevante (por ejemplo, si todos los nodos de almacenamiento son idénticos), puedes omitir este procedimiento y utilizar la opción **incluye todos los niveles de almacenamiento** para el nivel de almacenamiento cuando "crear grupos de almacenamiento". Usar esta opción asegura que el grupo de almacenamiento incluya todos los nodos de almacenamiento del sitio, sin importar su nivel de almacenamiento.

> ⓘ No crees más niveles de almacenamiento de los necesarios. Por ejemplo, no crees un nivel de almacenamiento para cada Storage Node. En su lugar, asigna cada nivel de almacenamiento a dos o más nodos. Los niveles de almacenamiento asignados a un solo nodo pueden provocar atascos en ILM si ese nodo deja de estar disponible.

Pasos

1. Selecciona **ILM** > **Niveles de almacenamiento**.
2. Define grados de almacenamiento personalizados:
   a. Para cada nivel de almacenamiento personalizado que quieras añadir, selecciona **Insert**  para añadir una fila.
   b. Introduce una etiqueta descriptiva.



c. Selecciona **Aplicar cambios**.

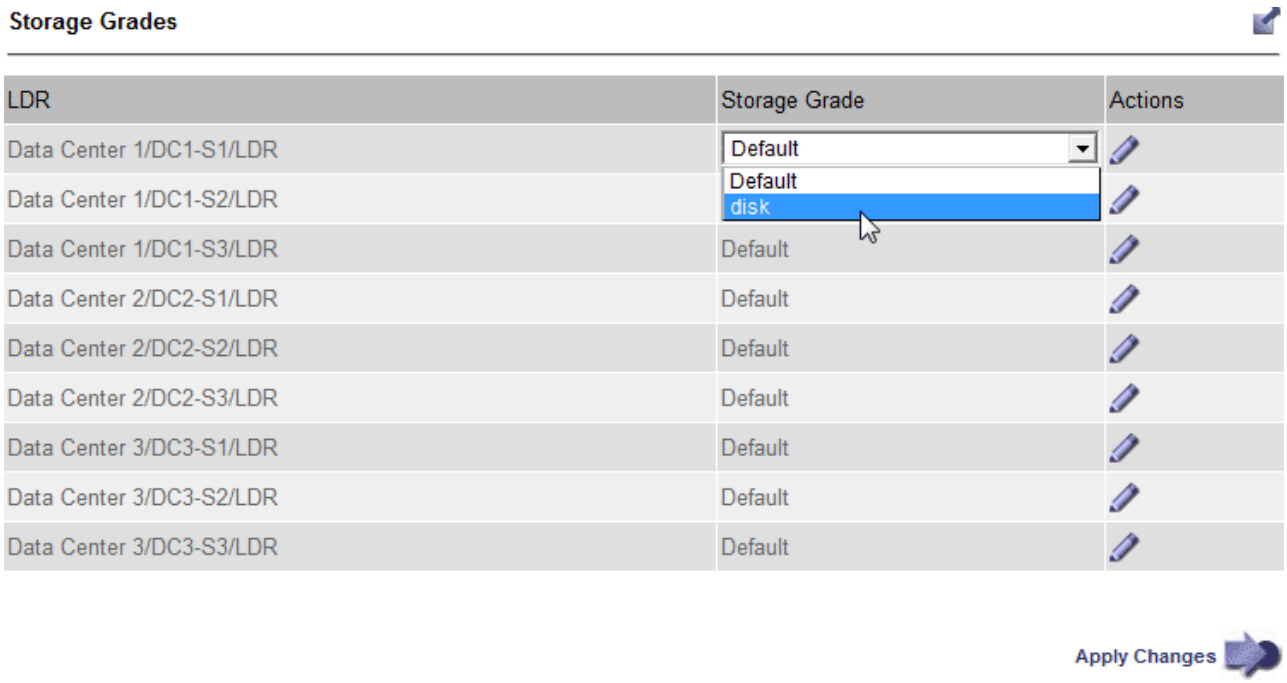
d. Si lo deseas, si necesitas modificar una etiqueta guardada, selecciona **Editar** y selecciona **Aplicar cambios**.

No puedes eliminar los niveles de almacenamiento.

3. Asigna nuevos niveles de almacenamiento a los nodos de almacenamiento:

a. Busca el nodo de almacenamiento en la lista LDR y selecciona su icono **Editar**.

b. Selecciona el grado de almacenamiento adecuado de la lista.



Asigna un nivel de almacenamiento a un Storage Node determinado solo una vez. Un Storage Node recuperado tras un fallo mantiene el nivel de almacenamiento asignado anteriormente. No cambies esta asignación después de que la política de ILM esté activada. Si se cambia la asignación, los datos se almacenan según el nuevo nivel de almacenamiento.

a. Selecciona **Aplicar cambios**.

Usa grupos de almacenamiento

Conoce los grupos de almacenamiento en StorageGRID

Un grupo de almacenamiento es una agrupación lógica de nodos de almacenamiento.

Al instalar StorageGRID, se crea automáticamente un grupo de almacenamiento por cada sitio. Puedes configurar grupos de almacenamiento adicionales según tus requisitos de almacenamiento.

Los nodos de almacenamiento pueden configurarse durante la instalación para que contengan datos de objetos y metadatos (nodo de almacenamiento «combinado»), solo metadatos de objetos o solo datos de objetos. Los nodos de almacenamiento que contienen únicamente metadatos no pueden utilizarse en grupos de almacenamiento. Para obtener más información, consulta "Tipos de nodos de almacenamiento".

Los grupos de almacenamiento tienen dos atributos:

- **Nivel de almacenamiento**: para los Storage Nodes, el rendimiento relativo del almacenamiento subyacente.
- **Ubicación**: el centro de datos donde se almacenarán los objetos.

Los grupos de almacenamiento se utilizan en las reglas de ILM para determinar dónde se almacenan los datos de los objetos y el tipo de almacenamiento que se utiliza. Cuando configuras las reglas de ILM para la

replicación, seleccionas uno o varios grupos de almacenamiento.

Directrices para la configuración de storage pool en StorageGRID

Configura y utiliza grupos de almacenamiento para protegerte contra la pérdida de datos distribuyéndolos entre varias ubicaciones. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de grupos de almacenamiento.

Consulta "Ejemplos de cómo habilitar la protección contra la pérdida de sitios mediante la replicación y el código de borrado".

Directrices para todos los grupos de almacenamiento

- Mantén las configuraciones de los grupos de almacenamiento lo más sencillas posible. No crees más grupos de almacenamiento de los necesarios.
- Crea grupos de almacenamiento con el mayor número posible de nodos. Cada grupo de almacenamiento debe contener dos o más nodos. Un grupo de almacenamiento con un número insuficiente de nodos puede provocar atascos en el ILM si un nodo deja de estar disponible.
- Evita crear o utilizar grupos de almacenamiento que se solapen (que contengan uno o más de los mismos nodos). Si los grupos de almacenamiento se solapan, es posible que se guarde más de una copia de los datos de los objetos en el mismo nodo.
- En general, no utilices el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) ni el sitio All Sites. Estos elementos se actualizan automáticamente para incluir cualquier sitio nuevo que añadas en una ampliación, lo que quizá no sea el comportamiento que deseas.

Directrices para los grupos de almacenamiento utilizados para copias replicadas

- Para la protección contra la pérdida de un sitio mediante "replicación", especifica uno o varios grupos de almacenamiento específicos del sitio en "instrucciones de colocación para cada regla del ILM".

  Durante la instalación de StorageGRID, se crea automáticamente un grupo de almacenamiento para cada sitio.

  El uso de un grupo de almacenamiento para cada sitio garantiza que las copias replicadas de los objetos se almacenen exactamente donde esperas (por ejemplo, una copia de cada objeto en cada sitio para protegerte ante la pérdida de un sitio).

- Si añades un sitio en una ampliación, crea un nuevo grupo de almacenamiento que contenga únicamente el nuevo sitio. Luego, "Actualizar las reglas de ILM" para controlar qué objetos se almacenan en el nuevo sitio.
- Si el número de copias es inferior al número de grupos de almacenamiento, el sistema distribuye las copias para equilibrar el uso del disco entre los grupos.
- Si los grupos de almacenamiento se solapan (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden únicamente en un solo sitio. Debes asegurarte de que los grupos de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Directrices para los grupos de almacenamiento usados para copias con código de borrado

- Para la protección contra la pérdida de sitios mediante "codificación de borrado", crea grupos de almacenamiento que consten de al menos tres sitios. Si un grupo de almacenamiento incluye solo dos sitios, no puedes usar ese grupo de almacenamiento para el código de borrado. No hay esquemas de

código de borrado disponibles para un grupo de almacenamiento que tenga dos sitios.

- El número de nodos de almacenamiento y de emplazamientos que componen el grupo de almacenamiento determina qué "esquemas de codificación de borrado" están disponibles.
- Si es posible, un grupo de almacenamiento debería incluir más que el número mínimo de nodos de almacenamiento requerido para el esquema de código de borrado que elijas. Por ejemplo, si utilizas un esquema de código de borrado 6+3, debes tener al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuye los nodos de almacenamiento entre los distintos emplazamientos de la forma más uniforme posible. Por ejemplo, para admitir un esquema de código de borrado 6+3, configura un grupo de almacenamiento que incluya al menos tres nodos de almacenamiento en tres emplazamientos.
- Si tienes requisitos de rendimiento elevados, no se recomienda utilizar un grupo de almacenamiento que incluya varios sitios si la latencia de red entre sitios es superior a 100 ms. A medida que aumenta la latencia, la velocidad a la que StorageGRID puede crear, colocar y recuperar fragmentos de objetos disminuye drásticamente debido a la reducción del rendimiento de la red TCP.

  La disminución del rendimiento afecta las velocidades máximas alcanzables de ingesta y recuperación de objetos (cuando se seleccionan los comportamientos de ingesta Balanced o Strict) o podría provocar atascos en las colas de ILM (cuando se selecciona el comportamiento de ingesta Dual commit). Consulta "Comportamiento de ingesta según la regla ILM".

> Si tu grid incluye solo un sitio, no podrás utilizar el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) ni el sitio All Sites en un perfil de código de borrado. Este comportamiento evita que el perfil deje de ser válido si se añade un segundo sitio.

Protección contra pérdida de sitios con pools de almacenamiento en StorageGRID

Si tu implementación de StorageGRID incluye más de un sitio, puedes utilizar la replicación y el código de borrado con grupos de almacenamiento configurados adecuadamente para habilitar la protección frente a la pérdida de un sitio.

La replicación y el código de borrado requieren diferentes configuraciones del grupo de almacenamiento:

- Para utilizar la replicación como protección frente a la pérdida de un sitio, utiliza los grupos de almacenamiento específicos de cada sitio que se crean automáticamente durante la instalación de StorageGRID. Luego crea reglas de ILM con "instrucciones de colocación" que especifiquen varios grupos de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar el código de borrado como protección frente a la pérdida de un sitio, "crear grupos de almacenamiento que consten de varios sitios". Luego crea reglas de ILM que usen un grupo de almacenamiento compuesto por varios sitios y cualquier esquema de código de borrado disponible.

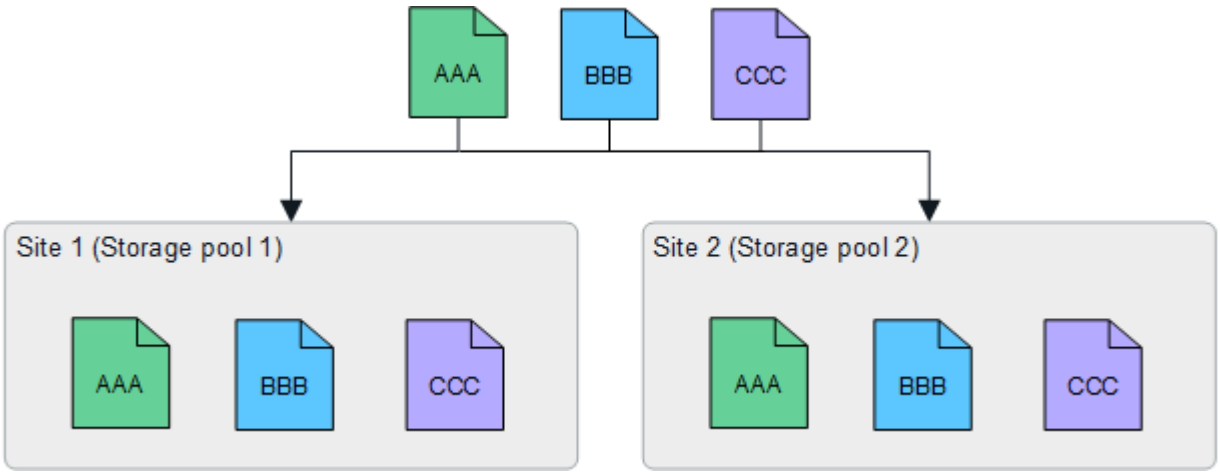
> Al configurar tu implementación de StorageGRID para la protección frente a la pérdida de un sitio, también debes tener en cuenta los efectos de "opciones de ingesta" y "coherencia".

Ejemplo de replicación

De forma predeterminada, durante la instalación de StorageGRID se crea un grupo de almacenamiento para cada sitio. Disponer de grupos de almacenamiento formados por un único sitio permite configurar reglas de ILM que utilicen la replicación como protección ante la pérdida de un sitio. En este ejemplo:

- El pool de almacenamiento 1 contiene Site 1
- El grupo de almacenamiento 2 contiene Site 2
- La regla ILM contiene dos ubicaciones:
  - Almacena objetos replicando 1 copia en el sitio 1
  - Almacena objetos replicando 1 copia en el sitio 2

Ubicaciones de las reglas de ILM:



Si se pierde una de las sedes, se dispone de copias de los objetos en la otra sede.

Ejemplo de erasure coding

Disponer de grupos de almacenamiento que consten de más de un sitio por grupo permite configurar reglas de ILM que utilicen el código de borrado para la protección frente a la pérdida de un sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene los sitios 1 al 3
- La regla ILM contiene una ubicación: almacenar objetos mediante el código de borrado utilizando un esquema EC 4+2 en Storage pool 1, que contiene tres sitios

Ubicaciones de las reglas de ILM:

En este ejemplo:

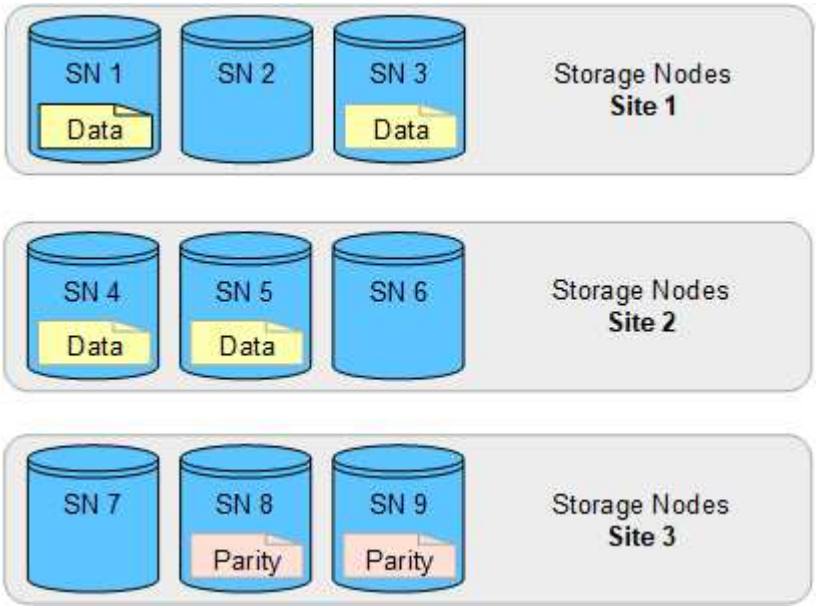
- La regla ILM utiliza un esquema de código de borrado 4+2.
- Cada objeto se divide en cuatro fragmentos de datos iguales, y a partir de los datos del objeto se calculan

dos fragmentos de paridad.

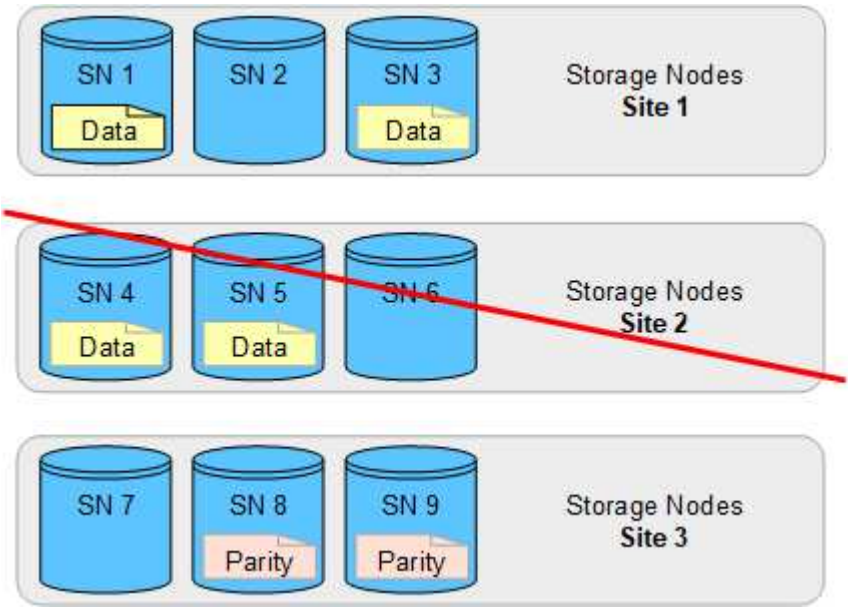
- Cada uno de los seis fragmentos se almacena en un nodo diferente repartido entre tres centros de datos para proporcionar protección de datos ante fallos de nodo o pérdida de sitio.

> El código de borrado está permitido en los grupos de almacenamiento que contienen cualquier número de sitios *excepto* dos sitios.

Regla ILM que utiliza el esquema de código de borrado 4+2:



Si se pierde un sitio, los datos aún se pueden recuperar:



Crea un pool de almacenamiento en StorageGRID

Creas grupos de almacenamiento para determinar dónde almacena el sistema StorageGRID los datos de los objetos y el tipo de almacenamiento que se usa. Cada

grupo de almacenamiento incluye uno o varios sitios y uno o varios niveles de almacenamiento.

> Al instalar StorageGRID 12.0 en una nueva grid, se crean automáticamente grupos de almacenamiento para cada sitio. Sin embargo, si inicialmente instalaste StorageGRID 11.6 o una versión anterior, los grupos de almacenamiento no se crean automáticamente para cada sitio.

Si deseas crear Cloud Storage Pools para almacenar datos de objetos fuera de tu sistema StorageGRID, consulta la "Información sobre el uso de Cloud Storage Pools".

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ya has consultado las directrices para crear grupos de almacenamiento.

Acerca de esta tarea

Los grupos de almacenamiento determinan dónde se almacenan los datos de los objetos. El número de grupos de almacenamiento que necesitas depende del número de sitios en tu grid y de los tipos de copias que quieres: replicadas o con código de borrado.

- Para la replicación y el código de borrado en un único sitio, crea un grupo de almacenamiento para cada sitio. Por ejemplo, si deseas almacenar copias replicadas de objetos en tres sitios, crea tres grupos de almacenamiento.
- Para el código de borrado en tres o más sitios, crea un grupo de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si quieres aplicar el código de borrado a objetos en tres sitios, crea un solo grupo de almacenamiento.

> No incluyas el sitio «All Sites» en un grupo de almacenamiento que se vaya a utilizar en un perfil de código de borrado. En su lugar, añade una entrada independiente al grupo de almacenamiento para cada sitio que vaya a almacenar datos con código de borrado. Consulta este paso para ver un ejemplo.

- Si tienes más de un nivel de almacenamiento, no crees un grupo de almacenamiento que incluya diferentes niveles de almacenamiento en un solo sitio. Consulta el "Directrices para la creación de grupos de almacenamiento".

Pasos

1. Selecciona **ILM** > **Storage pools**.

   La pestaña «Grupos de almacenamiento» muestra todos los grupos de almacenamiento definidos.

   > En las nuevas instalaciones de StorageGRID 11.6 o versiones anteriores, el grupo de almacenamiento All Storage Nodes se actualiza automáticamente cada vez que añades nuevas sedes de centro de datos. No utilices este grupo en las reglas de ILM.

2. Para crear un nuevo grupo de almacenamiento, selecciona **Crear**.
3. Introduce un nombre único para el grupo de almacenamiento. Elige un nombre que resulte fácil de identificar a la hora de configurar perfiles de código de borrado y reglas de ILM.
4. En la lista desplegable **Sitio**, selecciona un sitio para este grupo de almacenamiento.

Al seleccionar un sitio, el número de nodos de almacenamiento en la tabla se actualiza automáticamente.

En general, no utilices el sitio All Sites en ningún grupo de almacenamiento. Las reglas de ILM que utilizan un grupo de almacenamiento All Sites colocan los objetos en cualquier sitio disponible, lo que te da menos control sobre la ubicación de los objetos. Además, un grupo de almacenamiento All Sites utiliza inmediatamente los Storage Nodes de un nuevo sitio, lo que podría no ser el comportamiento que esperas.

5. En la lista desplegable **Storage grade**, selecciona el tipo de almacenamiento que se usará si una regla de ILM utiliza este grupo de almacenamiento.

   El nivel de almacenamiento, *incluye todos los niveles de almacenamiento*, abarca todos los Storage Nodes del emplazamiento seleccionado. Si has creado niveles de almacenamiento adicionales para los Storage Nodes de tu grid, aparecerán en el menú desplegable.

6. Si deseas utilizar el grupo de almacenamiento en un perfil de código de borrado multisitio, selecciona **Add more nodes** para añadir una entrada para cada sitio al grupo de almacenamiento.

   > Se te avisará si añades más de una entrada con distintos grados de almacenamiento para un sitio.

   Para eliminar una entrada, selecciona el icono de eliminación ✕.

7. Cuando estés satisfecho con tus selecciones, selecciona **Guardar**.

   El nuevo grupo de almacenamiento se añade a la lista.

Ver detalles del pool de almacenamiento en StorageGRID

Puedes consultar los detalles de un grupo de almacenamiento para determinar dónde se utiliza dicho grupo y ver qué nodos y niveles de almacenamiento incluye.

Antes de empezar

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

Pasos

1. Selecciona **ILM** > **Storage pools**.

   La tabla «Grupos de almacenamiento» incluye la siguiente información para cada grupo de almacenamiento que incluye nodos de almacenamiento:

   - **Nombre**: El nombre de visualización único del storage pool.
   - **Número de nodos**: el número de nodos en el grupo de almacenamiento.
   - **Uso del almacenamiento**: El porcentaje del espacio total utilizable que se ha utilizado para los datos de objetos en este nodo. Este valor no incluye los metadatos de los objetos.
   - **Capacidad total**: El tamaño del grupo de almacenamiento, que equivale a la cantidad total de espacio utilizable para los datos de los objetos de todos los nodos del grupo de almacenamiento.
   - **Uso de ILM**: Cómo se está utilizando actualmente el grupo de almacenamiento. Un grupo de almacenamiento puede estar sin utilizar o puede estar siendo utilizado en una o varias reglas de ILM, perfiles de código de borrado o en ambos.

2. Para ver los detalles de un grupo de almacenamiento concreto, selecciona su nombre.

   Aparece la página de detalles del grupo de almacenamiento.

3. Accede a la pestaña **Nodos** para obtener información sobre los Storage Nodes incluidos en el grupo de almacenamiento.

   La tabla incluye la siguiente información para cada nodo:

   - Nombre de nodo
   - Nombre del sitio
   - Nivel de almacenamiento
   - Uso del almacenamiento: el porcentaje del espacio total utilizable para datos de objetos que se ha utilizado para el nodo de almacenamiento.

   > El mismo valor de «Uso de almacenamiento (%)» también se muestra en el gráfico «Almacenamiento utilizado - Datos de objetos» para cada Storage Node (selecciona **Nodes** > ***Storage Node*** > **Storage**).

4. Consulta la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento se está utilizando actualmente en alguna regla de ILM o en algún perfil de código de borrado.
5. Opcionalmente, ve a la **página de reglas de ILM** para conocer y gestionar cualquier regla que use el grupo de almacenamiento.

   Consulta el "Instrucciones para trabajar con reglas de ILM".

Edita un pool de almacenamiento en StorageGRID

Puedes editar un grupo de almacenamiento para cambiar su nombre o para actualizar los sitios y los niveles de almacenamiento.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has revisado la "Directrices para la creación de grupos de almacenamiento".
- Si planeas editar un grupo de almacenamiento que está siendo usado por una regla en la política de ILM activa, ya has considerado cómo tus cambios afectarán la ubicación de los datos de los objetos.

Acerca de esta tarea

Si añades un nuevo emplazamiento o un nuevo nivel de almacenamiento a un grupo de almacenamiento que se utiliza en la política de ILM activa, ten en cuenta que los nodos de almacenamiento del nuevo emplazamiento o nivel de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a utilizar un nuevo emplazamiento o nivel de almacenamiento, debes activar una nueva política de ILM tras guardar el grupo de almacenamiento editado.

Pasos

1. Selecciona **ILM** > **Storage pools**.
2. Marca la casilla correspondiente al storage pool que deseas editar.

No puedes editar el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores).

3. Selecciona **Editar**.
4. Según sea necesario, cambia el nombre del grupo de almacenamiento.
5. Según sea necesario, selecciona otros sitios y niveles de almacenamiento.

   No puedes cambiar la ubicación o el nivel de almacenamiento si el grupo de almacenamiento se usa en un perfil de código de borrado y el cambio haría que el esquema de código de borrado dejara de ser válido. Por ejemplo, si un grupo de almacenamiento usado en un perfil de código de borrado incluye actualmente un nivel de almacenamiento con solo una ubicación, no puedes usar un nivel de almacenamiento con dos ubicaciones porque el cambio haría que el esquema de código de borrado dejara de ser válido.

   > Añadir o eliminar sitios de un grupo de almacenamiento existente no moverá ningún dato existente codificado por borrado. Si quieres mover los datos existentes del sitio, debes crear un nuevo grupo de almacenamiento y un perfil de EC para volver a codificar los datos.

6. Selecciona **Guardar**.

Después de que termines

Si añadiste un nuevo sitio o un nuevo nivel de almacenamiento a un grupo de almacenamiento usado en la política de ILM activa, activa una nueva política de ILM para obligar a StorageGRID a usar el nuevo sitio o nivel de almacenamiento. Por ejemplo, clona tu política de ILM existente y luego activa la copia. Consulta "Trabaja con reglas y políticas de ILM".

Eliminar un pool de almacenamiento en StorageGRID

Puedes eliminar un grupo de almacenamiento que no se está utilizando.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permisos de acceso necesarios".

Pasos

1. Selecciona **ILM** > **Storage pools**.
2. Consulta la columna «Uso de ILM» de la tabla para determinar si puedes eliminar el grupo de almacenamiento.

   No puedes eliminar un grupo de almacenamiento si se está utilizando en una regla de ILM o en un perfil de código de borrado. Según sea necesario, selecciona ***storage pool name*** > **ILM usage** para determinar dónde se utiliza el grupo de almacenamiento.

3. Si el grupo de almacenamiento que quieres eliminar no se está utilizando, selecciona la casilla.
4. Selecciona **Eliminar**.
5. Selecciona **Aceptar**.

Usa grupos de almacenamiento en la nube

Conoce los Cloud Storage Pools en StorageGRID

Un grupo de almacenamiento en la nube te permite utilizar ILM para trasladar datos de objetos fuera de tu sistema StorageGRID. Por ejemplo, podrías querer trasladar objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor coste, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso Archive en el almacenamiento de blobs de Microsoft Azure. O quizá quieras mantener una copia de seguridad en la nube de los objetos de StorageGRID para mejorar la recuperación ante desastres.

Desde el punto de vista de ILM, un grupo de almacenamiento en la nube es similar a un grupo de almacenamiento. Para almacenar objetos en cualquiera de estas ubicaciones, seleccionas el grupo al crear las instrucciones de ubicación para una regla de ILM. Sin embargo, mientras que los grupos de almacenamiento están formados por nodos de almacenamiento dentro del sistema StorageGRID, un grupo de almacenamiento en la nube está formado por un bucket externo (S3) o un contenedor (Azure Blob storage).

La tabla compara los grupos de almacenamiento con los Cloud Storage Pools y muestra las similitudes y diferencias a grandes rasgos.

	Pool de almacenamiento	**Grupo de almacenamiento en la nube**
¿Cómo se crea?	Utilizando la opción **ILM** > **Grupos de almacenamiento** en Grid Manager.	Utilizando la opción **ILM** > **Storage pools** > **Cloud Storage Pools** en Grid Manager. Debes configurar el bucket o contenedor externo antes de poder crear el Cloud Storage Pool.
¿Cuántos grupos puedes crear?	Ilimitado.	Hasta 10.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Dónde se almacenan los objetos?	En uno o varios nodos de almacenamiento de StorageGRID.	En un bucket de Amazon S3, un contenedor de Azure Blob storage o en Google Cloud que es externo al sistema StorageGRID. Si el Cloud Storage Pool es un bucket de Amazon S3: • Si lo deseas, puedes configurar el ciclo de vida de un bucket para trasladar los objetos a un almacenamiento a largo plazo y de bajo coste, 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 de S3 RestoreObject. • Puedes crear Cloud Storage Pools para utilizarlos con AWS Commercial Cloud Services (C2S), que son compatibles con AWS Secret Region. Si el Cloud Storage Pool es un contenedor de Azure Blob storage, StorageGRID traslada el objeto al nivel Archive. **Nota:** En general, no configures la gestión del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado para un Cloud Storage Pool. Las operaciones RestoreObject en objetos en el Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.
¿Qué determina la ubicación de los objetos?	Una regla de ILM en las políticas de ILM activas.	Una regla de ILM en las políticas de ILM activas.
¿Qué método de protección de datos se utiliza?	Replicación o codificación de borrado.	Replicación.
¿Cuántas copias de cada objeto se permiten?	Varios.	Una copia en el grupo de almacenamiento en la nube y, opcionalmente, una o más copias en StorageGRID. **Nota:** No puedes almacenar un objeto en más de un Cloud Storage Pool a la vez.
¿Cuáles son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento económico. **Nota**: Los datos de FabricPool no se pueden clasificar por niveles en Cloud Storage Pools.

Ciclo de vida de un objeto Cloud Storage Pool en StorageGRID

Antes de implementar Cloud Storage Pools, revisa el ciclo de vida de los objetos almacenados en cada tipo de Cloud Storage Pool.

S3: ciclo de vida de un objeto del Cloud Storage Pool

Estos pasos describen las fases del ciclo de vida de un objeto almacenado en un S3 Cloud Storage Pool.

> El término «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 Expedited. Solo se admite la recuperación Bulk o Standard.

> Google Cloud Platform (GCP) permite recuperar objetos del almacenamiento a largo plazo sin necesidad de realizar una operación POST Restore.

1. **Objeto almacenado en StorageGRID**

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

2. **Objeto trasladado al grupo de almacenamiento en la nube S3**
   - Cuando el objeto coincide con una regla de ILM que utiliza un grupo de almacenamiento en la nube S3 como ubicación de almacenamiento, StorageGRID mueve el objeto al bucket S3 externo especificado por el Cloud Storage Pool.
   - Cuando el objeto se ha movido al grupo de almacenamiento en la nube S3, la aplicación cliente puede recuperarlo usando una solicitud S3 GetObject desde StorageGRID, a menos que el objeto haya sido trasladado al almacenamiento Glacier.
3. **Objeto transferido a Glacier (estado no recuperable)**
   - Opcionalmente, el objeto puede trasladarse al almacenamiento Glacier. Por ejemplo, el bucket externo de S3 podría utilizar la configuración del ciclo de vida para trasladar un objeto al almacenamiento Glacier de forma inmediata o tras un determinado número de días.

     > Si deseas realizar la transición de objetos, debes crear una configuración de ciclo de vida para el bucket externo de S3 y debes usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API RestoreObject de S3.

   - Durante la transición, la aplicación cliente puede usar una solicitud S3 HeadObject para supervisar el estado del objeto.
4. **Objeto recuperado del almacenamiento de Glacier**

   Si un objeto se ha trasladado al almacenamiento Glacier, la aplicación cliente puede enviar una solicitud S3 RestoreObject para restaurar una copia recuperable en el grupo de almacenamiento en la nube de S3. La solicitud especifica durante cuántos días debe estar disponible la copia en el grupo de almacenamiento en la nube y el nivel de acceso a los datos que se utilizará para la operación de restauración (Expedited, Standard o Bulk). Cuando se alcanza la fecha de caducidad de la copia recuperable, esta vuelve automáticamente a un estado no recuperable.

Si también existen una o más copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier mediante una solicitud RestoreObject. En su lugar, 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 enviar una solicitud de GetObject para recuperar el objeto restaurado.

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

Estos pasos describen las fases 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 trasladado al grupo de almacenamiento en la nube de Azure**

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

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

   Inmediatamente después de trasladar el objeto al grupo de almacenamiento en la nube de Azure, StorageGRID traslada automáticamente el objeto al nivel de archivo de Azure Blob storage.

4. **Objeto recuperado del nivel Archive**

   Si un objeto se ha trasladado al nivel Archive, la aplicación cliente puede enviar una solicitud S3 RestoreObject para restaurar una copia recuperable en el Azure Cloud Storage Pool.

   Cuando StorageGRID recibe la RestoreObject, traslada temporalmente el objeto al nivel Cool del almacenamiento de blobs de Azure. En cuanto se alcanza la fecha de caducidad en la solicitud RestoreObject, StorageGRID traslada el objeto de nuevo al nivel Archive.

   Si también existen una o más copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso Archive mediante una solicitud RestoreObject. En su lugar, 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 enviar una solicitud de GetObject para recuperar el objeto restaurado.

Información relacionada

"Usa la API de REST de S3"

Casos de uso de Cloud Storage Pool en StorageGRID

Con los Cloud Storage Pools, puedes hacer backup o clasificar datos por niveles en una ubicación externa. Además, puedes hacer backup o clasificar datos por niveles en más de una nube.

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

Puedes utilizar un Cloud Storage Pool para hacer backup de los objetos de StorageGRID en una ubicación externa.

Si no se puede acceder a las copias de StorageGRID, se pueden utilizar los datos de los objetos del Cloud Storage Pool para atender las solicitudes de los clientes. No obstante, es posible que tengas que enviar una solicitud S3 RestoreObject para acceder a la copia de backup del objeto en el Cloud Storage Pool.

Los datos de los objetos de un Cloud Storage Pool también pueden utilizarse para recuperar datos perdidos de StorageGRID debido a un fallo en un volumen de almacenamiento o en un Storage Node. Si la única copia restante de un objeto está en un Cloud Storage Pool, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el Storage Node recuperado.

Para implementar una solución de backup:

1. Crea un único Cloud Storage Pool.
2. Configura una regla de ILM que almacene simultáneamente copias de objetos en Storage Nodes (como copias replicadas o con código de borrado) y una única copia de objeto en el Cloud Storage Pool.
3. Añade la regla a tu política de ILM. Luego, simula y activa la política.

Transfiere datos de niveles de StorageGRID a una ubicación externa

Puedes utilizar un grupo de almacenamiento en la nube para almacenar objetos fuera del sistema StorageGRID. Por ejemplo, supón que tienes un gran número de objetos que necesitas conservar, pero esperas acceder a esos objetos rara vez, si es que alguna vez lo haces. Puedes utilizar un grupo de almacenamiento en la nube para trasladar los objetos a un almacenamiento de menor coste y liberar espacio en StorageGRID.

Para implementar una solución de tiering:

1. Crea un único Cloud Storage Pool.
2. Configura una regla de ILM que traslade los objetos que se utilizan con poca frecuencia de los Storage Nodes al Cloud Storage Pool.
3. Añade la regla a tu política de ILM. Luego, simula y activa la política.

Gestiona múltiples puntos de conexión en la nube

Puedes configurar varios endpoints de Cloud Storage Pool si quieres clasificar por niveles o hacer backup de los datos de objetos en más de una nube. Los filtros en tus reglas de ILM te permiten especificar qué objetos se almacenan en cada Cloud Storage Pool. Por ejemplo, podrías querer almacenar objetos de algunos tenants o buckets en Amazon S3 Glacier y objetos de otros tenants o buckets en Azure Blob storage. O podrías querer mover datos entre Amazon S3 Glacier y Azure Blob storage.

Cuando utilices varios puntos de conexión de Cloud Storage Pool, ten en cuenta que un objeto solo puede almacenarse en un Cloud Storage Pool a la vez.

Para implementar varios puntos de conexión en la nube:

1. Crea hasta 10 Cloud Storage Pools.
2. Configura las reglas de ILM para almacenar los datos de objetos adecuados en el momento adecuado en cada Cloud Storage Pool. Por ejemplo, almacena objetos del bucket A en Cloud Storage Pool A y objetos del bucket B en Cloud Storage Pool B. O bien, almacena objetos en Cloud Storage Pool A durante un tiempo y luego muévelos a Cloud Storage Pool B.
3. Añade las reglas a tu política de ILM. Luego, simula y activa la política.

Requisitos y límites de Cloud Storage Pool en StorageGRID

Si tienes previsto usar un Cloud Storage Pool para mover objetos fuera del sistema StorageGRID, debes revisar las consideraciones para configurar y usar Cloud Storage Pools.

Consideraciones generales

- En general, el almacenamiento de archivo en la nube, como Amazon S3 Glacier o Azure Blob storage, es una opción económica para almacenar datos de objetos. Sin embargo, los costes de recuperar datos del almacenamiento de archivo en la nube son relativamente elevados. Para lograr el menor coste total, debes tener en cuenta cuándo y con qué frecuencia accederás a los objetos en el Cloud Storage Pool. Se recomienda usar un Cloud Storage Pool solo para contenido que esperas acceder con poca frecuencia.
- No se admite el uso de Cloud Storage Pools con FabricPool debido a la latencia adicional para recuperar un objeto del destino de Cloud Storage Pool.
- Los objetos con S3 Object Lock habilitado no se pueden colocar en Cloud Storage Pools.
- Las siguientes combinaciones de plataforma, autenticación y protocolo con S3 Object lock no son compatibles para Cloud Storage Pools:
  - **Plataformas**: Google Cloud Platform y Azure
  - **Tipos de autenticación**: Acceso anónimo
  - **Protocolo**: HTTP

Consideraciones para los puertos utilizados para Cloud Storage Pools

Para garantizar que las reglas de ILM puedan mover objetos hacia y desde el Cloud Storage Pool especificado, debes configurar la red o redes que contienen los Storage Nodes de tu sistema. Debes asegurarte de que los siguientes puertos puedan comunicarse con el Cloud Storage Pool.

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

- **80**: Para los URI de puntos finales que comienzan con http
- **443**: Para los URI de endpoint que comienzan con https

Puedes especificar un puerto diferente cuando creas o editas un Cloud Storage Pool.

Si utilizas un proxy no transparente, también debes "configurar un proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

Consideraciones para los costes

El acceso al almacenamiento en la nube usando un Cloud Storage Pool requiere conectividad de red con la nube. Debes tener en cuenta el coste de la infraestructura de red que vas a utilizar para acceder a la nube y aprovisionarla adecuadamente, según la cantidad de datos que esperas mover entre StorageGRID y la nube usando el Cloud Storage Pool.

Cuando StorageGRID se conecta al punto final externo del Cloud Storage Pool, envía varias solicitudes para supervisar la conectividad y asegurarse de que puede realizar las operaciones necesarias. Aunque estas solicitudes conllevan algunos costes adicionales, el coste de supervisar un Cloud Storage Pool solo debería ser una pequeña fracción del coste total de almacenar objetos en S3 o Azure.

Podrían generarse costes más elevados si necesitas trasladar objetos desde un endpoint externo de Cloud Storage Pool de vuelta a StorageGRID. Los objetos podrían trasladarse de vuelta a StorageGRID en cualquiera de estos casos:

- La única copia del objeto se encuentra en un Cloud Storage Pool y decides almacenarlo en StorageGRID en su lugar. En este caso, reconfiguras tus reglas y políticas de ILM. Cuando se lleva a cabo la evaluación de ILM, StorageGRID envía varias solicitudes para recuperar el objeto del Cloud Storage Pool. Luego, StorageGRID crea localmente el número especificado de copias replicadas o con código de borrado. Después de que el objeto se traslada de nuevo a StorageGRID, se elimina la copia en el Cloud Storage Pool.
- Los objetos se pierden debido a un fallo del nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

> ⓘ Cuando se devuelven objetos a StorageGRID desde un Cloud Storage Pool, StorageGRID envía varias solicitudes al endpoint del Cloud Storage Pool por cada objeto. Antes de mover un gran número de objetos, ponte en contacto con soporte técnico para que te ayuden a estimar el plazo y los costes asociados.

S3: permisos necesarios para el depósito del Cloud Storage Pool

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

El movimiento de objetos entre StorageGRID y el bucket externo de S3 especificado en el Cloud Storage Pool se controla mediante las reglas de ILM y las políticas de ILM activas en StorageGRID. Por el contrario, la transición de objetos desde el bucket externo de S3 especificado en el Cloud Storage Pool a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implemente la clase de almacenamiento Glacier) se controla mediante la configuración del ciclo de vida de ese bucket.

Si deseas trasladar objetos desde el Cloud Storage Pool, debes crear la configuración de ciclo de vida adecuada en el bucket externo de S3 y debes usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API S3 RestoreObject.

Por ejemplo, supongamos que quieres que todos los objetos que se trasladen desde StorageGRID al Cloud Storage Pool pasen inmediatamente al almacenamiento Amazon S3 Glacier. Deberías crear una configuración de ciclo de vida en el bucket externo de S3 que especifique una única acción (**Transition**) 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 los buckets a Amazon S3 Glacier el mismo 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 bucket externo, nunca utilices acciones de **Expiration** para definir cuándo expiran los objetos. Las acciones de Expiration hacen que el sistema de almacenamiento externo elimine los objetos expirados. Si más adelante intentas acceder a un objeto expirado desde StorageGRID, el objeto eliminado no se encontrará.

Si deseas trasladar los objetos del Cloud Storage Pool a S3 Glacier Deep Archive (en lugar de a Amazon S3 Glacier), especifica `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida del bucket. Sin embargo, ten en cuenta que no puedes usar el tier `Expedited` para restaurar objetos desde S3 Glacier Deep Archive.

Azure: consideraciones sobre el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puedes establecer el nivel de acceso predeterminado en Hot o Cool. Al crear una cuenta de almacenamiento para usarla con un Cloud Storage Pool, debes usar el nivel Hot como nivel predeterminado. Aunque StorageGRID establece inmediatamente el nivel en Archive al mover objetos al Cloud Storage Pool, usar la configuración predeterminada Hot asegura que no se te cobre

una tarifa por eliminación anticipada por los objetos eliminados del nivel Cool antes del mínimo de 30 días.

Azure: no se admite la gestión del ciclo de vida

No utilices la gestión del ciclo de vida del almacenamiento de blobs de Azure para el contenedor que se utiliza con un Cloud Storage Pool. Las operaciones del ciclo de vida podrían interferir con las operaciones de Cloud Storage Pool.

Información relacionada

"Crear un grupo de almacenamiento en la nube"

Cloud Storage Pools y replicación CloudMirror en StorageGRID

Al empezar 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 CloudMirror de StorageGRID.

	Grupo de almacenamiento en la nube	Servicio de replicación de CloudMirror
${post_edited_translations.segment}	Actúa como destino de archivo. La copia del objeto en el Cloud Storage Pool puede ser la única copia del objeto o puede ser una copia adicional. Es decir, en lugar de conservar dos copias en las instalaciones, puedes conservar una copia en StorageGRID y enviar una copia al Cloud Storage Pool.	Permite a un inquilino replicar automáticamente objetos desde un bucket en StorageGRID (origen) a un bucket externo de S3 (destino). Crea una copia independiente de un objeto en una infraestructura independiente de S3.
¿Cómo se configura?	Se definen de la misma forma que los grupos de almacenamiento, usando Grid Manager o la Grid Management API. Se pueden seleccionar como ubicación de colocación en una regla de ILM. Mientras que un grupo de almacenamiento está formado por un conjunto de Storage Nodes, un Cloud Storage Pool se define usando un endpoint remoto de S3 o Azure (dirección IP, credenciales, y así sucesivamente).	Un usuario de un inquilino "configura la replicación de CloudMirror" definiendo un punto final CloudMirror (dirección IP, credenciales, etc.) mediante el Gestor de inquilinos o la API de S3. Una vez configurado el punto final CloudMirror, cualquier depósito que pertenezca a esa cuenta de inquilino se puede configurar para que apunte al punto final CloudMirror.
¿Quién se encarga de configurarlo?	Normalmente, un administrador de la grid	Normalmente, un usuario de tenant
${post_edited_translations.segment}	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Nivel de archivo de Azure Blob • ${post_edited_translations.segment}	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • ${post_edited_translations.segment}

	Grupo de almacenamiento en la nube	Servicio de replicación de CloudMirror
¿Qué hace que los objetos se trasladen al destino?	Una o varias reglas de ILM en las políticas de ILM activas. Las reglas de ILM definen qué objetos StorageGRID mueve al Cloud Storage Pool y cuándo se mueven los objetos.	La acción de ingerir un nuevo objeto en un bucket de origen que se haya configurado con un endpoint CloudMirror. Los objetos que existían en el bucket de origen antes de que el bucket se configurara con el endpoint CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se recuperan los objetos?	Las aplicaciones deben enviar solicitudes a StorageGRID para recuperar objetos que se hayan trasladado a un Cloud Storage Pool. Si la única copia de un objeto se ha trasladado al almacenamiento de archivo, StorageGRID gestiona el proceso de restauración del objeto para que pueda recuperarse.	Dado que la copia duplicada en el bucket de destino es una copia independiente, las aplicaciones pueden recuperar el objeto enviando solicitudes tanto a StorageGRID como al destino S3. Por ejemplo, supongamos que usas la replicación de CloudMirror para duplicar objetos en una organización asociada. La organización asociada puede usar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Puedes leer directamente desde el destino?	No. Los objetos trasladados a un Cloud Storage Pool son gestionados por StorageGRID. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de recuperarlos del Cloud Storage Pool).	Sí, porque la copia reflejada es una copia independiente.
¿Qué ocurre si se elimina un objeto de la fuente?	El objeto también se elimina del Cloud Storage Pool.	La acción de eliminación no se replica. Un objeto eliminado deja de existir en el depósito de StorageGRID, pero sigue existiendo en el depósito de destino. Del mismo modo, los objetos del depósito de destino pueden eliminarse sin afectar al de origen.
¿Cómo accedes a los objetos después de un desastre (cuando el sistema StorageGRID no está operativo)?	Los nodos de StorageGRID que hayan fallado deben recuperarse. Durante este proceso, es posible que se restauren copias de objetos replicados utilizando las copias en el Cloud Storage Pool.	Las copias de los objetos en el destino CloudMirror son independientes de StorageGRID, así que puedes acceder a ellas directamente antes de que se recuperen los nodos de StorageGRID.

Crea un Cloud Storage Pool en StorageGRID

Un grupo de almacenamiento en la nube especifica un único bucket externo de Amazon

S3, otro proveedor compatible con S3 o un contenedor de almacenamiento de blobs de Azure.

Al crear un grupo de almacenamiento en la nube, debes especificar el nombre y la ubicación del bucket o contenedor externo que StorageGRID utilizará 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 bucket o contenedor externo.

StorageGRID valida el Cloud Storage Pool en cuanto lo guardas, así que debes asegurarte de que el bucket o contenedor especificado en el Cloud Storage Pool exista y sea accesible.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permisos de acceso necesarios".
- Has revisado la "Consideraciones para Cloud Storage Pools".
- El bucket o contenedor externo al que hace referencia el Cloud Storage Pool ya existe, y tienes el información sobre el endpoint del servicio.
- Para acceder al bucket o al contenedor, tienes la información de la cuenta para el tipo de autenticación que elijas.

Pasos

1. Selecciona **ILM** > **Storage pools** > **Cloud Storage Pools**.
2. Selecciona **Crear** y luego introduce la siguiente información:

Campo	Descripción
Nombre del Cloud Storage Pool	Un nombre que describa brevemente el Cloud Storage Pool y su finalidad. Utiliza un nombre que resulte fácil de identificar a la hora de configurar las reglas de ILM.
Tipo de proveedor	¿Qué proveedor de servicios en la nube vas a utilizar para este Cloud Storage Pool: • **Amazon S3/GCP**: Selecciona esta opción para Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • **Azure Blob Storage**
Bucket o contenedor	El nombre del bucket externo de S3 o del contenedor de Azure. No puedes cambiar este valor después de guardar el Cloud Storage Pool.

3. En función del tipo de proveedor que hayas seleccionado, introduce la información del punto final del servicio.

Amazon S3/GCP

a. Para el protocolo, selecciona HTTPS o HTTP.

> No utilices conexiones HTTP para datos confidenciales.

b. Introduce el nombre de host. Ejemplo:

`s3-aws-region.amazonaws.com`

c. Selecciona el estilo de la URL:

Opción	Descripción
Detección automática	Intenta detectar automáticamente qué estilo de URL usar, basándose en la información proporcionada. Por ejemplo, si especificas una dirección IP, StorageGRID usará una URL de tipo path. Selecciona esta opción solo si no sabes qué estilo específico usar.
Estilo de alojamiento virtual	Utiliza una URL de tipo «host virtual» para acceder al bucket. Las URL de tipo «host virtual» incluyen el nombre del bucket como parte del nombre de dominio. Ejemplo: `https://bucket-name.s3.company.com/key-name`
Estilo path	Utiliza una URL de tipo path para acceder al bucket. Las URL de tipo path incluyen el nombre del bucket al final. Ejemplo: `https://s3.company.com/bucket-name/key-name` **Nota:** No se recomienda utilizar la opción de URL de tipo «path» y dejará de estar disponible en una futura versión de StorageGRID.

d. Si lo deseas, introduce el número de puerto o utiliza el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de blobs de Azure

a. Introduce el URI del endpoint del servicio utilizando uno de los siguientes formatos.

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

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

Si no especificas un puerto, por defecto se usa el puerto 443 para HTTPS y el puerto 80 para HTTP.

4. Selecciona **Continuar**. Luego selecciona el tipo de autenticación e introduce la información necesaria para el endpoint del Cloud Storage Pool:

Clave de acceso

Para Amazon S3/GCP u otros proveedores compatibles con S3

a. **ID de la clave de acceso**: Introduce el ID de la clave de acceso de la cuenta propietaria del bucket externo.
b. **Clave de acceso secreta**: introduce la clave de acceso secreta.

IAM Roles Anywhere

Para el servicio AWS IAM Roles Anywhere

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

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

CAP (portal de acceso C2S)

Para el servicio S3 de Commercial Cloud Services (C2S)

a. **URL de credenciales temporales**: Introduce la URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluyendo todos los parámetros de API obligatorios y opcionales asignados a tu cuenta C2S.
b. **Certificado de CA del servidor**: Selecciona **Examinar** y carga el certificado de CA que StorageGRID utilizará para verificar el servidor CAP. El certificado debe estar codificado en formato PEM y haber sido emitido por una autoridad de certificación (CA) gubernamental adecuada.
c. **Certificado de cliente**: Selecciona **Examinar** y carga el certificado que StorageGRID utilizará para identificarse ante el servidor CAP. El certificado de cliente debe estar codificado en formato PEM, emitido por una autoridad de certificación (CA) gubernamental adecuada y tener acceso a tu cuenta de C2S.
d. **Clave privada del cliente**: Selecciona **Examinar** y carga la clave privada codificada en formato PEM para el certificado de cliente.
e. Si la clave privada del cliente está cifrada, introduce la frase de contraseña para descifrar la clave privada del cliente. En caso contrario, deja en blanco el campo **Frase de contraseña de la clave**

privada del cliente.

> Si el certificado de cliente va a estar cifrado, utiliza el formato tradicional para el cifrado. No se admite el formato cifrado PKCS #8.

Almacenamiento de blobs de Azure

Solo para Azure Blob Storage, clave compartida

a. **Nombre de la cuenta**: Introduce el nombre de la cuenta de almacenamiento que es propietaria del contenedor externo
b. **Clave de la cuenta**: Ingresa la clave secreta para la cuenta de almacenamiento

Puedes utilizar el portal de Azure para encontrar estos valores.

Anónimo

No se requiere información adicional.

5. Selecciona **Continuar**. Luego elige el tipo de verificación del servidor que quieres usar:

Opción	Descripción
Usa certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utiliza los certificados CA de Grid instalados en el sistema operativo para proteger las conexiones.
Usa un certificado de CA personalizado	Utiliza un certificado de CA personalizado. Selecciona **Examinar** y sube el certificado codificado en formato PEM.
No verificar el certificado	Seleccionar esta opción significa que las conexiones TLS al Cloud Storage Pool no son seguras.

6. Selecciona **Guardar**.

   Al guardar un grupo de almacenamiento en la nube, StorageGRID realiza lo siguiente:

   - Comprueba que el bucket o contenedor y el punto final del servicio existan y que se pueda acceder a ellos utilizando las credenciales que hayas especificado.
   - Escribe un archivo de marcador en el bucket o contenedor para identificarlo como un Cloud Storage Pool. Nunca elimines este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

     Si falla la validación del Cloud Storage Pool, recibirás un mensaje de error que explica por qué falló la validación. Por ejemplo, podría aparecer un error si hay un problema con el certificado o si el bucket o contenedor que especificaste no existe todavía.

7. Si se produce un error, consulta la "Instrucciones para solucionar problemas de Cloud Storage Pools", resuelve cualquier problema y luego intenta guardar el Cloud Storage Pool de nuevo.

Ver detalles de Cloud Storage Pool en StorageGRID

Puedes consultar los detalles de un Cloud Storage Pool para determinar dónde se utiliza

y ver qué nodos y niveles de almacenamiento incluye.

Antes de empezar

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

Pasos

1. Selecciona **ILM** > **Storage pools** > **Cloud Storage Pools**.

   La tabla «Cloud Storage Pools» incluye la siguiente información para cada Cloud Storage Pool que incluye Storage Nodes:

   - **Nombre**: El nombre de visualización único del pool.
   - **URI**: El identificador uniforme de recursos del Cloud Storage Pool.
   - **Tipo de proveedor**: qué proveedor de cloud se utiliza para este Cloud Storage Pool.
   - **Contenedor**: El nombre del bucket utilizado para el Cloud Storage Pool.
   - **Uso de ILM**: cómo se está utilizando actualmente el pool. Un Cloud Storage Pool puede estar sin usar o puede estar siendo usado en una o varias reglas de ILM, perfiles de erasure-coding o ambos.
   - **Último error**: El último error detectado durante una comprobación de estado de este Cloud Storage Pool.

2. Para ver los detalles de un Cloud Storage Pool específico, selecciona su nombre.

   Aparece la página de detalles del pool.

3. Accede a la pestaña **Autenticación** para conocer el tipo de autenticación de este Cloud Storage Pool y para modificar los datos de autenticación.
4. Accede a la pestaña **Verificación del servidor** para consultar los detalles de la verificación, editar la verificación, descargar un nuevo certificado o copiar el certificado PEM.
5. Consulta la pestaña **Uso de ILM** para determinar si el Cloud Storage Pool se está utilizando actualmente en alguna regla de ILM o en algún perfil de código de borrado.
6. Si lo deseas, ve a la **página de reglas de ILM** para "conocer y gestionar cualquier norma" que usan el Cloud Storage Pool.

Edita un Cloud Storage Pool en StorageGRID

Puedes editar un grupo de almacenamiento en la nube para cambiar su nombre, el punto final del servicio u otros detalles; sin embargo, no puedes cambiar el S3 bucket ni el Azure container de un grupo de almacenamiento en la nube.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has revisado la "Consideraciones para Cloud Storage Pools".

Pasos

1. Selecciona **ILM** > **Storage pools** > **Cloud Storage Pools**.

La tabla «Cloud Storage Pools» muestra los Cloud Storage Pools existentes.

2. Marca la casilla correspondiente al Cloud Storage Pool que quieras editar y, a continuación, selecciona **Actions** > **Edit**.

   También puedes seleccionar el nombre del Cloud Storage Pool y luego seleccionar **Editar**.

3. Según sea necesario, cambia el nombre del Cloud Storage Pool, el service endpoint, las credenciales de autenticación o el método de verificación de certificados.

   > No puedes cambiar el tipo de proveedor, ni el bucket de S3 ni el contenedor de Azure para un Cloud Storage Pool.

   Si ya has subido un certificado de servidor o de cliente, puedes desplegar el acordeón **Detalles del certificado** para consultar el certificado que se está utilizando actualmente.

4. Selecciona **Guardar**.

   Al guardar un grupo de almacenamiento en la nube, StorageGRID comprueba que el depósito o contenedor y el punto final del servicio existan, y que se pueda acceder a ellos utilizando las credenciales que hayas especificado.

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

   Consulta las instrucciones de "Solución de problemas de Cloud Storage Pools", resuelve el problema y luego intenta guardar el Cloud Storage Pool de nuevo.

Eliminar un Cloud Storage Pool en StorageGRID

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

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permisos de acceso necesarios".

Si es necesario, utiliza ILM para mover los datos de los objetos

Si el Cloud Storage Pool que deseas eliminar contiene datos de objetos, debes utilizar ILM para trasladar los datos a otra ubicación. Por ejemplo, puedes trasladar los datos a Storage Nodes en tu grid o a otro Cloud Storage Pool.

Pasos

1. Selecciona **ILM** > **Storage pools** > **Cloud Storage Pools**.
2. Consulta la columna de uso de ILM en la tabla para determinar si puedes eliminar el Cloud Storage Pool.

   No puedes eliminar un Cloud Storage Pool si se está usando en una regla de ILM o en un perfil de erasure-coding.

3. Si se está utilizando el Cloud Storage Pool, selecciona ***cloud storage pool name*** > **ILM usage**.

4. "Clona cada regla de ILM" que actualmente coloca objetos en el Cloud Storage Pool que quieres eliminar.
5. Decide a dónde quieres mover los objetos existentes gestionados por cada regla que clonaste.

   Puedes utilizar uno o varios grupos de almacenamiento o un Cloud Storage Pool diferente.

6. Edita cada una de las reglas que clonaste.

   En el paso 2 del asistente para crear una regla de ILM, selecciona la nueva ubicación en el campo **copias en**.

7. "Crear una nueva política de ILM" y sustituye cada una de las reglas antiguas por una regla clonada.
8. Activa la nueva política.
9. Espera a que ILM elimine los objetos del Cloud Storage Pool y los coloque en la nueva ubicación.

Eliminar Cloud Storage Pool

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

Antes de empezar

- Has eliminado todas las reglas de ILM que pudieran haber utilizado el pool.
- Has confirmado que el bucket de S3 o el contenedor de Azure no contiene ningún objeto.

  Se produce un error si intentas eliminar un grupo de almacenamiento en la nube que contenga objetos. Consulta "Soluciona problemas de los grupos de almacenamiento en la nube".

> Al crear 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 elimines este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Selecciona **ILM** > **Storage pools** > **Cloud Storage Pools**.
2. Si la columna «Uso de ILM» indica que no se está utilizando Cloud Storage Pool, marca la casilla.
3. ${post_edited_translations.segment}
4. Selecciona **Aceptar**.

Soluciona problemas de los Cloud Storage Pools en StorageGRID

Sigue estos pasos de resolución de problemas para solucionar los errores que puedas encontrar al crear, editar o eliminar un Cloud Storage Pool.

Determina si se ha producido un error

StorageGRID realiza una sencilla comprobación de estado en cada Cloud Storage Pool leyendo el objeto conocido `x-ntap-sgws-cloud-pool-uuid` para garantizar que se puede acceder al Cloud Storage Pool y que está funcionando correctamente. Cuando StorageGRID detecta un error en el endpoint, realiza una comprobación de estado cada minuto desde cada Storage Node. Cuando se resuelve el error, las comprobaciones de estado se detienen. Si una comprobación de estado detecta un problema, se muestra un mensaje en la columna Last error de la tabla Cloud Storage Pools en la página Storage pools.

La tabla muestra el error más reciente detectado para cada Cloud Storage Pool e indica hace cuánto ocurrió el error.

Además, se activa una alerta de **Cloud Storage Pool connectivity error** si la comprobación de estado detecta que se han producido uno o más errores nuevos en Cloud Storage Pool en los últimos 5 minutos. Si recibes una notificación por correo electrónico sobre esta alerta, ve a la página Storage pools (selecciona **ILM** > **Storage pools**), revisa los mensajes de error en la columna Last error y consulta las pautas de resolución de problemas que aparecen a continuación.

Comprueba si se ha solucionado un error

Después de resolver cualquier problema subyacente, puedes comprobar si el error se ha solucionado. En la página Cloud Storage Pool, selecciona el endpoint y selecciona **Borrar error**. Un mensaje de confirmación indica que StorageGRID ha borrado el error del Cloud Storage Pool.

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

Error: Fallo en la comprobación de estado. Error del endpoint

Es posible que te encuentres con este error al habilitar S3 Object Lock con la retención predeterminada para tu bucket de Amazon S3 después de empezar a usar este bucket para un Cloud Storage Pool. Este error se produce cuando la operación PUT no incluye un encabezado HTTP con un valor de suma de comprobación de la carga útil, como `Content-MD5`. Este valor de encabezado es obligatorio para AWS en las operaciones PUT en buckets con S3 Object Lock habilitado.

Para solucionar este problema, sigue los pasos que se indican en "Editar un Cloud Storage Pool" sin realizar ningún cambio. Esta acción activa la validación de la configuración del Cloud Storage Pool, que detecta y actualiza automáticamente la bandera S3 Object Lock en la configuración del endpoint del Cloud Storage Pool.

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

Es posible que te encuentres con este error al intentar crear, editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el bucket o el 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, este error solo aparecerá si estás creando un nuevo Cloud Storage Pool y ya hay otra instancia de StorageGRID utilizando ese mismo Cloud Storage Pool.

Prueba a seguir uno de estos pasos para solucionar el problema:

- Si estás configurando un nuevo grupo de almacenamiento en la nube y el bucket contiene el archivo `x-ntap-sgws-cloud-pool-uuid` y claves de objetos adicionales similares al siguiente ejemplo, crea un bucket nuevo y usa este bucket nuevo en su lugar.

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

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

Si estos pasos no se ajustan a tu caso, ponte en contacto con soporte técnico.

Error: No se pudo crear ni actualizar el Cloud Storage Pool. Error del endpoint

Es posible que te encuentres con este error en las siguientes circunstancias:

- Cuando intentas crear o editar un Cloud Storage Pool.
- Cuando seleccionas una combinación de plataforma, autenticación o protocolo no compatible con S3 Object Lock durante la configuración de un nuevo Cloud Storage Pool. Consulta "Aspectos a tener en cuenta sobre los grupos de almacenamiento en la nube".

Este error indica que un problema de conectividad o de configuración impide que StorageGRID escriba en el Cloud Storage Pool.

Para solucionar el problema, revisa el mensaje de error del endpoint.

- Si el mensaje de error incluye `Get *url*: EOF`, comprueba que el punto final del servicio utilizado para el Cloud Storage Pool no utilice HTTP para un contenedor o bucket que requiera HTTPS.
- Si el mensaje de error incluye `Get *url*: net/http: request canceled while waiting for connection`, comprueba que la configuración de red permita que los Storage Nodes accedan al endpoint del servicio usado para el Cloud Storage Pool.
- Si el error se debe a una plataforma, autenticación o protocolo no compatibles, cambia a una configuración compatible con S3 Object Lock e intenta guardar de nuevo el nuevo Cloud Storage Pool.
- Para el resto de mensajes de error del punto final, prueba una o varias de las siguientes opciones:
  - Crea un contenedor o bucket externo con el mismo nombre que ingresaste para el Cloud Storage Pool e intenta guardar el nuevo Cloud Storage Pool otra vez.
  - Corrige el nombre del contenedor o del bucket que has especificado para el Cloud Storage Pool e intenta guardar de nuevo el nuevo Cloud Storage Pool.

Error: No se pudo analizar el certificado de CA

Es posible que te encuentres con este error al intentar crear o editar un Cloud Storage Pool. El error se produce si StorageGRID no pudo analizar el certificado que introdujiste al configurar el Cloud Storage Pool.

Para solucionar el problema, comprueba si el certificado de la CA que has proporcionado presenta algún problema.

Error: No se ha encontrado ningún Cloud Storage Pool con este ID

Es posible que te encuentres con este error al intentar editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el endpoint devuelve una respuesta 404, lo que puede significar cualquiera de las siguientes situaciones:

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

Prueba uno o varios de estos pasos para corregir el problema:

- Comprueba que el usuario asociado a la clave de acceso configurada disponga de los permisos necesarios.
- Edita el Cloud Storage Pool con credenciales que cuenten con los permisos necesarios.

- Si los permisos son correctos, ponte en contacto con soporte.

Error: No se pudo comprobar el contenido del Cloud Storage Pool. Error del endpoint

Es posible que te encuentres con este error al intentar eliminar un Cloud Storage Pool. Este error indica que algún tipo de problema de conectividad o de configuración impide que StorageGRID lea el contenido del bucket del Cloud Storage Pool.

Para solucionar el problema, revisa el mensaje de error del endpoint.

Error: Ya hay objetos en este bucket

Es posible que te encuentres con este error al intentar eliminar un Cloud Storage Pool. No puedes eliminar un Cloud Storage Pool si contiene datos que fueron trasladados allí por ILM, datos que ya estaban en el bucket antes de configurar el Cloud Storage Pool, o datos que se pusieron en el bucket desde otra fuente después de que se creó el Cloud Storage Pool.

Prueba uno o varios de estos pasos para corregir el problema:

- Sigue las instrucciones para devolver los objetos a StorageGRID en «Ciclo de vida de un objeto de un Cloud Storage Pool».
- Si estás seguro de que los objetos restantes no fueron colocados en el Cloud Storage Pool por ILM, elimina manualmente los objetos del bucket.

> Nunca elimines manualmente objetos de un Cloud Storage Pool que puedan haber sido colocados allí por ILM. Si más adelante intentas acceder a un objeto eliminado manualmente desde StorageGRID, el objeto eliminado no se encontrará.

Error: El proxy encontró un error externo al intentar acceder al Cloud Storage Pool

Es posible que aparezca este error si has configurado un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el endpoint S3 externo utilizado para el Cloud Storage Pool. Este error se produce si el servidor proxy externo no puede acceder al endpoint del 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.

Prueba uno o varios de estos pasos para corregir el problema:

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

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

Es posible que aparezca este error al intentar eliminar un Cloud Storage Pool. Este error se produce cuando la autenticación requiere un certificado X.509 para garantizar que se valida correctamente el Cloud Storage Pool externo y que este está vacío antes de eliminar la configuración del Cloud Storage Pool.

Sigue estos pasos para solucionar el problema:

- Actualiza el certificado configurado para la autenticación en el Cloud Storage Pool.
- Asegúrate de que se resuelva cualquier alerta de caducidad de certificados en este Cloud Storage Pool.

Información relacionada

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

Administra los perfiles de código de borrado en StorageGRID

Puedes consultar los detalles de un perfil de código de borrado y cambiarle el nombre si es necesario. Puedes desactivar un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permisos de acceso necesarios".

Ver los detalles del perfil de código de borrado

Puedes consultar los detalles de un perfil de código de borrado para conocer su estado, el esquema de código de borrado utilizado y otra información.

Pasos

1. Selecciona **Configuración** > **Sistema** > **Erasure coding**.
2. Selecciona el perfil. Aparece la página de detalles del perfil.
3. Opcionalmente, consulta la pestaña de reglas de ILM para ver una lista de las reglas de ILM que usan el perfil y las políticas de ILM que usan esas reglas.
4. Si lo deseas, consulta la pestaña Storage Nodes para ver detalles sobre cada Storage Node en el grupo de almacenamiento del perfil, como el sitio donde se encuentra y el uso de almacenamiento.

Cambiar el nombre de un perfil de código de borrado

Quizá te interese cambiar el nombre de un perfil de código de borrado para que quede más claro qué hace dicho perfil.

Pasos

1. Selecciona **Configuración** > **Sistema** > **Erasure coding**.
2. Selecciona el perfil al que quieras cambiar el nombre.
3. Selecciona **Renombrar**.
4. Introduce un nombre único para el perfil de código de borrado.

   El nombre del perfil de código de borrado se añade al nombre del grupo de almacenamiento en la instrucción de ubicación de una regla de ILM.

   > Los nombres de los perfiles de código de borrado deben ser únicos. Se produce un error de validación si usas el nombre de un perfil existente, incluso si ese perfil ha sido desactivado.

5. Selecciona **Guardar**.

Desactivar un perfil de código de borrado

Puedes desactivar un perfil de código de borrado si ya no tienes previsto utilizarlo y si dicho perfil no se está utilizando actualmente en ninguna regla de ILM.

> Confirma que no haya ninguna operación de reparación de datos con código de borrado ni ningún procedimiento de descomisionado en curso. Se muestra un mensaje de error si intentas desactivar un perfil de codificación de borrado mientras cualquiera de estas operaciones está en curso.

Acerca de esta tarea

StorageGRID no te permite desactivar un perfil de código de borrado si se cumple alguna de las siguientes condiciones:

- El perfil de código de borrado se utiliza actualmente en una regla de ILM.
- El perfil de código de borrado ya no se utiliza en ninguna regla de ILM, pero los datos de los objetos y los fragmentos de paridad para el perfil siguen existiendo.

Pasos

1. Selecciona **Configuración** > **Sistema** > **Erasure coding**.
2. En la pestaña **Activo**, revisa la columna **Estado** para confirmar que el perfil de código de borrado que quieres desactivar no se usa en ninguna regla de ILM.

   No puedes desactivar un perfil de código de borrado si se usa en alguna regla de ILM. En el ejemplo, el perfil 2+1 Data Center 1 se usa en al menos una regla de ILM.

Profile name	Status	Storage pool	Erasure-coding scheme
2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
New profile	Deactivated	Data Center 1	2+1

3. Si el perfil se utiliza en una regla de ILM, sigue estos pasos:
   a. Selecciona **ILM** > **Reglas**.
   b. Selecciona cada regla y revisa el diagrama de retención para determinar si la regla utiliza el perfil de código de borrado que deseas desactivar.
   c. Si la regla de ILM utiliza el perfil de código de borrado que deseas desactivar, comprueba si la regla se usa en alguna política de ILM.
   d. Completa los pasos adicionales que aparecen en la tabla, según dónde se use el perfil de código de borrado.

¿Dónde se ha utilizado el perfil?	Pasos adicionales que hay que realizar antes de desactivar el perfil	Consulta estas instrucciones adicionales
Nunca se ha utilizado en ninguna regla de ILM	No es necesario realizar ningún paso adicional. Continúa con este procedimiento.	*Ninguno*
En una regla de ILM que nunca se ha usado en ninguna política de ILM	i. Modifica o elimina todas las reglas de ILM afectadas. Si modificas la regla, elimina todas las ubicaciones que utilicen el perfil de código de borrado. ii. Continúa con este procedimiento.	"Trabaja con reglas y políticas de ILM"
En una regla de ILM que está actualmente en una política de ILM activa	i. Clona la política. ii. Elimina la regla de ILM que utiliza el perfil de código de borrado. iii. Agrega una o más reglas ILM nuevas para asegurarte de que los objetos estén protegidos. iv. Guarda, simula y activa la nueva política. v. Espera a que se aplique la nueva política y a que los objetos existentes se trasladen a nuevas ubicaciones según las nuevas reglas que añadiste. **Nota:** Dependiendo del número de objetos y del tamaño de tu sistema StorageGRID, las operaciones de ILM podrían tardar semanas o incluso meses en trasladar los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Aunque puedes intentar desactivar sin problemas un perfil de código de borrado mientras siga asociado a datos, la operación de desactivación fallará. Un mensaje de error te informará si el perfil aún no está listo para ser desactivado. vi. Edita o elimina la regla que eliminaste de la política. Si editas la regla, elimina todas las ubicaciones que usan el perfil de código de borrado. vii. Continúa con este procedimiento.	"Crear una política de ILM" "Trabaja con reglas y políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales que hay que realizar antes de desactivar el perfil	Consulta estas instrucciones adicionales
En una regla de ILM que actualmente está en una política de ILM	i. Edita la política. ii. Elimina la regla de ILM que utiliza el perfil de código de borrado. iii. Agrega una o más reglas nuevas de ILM para asegurarte de que todos los objetos estén protegidos. iv. Guarda la directiva. v. Edita o elimina la regla que eliminaste de la política. Si editas la regla, elimina todas las ubicaciones que usan el perfil de código de borrado. vi. Continúa con este procedimiento.	"Crear una política de ILM" "Trabaja con reglas y políticas de ILM"

e. Actualiza la página «Perfiles de código de borrado» para asegurarte de que el perfil no se utilice en una regla de ILM.

4. Si el perfil no se utiliza en ninguna regla de ILM, selecciona el botón de opción y selecciona **Desactivar**. Aparece el cuadro de diálogo Desactivar perfil de código de borrado.

> Puedes seleccionar varios perfiles para desactivarlos al mismo tiempo, siempre y cuando cada perfil no se use en ninguna regla.

5. Si estás seguro de que quieres desactivar el perfil, selecciona **Desactivar**.

Resultados

- Si StorageGRID puede desactivar el perfil de erasure-coding, su estado es desactivado. Ya no puedes seleccionar este perfil para ninguna regla de ILM. No puedes volver a activar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparece un mensaje de error. Por ejemplo, aparece un mensaje de error si todavía hay datos de objetos asociados a este perfil. Es posible que tengas que esperar varias semanas antes de volver a intentar el proceso de desactivación.

Configura las regiones de S3 para StorageGRID

Las reglas de ILM permiten filtrar objetos en función de las regiones opcionales en las que se crean los buckets de S3, lo que te permite almacenar objetos de diferentes regiones en distintas ubicaciones de almacenamiento.

Si quieres utilizar la región de un bucket de S3 como filtro en una regla, primero debes crear las regiones que puedan utilizar los buckets de tu sistema.

> No puedes cambiar la región de un bucket después de que el bucket ha sido creado.

Antes de empezar

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

Acerca de esta tarea

Al crear un depósito de S3, puedes especificar que se cree en una región concreta. Especificar una región permite que el depósito esté geográficamente cerca de sus usuarios, lo que puede ayudar a optimizar la latencia, minimizar los costes y cumplir los requisitos normativos.

Cuando creas una regla de ILM, puede que quieras usar la región asociada con un bucket de S3 como filtro avanzado. Por ejemplo, puedes diseñar una regla que se aplique solo a los objetos en buckets de S3 creados en la región `us-west-2`. Luego puedes especificar que las copias de esos objetos se coloquen en Storage Nodes en un sitio de centro de datos dentro de esa región para optimizar la latencia.

A la hora de configurar las regiones, sigue estas directrices:

- Por defecto, se considera que todos los buckets pertenecen a la región `us-east-1`.
- Debes crear las regiones usando el Grid Manager antes de poder especificar una región no predeterminada al crear buckets con el Tenant Manager o la Tenant Management API, o con el elemento de solicitud LocationConstraint para las solicitudes S3 PUT Bucket API. Se produce un error si una solicitud PUT Bucket usa una región que no se ha definido en StorageGRID.
- Debes utilizar el nombre exacto de la región al crear el bucket de S3. Los nombres de las regiones distinguen mayúsculas de minúsculas. Los caracteres válidos son números, letras y guiones.

  > «EU» no se considera un alias de «eu-west-1». Si quieres utilizar la región «EU» o «eu-west-1», debes utilizar el nombre exacto.

- No puedes eliminar ni modificar una región si se utiliza en una regla asignada a cualquier política (activa o inactiva).
- Si utilizas una región no válida como filtro avanzado en una regla de ILM, no puedes añadir esa regla a una política.

  Puede producirse una región no válida si utilizas una región como filtro avanzado en una regla de ILM y luego eliminas esa región, o si usas la Grid Management API para crear una regla y especificas una región que aún no has definido.

- Si eliminas una región después de haberla utilizado para crear un bucket de S3, tendrás que volver a añadir la región si en algún momento quieres usar el filtro avanzado de Location Constraint para encontrar objetos en ese bucket.

Pasos

1. Selecciona **ILM** > **Regiones**.

   Aparece la página «Regiones».

2. Selecciona la pestaña **Todas las regiones** o **Región predeterminada**.

Todas las regiones

La pestaña **Todas las regiones** muestra las regiones definidas actualmente, incluida la región predeterminada.

> No puedes eliminar ni modificar la región predeterminada en la pestaña **Todas las regiones**. Usa la pestaña **Región predeterminada** para cambiar la región predeterminada.

a. Para añadir una región, selecciona **Add another region**.
b. Introduce el nombre de una región que quieres usar al crear buckets de S3.

   Debes utilizar este nombre exacto de la región como el elemento de solicitud LocationConstraint cuando crees el bucket de S3 correspondiente.

c. Para eliminar una región que no se utilice, selecciona el icono de eliminación ✕.

   Aparece un mensaje de error si intentas eliminar una región que se está utilizando actualmente en alguna política (activa o inactiva).

d. Cuando hayas terminado de realizar los cambios, selecciona **Guardar**.

   Ahora puedes seleccionar estas regiones en la sección «Filtros avanzados» del paso 1 del asistente para crear reglas de ILM. Consulta "Usa filtros avanzados en las reglas de ILM".

Región predeterminada

La pestaña **Región predeterminada** muestra la región predeterminada definida actualmente, que puedes modificar.

a. Para cambiar la región predeterminada, selecciona el nombre de la región entre las opciones disponibles en la lista desplegable **Región predeterminada**.
b. Selecciona **Guardar**.

Crear regla de ILM

Conoce las reglas ILM en StorageGRID

Para gestionar los objetos, creas un conjunto de reglas de gestión del ciclo de vida de la información (ILM) y las organizas en una política de ILM.

Cada objeto que se introduce en el sistema se evalúa en función de la política activa. Cuando una regla de la política coincide con los metadatos de un objeto, las instrucciones de la regla determinan qué acciones toma StorageGRID para copiar y almacenar ese objeto.

> Los metadatos de los objetos no se gestionan mediante reglas de ILM. En su lugar, los metadatos de los objetos se almacenan en una base de datos Cassandra en lo que se conoce como un almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proteger los datos de la pérdida.

Elementos de una regla ILM

Una regla de ILM consta de tres elementos:

- **Criterios de filtrado**: Los filtros básicos y avanzados de una regla definen a qué objetos se aplica dicha regla. Si un objeto cumple todos los filtros, StorageGRID aplica la regla y crea las copias del objeto especificadas en las instrucciones de ubicación de la regla.
- **Instrucciones de ubicación**: Las instrucciones de ubicación de una regla definen el número, el tipo y la ubicación de las copias de los objetos. Cada regla puede incluir una secuencia de instrucciones de ubicación para modificar el número, el tipo y la ubicación de las copias de los objetos a lo largo del tiempo. Cuando expira el periodo de tiempo de una ubicación, las instrucciones de la siguiente ubicación se aplican automáticamente en la siguiente evaluación de ILM.
- **Comportamiento de ingesta**: El comportamiento de ingesta de una regla te permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 guarda un objeto en el grid).

Filtrado de reglas ILM

Cuando creas una regla de ILM, especificas filtros para identificar a qué objetos se aplica la regla.

En el caso más sencillo, una regla podría no usar ningún filtro. Cualquier regla que no use filtros se aplica a todos los objetos, así que debe ser la última (por defecto) en una política de ILM. La regla por defecto proporciona instrucciones de almacenamiento para los objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos te permiten aplicar diferentes reglas a grupos grandes y diferenciados de objetos. Estos filtros te permiten aplicar una regla a cuentas de inquilino específicas, buckets de S3 específicos o ambos.

  Los filtros básicos te ofrecen una forma sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que los registros financieros de tu empresa deban almacenarse para cumplir con los requisitos normativos, mientras que los datos del departamento de marketing quizá deban almacenarse para facilitar las operaciones diarias. Tras crear cuentas de inquilino independientes para cada departamento o tras segregar los datos de los distintos departamentos en buckets de S3 separados, puedes crear fácilmente una regla que se aplique a todos los registros financieros y una segunda regla que se aplique a todos los datos de marketing.

- Los filtros avanzados te ofrecen un control muy preciso. Puedes crear filtros para seleccionar objetos en función de las siguientes propiedades de objeto:
  - Tiempo de ingesta
  - Último tiempo de acceso
  - Todo o parte del nombre del objeto (clave)
  - Restricción de ubicación (solo S3)
  - Tamaño del objeto
  - Metadatos del usuario
  - Etiqueta de objeto (solo S3)

Puedes filtrar los objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de diagnóstico por imagen de un hospital pueden utilizarse con frecuencia cuando tienen menos de 30 días de antigüedad y con poca frecuencia después, mientras que los objetos que contienen información sobre las visitas de los pacientes pueden necesitar copiarse al departamento de facturación en la sede central de la red sanitaria. Puedes crear filtros que identifiquen cada tipo de objeto según el nombre del objeto, el tamaño, las etiquetas de objetos S3 o cualquier otro criterio relevante, y luego crear reglas

independientes para almacenar cada conjunto de objetos de forma adecuada.

Puedes combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imagen grandes de manera diferente a los registros de sus proveedores, mientras que el departamento de Recursos Humanos podría necesitar almacenar los expedientes del personal en una ubicación geográfica específica y la información sobre políticas de forma centralizada. En este caso, puedes crear reglas que filtren por cuenta de inquilino para separar los registros de cada departamento, mientras usas filtros en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

Instrucciones para la colocación de reglas ILM

Las instrucciones de ubicación determinan dónde, cuándo y cómo se almacenan los datos de los objetos. Una regla ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de ubicación se aplica a un único periodo de tiempo.

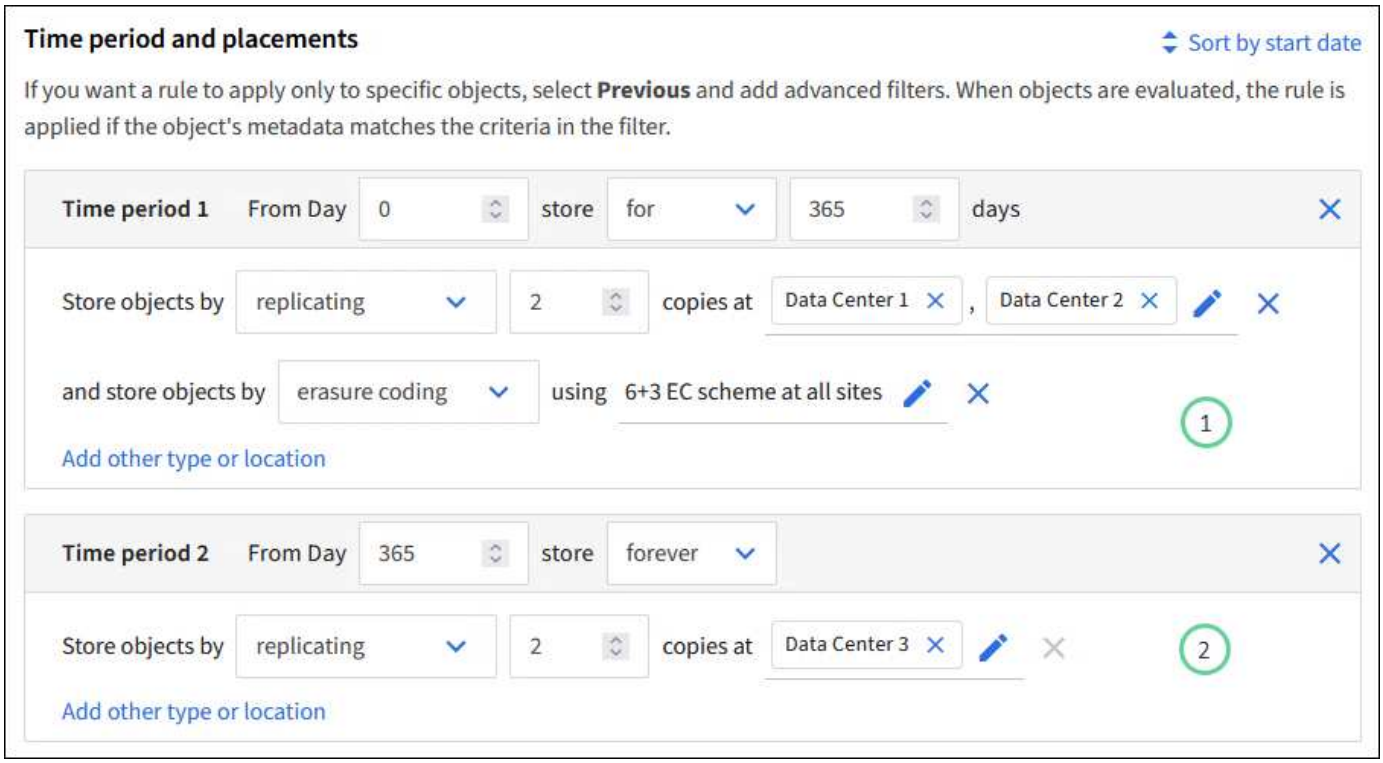
Al crear instrucciones de colocación:

- Lo primero que tienes que hacer es especificar la hora de referencia, que determina cuándo comienzan las instrucciones de ubicación. La hora de referencia puede ser el momento en que se ingresa un objeto, cuando se accede a él, cuando un objeto versionado deja de estar vigente o una hora definida por el usuario.
- A continuación, especificas cuándo se aplicará la ubicación, en relación con el momento de referencia. Por ejemplo, una ubicación podría comenzar el día 0 y continuar durante 365 días, en relación con el momento en que se incorporó el objeto.
- Por último, especificas el tipo de copias (replicación o código de borrado) y la ubicación donde se almacenan las copias. Por ejemplo, podrías querer almacenar dos copias replicadas en dos sitios diferentes.

Cada regla puede definir varias ubicaciones para un mismo periodo de tiempo y ubicaciones diferentes para distintos periodos de tiempo.

- Para situar objetos en varias ubicaciones durante un mismo periodo de tiempo, selecciona **Add other type or location** para añadir más de una línea para ese periodo.
- Para situar objetos en diferentes ubicaciones en distintos periodos de tiempo, selecciona **Add another time period** para añadir el siguiente periodo. Luego, especifica una o más líneas dentro de ese periodo.

El ejemplo muestra dos instrucciones de ubicación en la página Definir ubicaciones del asistente para crear reglas ILM.



La primera instrucción de asignación (1) tiene dos líneas para el primer año:

- La primera línea crea dos copias replicadas del objeto en dos centros de datos.
- La segunda línea crea una copia con código de borrado 6+3 utilizando todos los sitios del centro de datos.

La segunda instrucción de asignación (2) crea dos copias al cabo de un año y las conserva indefinidamente.

Al definir el conjunto de instrucciones de ubicación para una regla, debes asegurarte de que al menos una instrucción de ubicación comience en el día 0, que no haya huecos entre los periodos de tiempo que hayas definido y que la última instrucción de ubicación continúe indefinidamente o hasta que ya no necesites más copias de ningún objeto.

A medida que vence cada período de la regla, se aplican las instrucciones de ubicación de contenido para el siguiente período. Se crean nuevas copias del objeto y se eliminan las copias que no sean necesarias.

Comportamiento de ingesta según la regla ILM

El comportamiento de ingesta determina si las copias de los objetos se colocan inmediatamente según las instrucciones de la regla o si se crean copias provisionales y las instrucciones de colocación se aplican más tarde. Los siguientes comportamientos de ingesta están disponibles para las reglas de ILM:

- **Equilibrado**: StorageGRID intenta crear todas las copias especificadas en la regla ILM en el momento de la ingesta; si esto no es posible, se crean copias provisionales y se devuelve un mensaje de éxito al cliente. Las copias especificadas en la regla ILM se crean cuando es posible.
- **Estricta**: Todas las copias especificadas en la regla de ILM deben crearse antes de que se devuelva un mensaje de éxito al cliente.
- **Confirmación doble**: StorageGRID crea inmediatamente copias provisionales del objeto y devuelve éxito al cliente. Las copias especificadas en la regla ILM se crean cuando es posible.

Información relacionada

- "Opciones de ingesta"
- "Ventajas, desventajas y limitaciones de las opciones de ingesta"
- "Cómo interactúan la coherencia y las reglas de ILM para influir en la protección de datos"

Ejemplo de regla ILM

A modo de ejemplo, una regla de ILM podría especificar lo siguiente:

- Aplícalo únicamente a los objetos que pertenecen a Tenant A.
- Crea dos copias replicadas de esos objetos y almacena cada copia en una ubicación diferente.
- Conservar las dos copias «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que sean eliminados mediante una solicitud de eliminación del cliente o hasta que expire el ciclo de vida del bucket.
- Utiliza la opción Equilibrada para el comportamiento de ingesta: la instrucción de distribución en dos sitios se aplica en cuanto Tenant A guarda un objeto en StorageGRID, a menos que no sea posible crear inmediatamente ambas copias requeridas.

  Por ejemplo, si no se puede acceder al sitio 2 cuando el inquilino A guarda un objeto, StorageGRID creará dos copias provisionales en los nodos de almacenamiento del sitio 1. En cuanto el sitio 2 vuelva a estar disponible, StorageGRID creará la copia necesaria en ese sitio.

Información relacionada

- "¿Qué es un storage pool?"
- "¿Qué es un grupo de almacenamiento en la nube?"

Accede al asistente para crear una regla ILM en StorageGRID

Las reglas de ILM te permiten gestionar la ubicación de los datos de los objetos a lo largo del tiempo. Para crear una regla de ILM, usas el asistente Crear una regla de ILM.

> Si deseas crear la regla ILM predeterminada para una política, sigue la "Instrucciones para crear una regla ILM predeterminada" en su lugar.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Si quieres especificar a qué cuentas de inquilino se aplica esta regla, tienes la "Permisos de las cuentas de inquilinos" o sabes el ID de cada cuenta.
- Si quieres que la regla filtre los objetos según los metadatos del tiempo de acceso, debes habilitar las actualizaciones del tiempo de acceso en el bucket de S3.
- Ya has configurado los grupos de almacenamiento en la nube que tienes previsto utilizar. Consulta "Crear Cloud Storage Pool".
- Seguro que conoces el "opciones de ingesta".
- Si necesitas crear una regla que cumpla con los requisitos para su uso con S3 Object Lock, ya conoces el "Requisitos para S3 Object Lock".

- Opcionalmente, has visto el vídeo:

  Resumen de las reglas de ILM

Acerca de esta tarea

Al crear reglas de ILM:

- Ten en cuenta la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Piensa qué tipos de copias de objetos quieres crear (replicadas o con código de borrado) y el número de copias de cada objeto que se requieren.
- Determina qué tipos de metadatos de objetos se utilizan en las aplicaciones que se conectan al sistema StorageGRID. Las reglas de ILM filtran los objetos en función de sus metadatos.
- Piensa dónde quieres que se coloquen las copias de los objetos a lo largo del tiempo.
- Decide qué opción de ingesta quieres utilizar (Balanced, Strict o Dual commit).

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Selecciona **Crear**. "Paso 1 (Introducir datos)" de la pantalla del asistente para crear una regla de ILM aparece.

Ingresa detalles y filtros para una regla StorageGRID ILM

El paso **Introducir detalles** del asistente para crear una regla de ILM te permite introducir un nombre y una descripción para la regla y definir filtros para la regla.

Introducir una descripción y definir filtros para la regla es opcional.

Acerca de esta tarea

Al evaluar un objeto según una "Regla de ILM" regla, StorageGRID compara los metadatos del objeto con los filtros de la regla. Si los metadatos del objeto coinciden con todos los filtros, StorageGRID usa la regla para colocar el objeto. Puedes diseñar una regla para que se aplique a todos los objetos, o puedes especificar filtros básicos, como una o más cuentas de tenant o nombres de buckets, o filtros avanzados, como el tamaño del objeto o los metadatos de usuario.

Pasos

1. Introduce un nombre único para la regla en el campo **Nombre**.
2. Si lo deseas, introduce una breve descripción para la regla en el campo **Descripción**.

   Deberías describir el propósito o la función de la regla para que puedas reconocerla después.

3. Si lo deseas, selecciona una o más cuentas de inquilino de S3 a las que se aplique esta regla. Si esta regla se aplica a todos los inquilinos, deja este campo en blanco.

   Si no dispones ni del permiso de acceso Root ni del permiso de cuentas de Tenant, no puedes seleccionar tenants de la lista. En su lugar, introduce el tenant ID o varios IDs como una cadena separada por comas.

4. Si lo deseas, especifica los buckets de S3 a los que se aplica esta regla.

   Si se selecciona **aplica a todos los buckets** (predeterminado), la regla se aplica a todos los buckets de S3.

5. Para los inquilinos de S3, puedes seleccionar **Sí** para aplicar la regla solo a las versiones anteriores de los objetos en los buckets de S3 que tengan habilitado el versionado.

   Si seleccionas **Sí**, se seleccionará automáticamente «Hora no actual» como hora de referencia en "Paso 2 del asistente para crear una regla de ILM".

   > El tiempo no actual solo se aplica a los objetos S3 en buckets con control de versiones habilitado. Consulta "Operaciones en los buckets, PutBucketVersioning" y "Gestiona objetos con S3 Object Lock".

   Puedes usar esta opción para reducir el impacto en el almacenamiento de los objetos versionados filtrando las versiones de objetos no actuales. Consulta "Ejemplo 4: reglas y política de ILM para objetos versionados de S3".

6. Si lo deseas, selecciona **Add an advanced filter** para especificar filtros adicionales.

   Si no configuras el filtrado avanzado, la regla se aplica a todos los objetos que coincidan con los filtros básicos. Para obtener más información sobre el filtrado avanzado, consulta Usa filtros avanzados en las reglas de ILM y Especifica varios tipos y valores de metadatos.

7. Selecciona **Continuar**. "Paso 2 (Definir ubicaciones)" de la pantalla del asistente para crear una regla ILM aparece.

Usa filtros avanzados en las reglas de ILM

El filtrado avanzado te permite crear reglas de ILM que se aplican únicamente a objetos específicos en función de sus metadatos. Al configurar el filtrado avanzado para una regla, seleccionas el tipo de metadatos con el que quieres hacer la coincidencia, eliges un operador y especificas un valor de metadatos. Cuando se evalúan los objetos, la regla de ILM se aplica solo a aquellos objetos que tienen metadatos que coinciden con el filtro avanzado.

La tabla muestra los tipos de metadatos que puedes especificar en los filtros avanzados, los operadores que puedes usar para cada tipo de metadatos y los valores de metadatos esperados.

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Tiempo de ingesta	• es • no es • es antes de • es en o antes de • es después de • es a partir de	Fecha y hora en que se ingirió el objeto. **Nota:** Para evitar problemas con los recursos al activar una nueva política de ILM, puedes utilizar el filtro avanzado «Hora de ingesta» en cualquier regla que pueda modificar la ubicación de un gran número de objetos existentes. Establece la «Hora de ingesta» en un valor mayor o igual a la hora aproximada en la que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Clave	• es igual a • no es igual a • contiene • no contiene • comienza con • no empieza por • termina con • no termina con	Todo o parte de la clave única de un objeto S3. Por ejemplo, quizá quieras buscar objetos que terminen con `.txt` o que empiecen con `test-object/`.
Último tiempo de acceso	• es • no es • es antes de • es en o antes de • es después de • es a partir de	Fecha y hora de la última vez que se recuperó (leyó o visualizó) el objeto. **Nota:** Si tienes pensado usar "usar el tiempo de acceso más reciente" como filtro avanzado, debes habilitar las actualizaciones del tiempo de acceso más reciente para el bucket de S3.
Restricción de ubicación (solo S3)	• es igual a • no es igual a	La región en la que se creó un bucket de S3. Utiliza **ILM** > **Regiones** para definir las regiones que se muestran. **Nota:** El valor «us-east-1» coincidirá con los objetos de los buckets creados en la región us-east-1, así como con los objetos de los buckets que no tengan especificada ninguna región. Consulta "Configurar regiones de S3".
Tamaño del objeto	• es igual a • no es igual a • menos de • menor o igual que • mayor que • mayor o igual que	El tamaño del objeto. El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

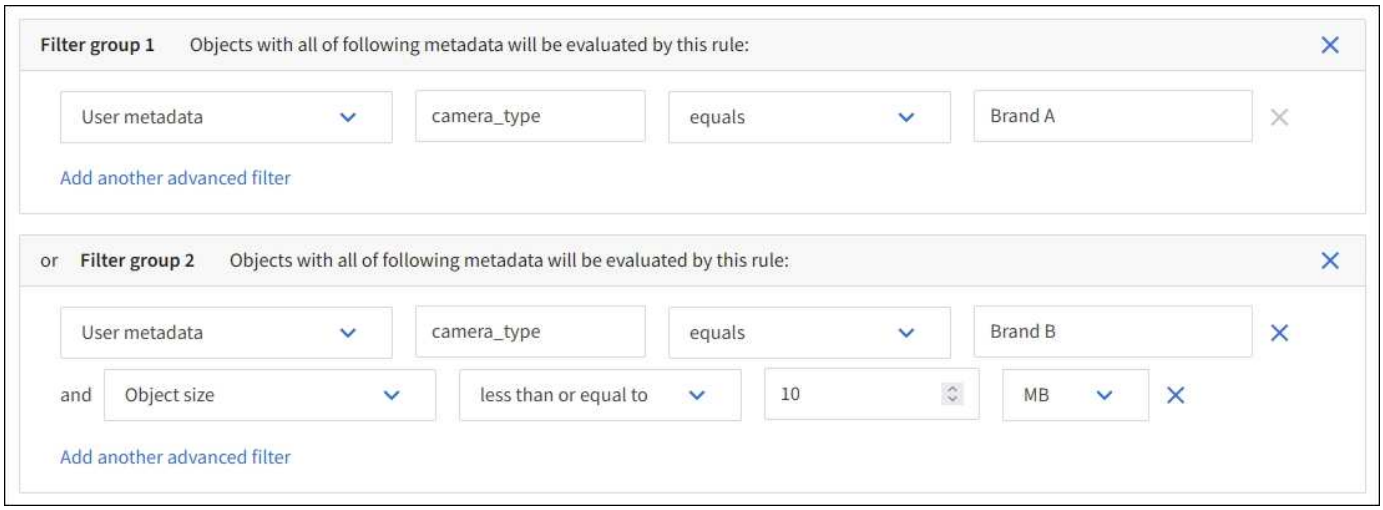
Tipo de metadatos	Operadores compatibles	Valor de metadatos
Metadatos del usuario	• contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual a • no existe • no empieza por	Par clave-valor, donde **User metadata name** es la clave y **Metadata value** es el valor. Por ejemplo, para filtrar objetos que tengan metadatos de usuario `color=blue`, especifica `color` para **User metadata name**, `equals` para el operador y `blue` para **Metadata value**. **Nota:** Los nombres de los metadatos de usuario no distinguen mayúsculas de minúsculas; los valores de los metadatos de usuario sí distinguen mayúsculas de minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual a • no existe • no empieza por	Par clave-valor, donde **Object tag name** es la clave y **Object tag value** es el valor. Por ejemplo, para filtrar objetos que tengan una etiqueta de objeto de `Image=True`, especifica `Image` para **Nombre de la etiqueta de objeto**, `equals` para el operador y `True` para **Valor de la etiqueta de objeto**. **Nota:** Los nombres y valores de las etiquetas de los objetos distinguen mayúsculas de minúsculas. Debes introducir estos elementos exactamente tal y como se definieron para el objeto.

Especifica varios tipos y valores de metadatos

Al definir un filtrado avanzado, puedes especificar varios tipos de metadatos y varios valores de metadatos. Por ejemplo, si quieres que una regla coincida con objetos entre 10 MB y 100 MB de tamaño, debes seleccionar el tipo de metadatos **Object size** y especificar dos valores de metadatos.

- El primer valor de metadatos especifica los objetos mayores o iguales a 10 MB.
- El segundo valor de metadatos especifica los objetos de un tamaño igual o menor a 100 MB.

El uso de entradas múltiples te permite controlar con precisión qué objetos se seleccionan. En el siguiente ejemplo, la regla se aplica a los objetos que tienen Brand A o Brand B como valor del metadato de usuario camera_type. Sin embargo, la regla solo se aplica a aquellos objetos Brand B que sean menores de 10 MB.



Define instrucciones de colocación para una regla de StorageGRID ILM

El paso **Definir ubicaciones** del asistente para crear reglas de ILM te permite definir las instrucciones de ubicación que determinan cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y el número de copias.

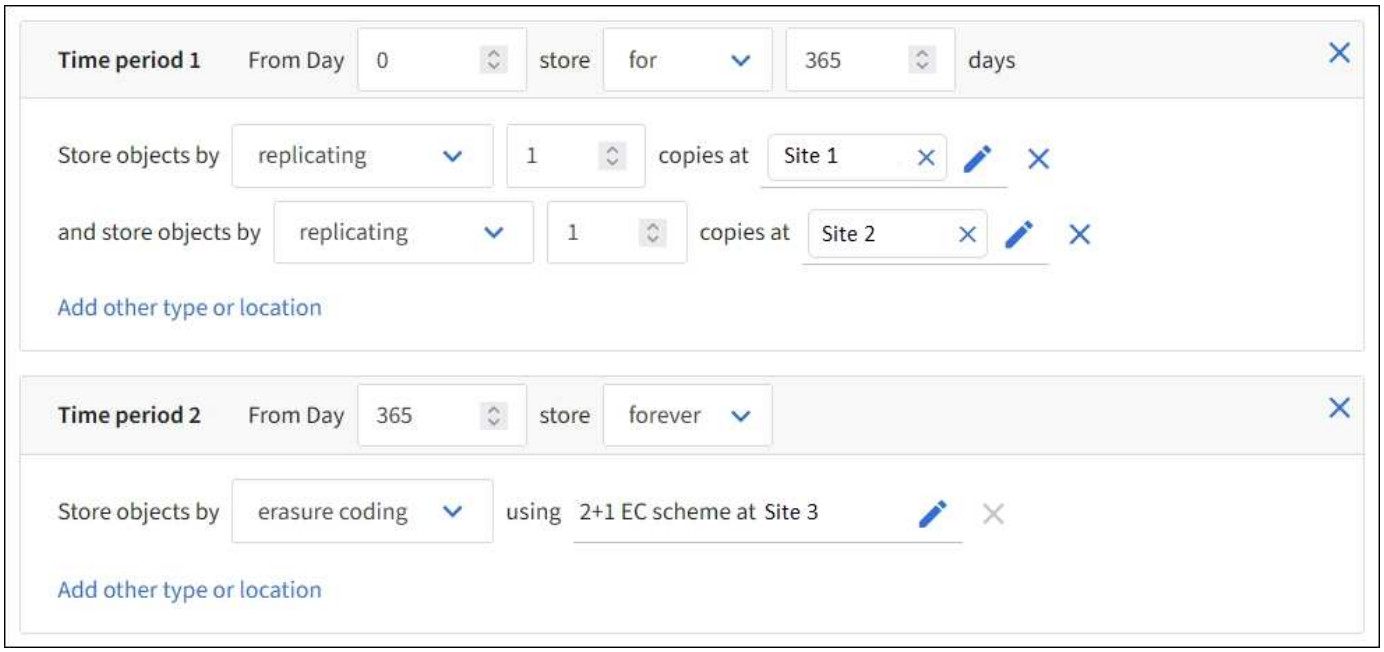
> Las capturas de pantalla que se muestran son ejemplos. Tus resultados pueden variar en función de tu versión de StorageGRID.

Acerca de esta tarea

Una regla ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de ubicación se aplica a un único periodo de tiempo. Cuando usas más de una instrucción, los periodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar en el día 0. Las instrucciones pueden continuar para siempre o hasta que ya no necesites copias de ningún objeto.

Cada instrucción de colocación puede constar de varias líneas si deseas crear diferentes tipos de copias o usar diferentes ubicaciones durante ese periodo de tiempo.

En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y otra en el sitio 2 durante el primer año. Después de un año, se crea una copia con código de borrado 2+1 y se guarda únicamente en un sitio.



Pasos

1. Para **Hora de referencia**, selecciona el tipo de hora que quieres usar al calcular la hora de inicio de una instrucción de asignación.

Opción	Descripción
Tiempo de ingesta	El momento en que se ingirió el objeto.
Último tiempo de acceso	El momento en que se recuperó (leyó o visualizó) el objeto por última vez. Para utilizar esta opción, deben estar habilitadas las actualizaciones del tiempo de acceso para el bucket de S3. Consulta "Usa el tiempo de acceso en las reglas de ILM".
Hora de creación definida por el usuario	Una hora especificada en los metadatos definidos por el usuario.
Tiempo no corriente	La opción «Tiempo no actual» se selecciona automáticamente si seleccionaste **Sí** en la pregunta «¿Aplicar esta regla solo a versiones antiguas de objetos (en S3 buckets con versioning habilitado)?» en "Paso 1 del asistente para crear una regla de ILM".

   Si quieres crear una regla *conforme*, debes seleccionar **Hora de ingesta**. Consulta "Gestiona objetos con S3 Object Lock".

2. En la sección **Periodo de tiempo y asignaciones**, introduce una hora de inicio y una duración para el primer periodo de tiempo.

   Por ejemplo, es posible que quieras especificar dónde almacenar los objetos durante el primer año (*A partir del día 0, almacénalos durante 365 días*). Al menos una instrucción debe comenzar en el día 0.

3. Si quieres crear copias replicadas:
   a. En la lista desplegable **Almacenar objetos por**, selecciona **replicando**.
   b. Selecciona el número de copias que deseas hacer.

      Aparece una advertencia si cambias el número de copias a 1. Una regla de ILM que crea solo una copia replicada para cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Consulta "Por qué no debes utilizar la replicación de copia única".

      Para evitar el riesgo, haz una o más de las siguientes acciones:

      - Aumenta el número de copias para el periodo de tiempo.
      - Agrega copias a otros pools de almacenamiento o a un Cloud Storage Pool.
      - Selecciona **código de borrado** en lugar de **replicación**.

        Puedes ignorar esta advertencia sin problema si esta regla ya crea varias copias para todos los periodos.

   c. En el campo **copias en**, selecciona los grupos de almacenamiento que quieras añadir.

      Si solo especificas un grupo de almacenamiento, ten en cuenta que StorageGRID solo puede almacenar una copia replicada de un objeto en cada nodo de almacenamiento. Si tu grid incluye tres nodos de almacenamiento y seleccionas 4 como número de copias, solo se crearán tres copias—una copia por cada nodo de almacenamiento.

      Se activa la alerta **ILM placement unachievable** para indicar que no se ha podido aplicar completamente la regla de ILM.

      Si especificas más de un grupo de almacenamiento, ten en cuenta las siguientes reglas:

      - El número de copias no puede ser mayor que el número de grupos de almacenamiento.
      - Si el número de copias es igual al número de grupos de almacenamiento, se almacena una copia del objeto en cada grupo de almacenamiento.
      - Si el número de copias es inferior al número de grupos de almacenamiento, se almacena una copia en el sitio de ingesta y luego el sistema distribuye las copias restantes para mantener equilibrado el uso del disco entre los grupos de almacenamiento, asegurando que ningún sitio reciba más de una copia de un objeto.
      - Si los grupos de almacenamiento se solapan (contienen los mismos Storage Nodes), es posible que todas las copias del objeto se guarden únicamente en un sitio. Por este motivo, no especifiques el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) junto con otro grupo de almacenamiento.
4. Si quieres crear una copia con código de borrado:
   a. En la lista desplegable **Almacenar objetos por**, selecciona **código de borrado**.

      > El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

   b. Si no has añadido un filtro de «Tamaño del objeto» para un valor superior a 200 KB, selecciona **Anterior** para volver al paso 1. Luego, selecciona **Añadir un filtro avanzado** y configura un filtro de «Tamaño del objeto» con cualquier valor superior a 200 KB.

c. Selecciona el grupo de almacenamiento que quieras añadir y el esquema de código de borrado que quieras utilizar.

   La ubicación de almacenamiento de una copia con código de borrado incluye el nombre del esquema de código de borrado, seguido del nombre del grupo de almacenamiento.

Los esquemas de código de borrado disponibles están limitados por el número de nodos de almacenamiento del grupo de almacenamiento que selecciones. Aparece una insignia de `Recommended` junto a los esquemas que ofrecen ya sea el "la mejor protección o la menor sobrecarga de almacenamiento".

5. Opcionalmente:
   a. Selecciona **Add other type or location** para crear copias adicionales en distintas ubicaciones.
   b. Selecciona **Add another time period** para añadir diferentes periodos.

> ⓘ La eliminación de objetos se realiza según los siguientes ajustes:
>
> - Los objetos se eliminan automáticamente al finalizar el último periodo de tiempo, a menos que otro periodo de tiempo termine con **forever**.
> - Según "Configuración del periodo de retención de buckets y de inquilinos", es posible que los objetos no se eliminen aunque finalice el periodo de retención de ILM.

6. Si quieres almacenar objetos en un grupo de almacenamiento en la nube:
   a. En la lista desplegable **Almacenar objetos por**, selecciona **replicating**.
   b. Selecciona el campo **copias en**, luego selecciona un Cloud Storage Pool.

      Cuando uses Cloud Storage Pools, ten en cuenta estas reglas:

      - No puedes seleccionar más de un Cloud Storage Pool en una sola instrucción de ubicación. Del mismo modo, no puedes seleccionar un Cloud Storage Pool y un storage pool en la misma instrucción de ubicación.
      - Solo puedes almacenar una sola copia de un objeto en cualquier Cloud Storage Pool. Aparece un mensaje de error si configuras **Copias** en 2 o más.
      - No puedes almacenar más de una copia de un objeto en cualquier Cloud Storage Pool al mismo tiempo. Aparece un mensaje de error si varias ubicaciones que usan un Cloud Storage Pool tienen fechas que se solapan o si varias líneas de la misma ubicación usan un Cloud Storage Pool.
      - Puedes almacenar un objeto en un Cloud Storage Pool al mismo tiempo que dicho objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debes incluir más de una línea en la instrucción de ubicación para ese periodo de tiempo, de modo que puedas especificar el número y los tipos de copias para cada ubicación.

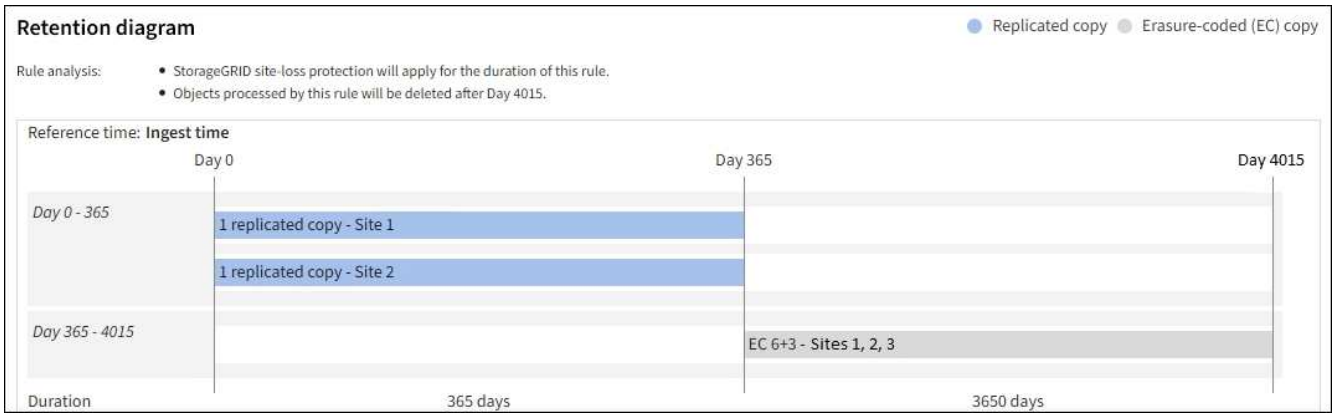
7. En el diagrama de retención, comprueba tus instrucciones de colocación.

   En este ejemplo, la regla de ILM almacena una copia replicada en el Site 1 y otra copia replicada en el Site 2 durante el primer año. Después de un año y durante 10 años adicionales, se guardará una copia con código de borrado 6+3 en tres sites. Después de 11 años en total, los objetos se eliminarán de StorageGRID.

   La sección de análisis de reglas del diagrama de retención dice:

- La protección contra la pérdida de un sitio de StorageGRID se aplicará mientras esté vigente esta regla.
- Los objetos procesados por esta regla se eliminarán después del día 4015.

  Consulta "Activa la protección contra la pérdida del sitio."



8. Selecciona **Continuar**. "Paso 3 (Selecciona el comportamiento de ingesta)" del asistente para crear una regla ILM aparece.

Usa el tiempo de último acceso en las reglas ILM de StorageGRID

Puedes usar el tiempo de acceso como la hora de referencia en una regla de ILM. Por ejemplo, podrías querer dejar los objetos que se han visto en los últimos tres meses en los nodos de almacenamiento locales, mientras que los objetos que no se han visto recientemente se muevan a una ubicación externa. También puedes usar el tiempo de acceso como un filtro avanzado si quieres que una regla de ILM se aplique solo a los objetos a los que se accedió por última vez en una fecha específica.

Acerca de esta tarea

Antes de utilizar el tiempo de acceso en una regla de ILM, ten en cuenta las siguientes consideraciones:

- Cuando uses el tiempo de acceso como fecha de referencia, ten en cuenta que cambiar el tiempo de acceso de un objeto no activa una evaluación inmediata de ILM. En su lugar, se evalúan las ubicaciones del objeto y este se mueve según sea necesario cuando ILM en segundo plano evalúa el objeto. Esto podría tardar dos semanas o más después de que se accede al objeto.

  Ten en cuenta esta latencia al crear reglas de ILM basadas en el tiempo de acceso y evita las ubicaciones que utilicen periodos de tiempo cortos (menos de un mes).

- Si utilizas el tiempo de acceso más reciente como filtro avanzado o como hora de referencia, debes habilitar las actualizaciones del tiempo de acceso más reciente para los buckets de S3. Puedes usar el "Administrador de inquilinos" o el "API de gestión de inquilinos".

  > ⓘ Las actualizaciones del tiempo de acceso están desactivadas por defecto para los buckets de S3.

Ten en cuenta que habilitar las actualizaciones del tiempo de acceso puede reducir el rendimiento, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento ocurre porque StorageGRID debe actualizar los objetos con nuevas marcas de tiempo cada vez que se recuperan.

La siguiente tabla resume si el tiempo de acceso se actualiza para todos los objetos del bucket según los distintos tipos de solicitudes.

Tipo de solicitud	Si se actualiza el tiempo de acceso más reciente cuando las actualizaciones del tiempo de acceso están desactivadas	Si el tiempo de acceso más reciente se actualiza cuando están activadas las actualizaciones del tiempo de acceso más reciente
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí
Solicitud para copiar un objeto de un bucket a otro	• No, para la copia original • Sí, para la copia de destino	• Sí, para la copia original • Sí, para la copia de destino
Solicitud para completar una subida en varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Selecciona el comportamiento de ingesta para una regla StorageGRID ILM

El paso **Seleccionar comportamiento de incorporación** del asistente para crear reglas de ILM te permite elegir cómo se protegen los objetos filtrados por esta regla en el momento de su incorporación.

Acerca de esta tarea

StorageGRID puede crear copias provisionales y poner los objetos en cola para su posterior evaluación según el ILM, o puede crear copias de inmediato para cumplir con las instrucciones de ubicación de la regla.

Pasos

1. Selecciona el "comportamiento de ingesta" que quieres usar.

   Para más información, consulta "Ventajas, desventajas y limitaciones de las opciones de ingesta".

No puedes utilizar la opción «Equilibrada» o «Estricta» si la regla utiliza una de estas ubicaciones:

- Un Cloud Storage Pool desde el día 0
- Un Cloud Storage Pool cuando la regla utiliza una hora de creación definida por el usuario como hora de referencia

Consulta "Ejemplo 5: normas y política de ILM para un comportamiento de ingesta estricto".

2. Selecciona **Crear**.

   Se ha creado la regla ILM. La regla no se activa hasta que se añade a una "Política de ILM" y esa política se activa.

   Para ver los detalles de la regla, selecciona el nombre de la regla en la página de reglas de ILM.

Crea una regla ILM predeterminada en StorageGRID

Antes de crear una política de ILM, debes crear una regla predeterminada para incluir en la política cualquier objeto que no se ajuste a otra regla. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los buckets y todas las versiones de los objetos.

Antes de empezar

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

Acerca de esta tarea

La regla predeterminada es la última regla que se evalúa en una política de ILM, por lo que no puede usar ningún filtro. Las instrucciones de ubicación de la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla de la política.

En esta política de ejemplo, la primera regla se aplica únicamente a los objetos que pertenecen a test-tenant-1. La regla predeterminada, que es la última, se aplica a los objetos que pertenecen a todas las demás cuentas de tenant.

Al crear la regla predeterminada, ten en cuenta estos requisitos:

- La regla predeterminada se colocará automáticamente como la última regla cuando la añadas a una política.
- La regla predeterminada no puede utilizar ningún filtro básico ni avanzado.
- La regla por defecto debe aplicarse a todas las versiones de los objetos.
- La regla predeterminada debería crear copias replicadas.

> No utilices una regla que cree copias con código de borrado como regla predeterminada de una política. Las reglas de código de borrado deben usar un filtro avanzado para evitar que los objetos más pequeños se codifiquen con código de borrado.

- En general, la regla por defecto debería conservar los objetos para siempre.
- Si estás utilizando (o tienes previsto activar) la configuración global de S3 Object Lock, la regla predeterminada debe ser compatible.

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Selecciona **Crear**.

   Aparece el paso 1 (Introducir datos) del asistente para crear una regla de ILM.

3. Introduce un nombre único para la regla en el campo **Nombre de la regla**.
4. Si lo deseas, introduce una breve descripción para la regla en el campo **Descripción**.
5. Deja en blanco el campo **Tenant accounts**.

   La regla predeterminada debe aplicarse a todas las cuentas de inquilino.

6. Deja el menú desplegable «Nombre del bucket» en la opción **se aplica a todos los buckets**.

   La regla predeterminada debe aplicarse a todos los buckets de S3.

7. Mantén la respuesta predeterminada, **No**, para la pregunta, «¿Aplicar esta regla solo a las versiones anteriores de los objetos (en buckets de S3 con control de versiones activado)?»
8. No añadas filtros avanzados.

   La regla predeterminada no puede especificar ningún filtro.

9. Selecciona **Siguiente**.

   Aparece el paso 2 (Definir ubicaciones).

10. Para Hora de referencia, selecciona cualquier opción.

    Si has mantenido la respuesta predeterminada, **No**, para la pregunta «¿Aplicar esta regla solo a las versiones anteriores del objeto?» La hora no actual no aparecerá en la lista desplegable. La regla predeterminada debe aplicarse a todas las versiones del objeto.

11. Especifica las instrucciones de ubicación para la regla predeterminada.
    - La regla predeterminada debe conservar los objetos indefinidamente. Aparece una advertencia cuando activas una nueva política si la regla predeterminada no conserva los objetos indefinidamente. Debes confirmar que este es el comportamiento que esperas.
    - La regla predeterminada debería crear copias replicadas.

      > No utilices una regla que cree copias con código de borrado como regla predeterminada de una política. Las reglas de código de borrado deben incluir el filtro avanzado **Tamaño del objeto (MB) superior a 200 KB** para evitar que los objetos más pequeños se codifiquen con código de borrado.

    - Si estás utilizando (o tienes previsto activar) la configuración global de S3 Object Lock, la regla predeterminada debe ser compatible:
      - Debe crear al menos dos copias replicadas de objetos o una copia con código de borrado.
      - Estas copias deben existir en los nodos de almacenamiento durante toda la duración de cada línea en las instrucciones de ubicación.
      - Las copias de objetos no se pueden guardar en un Cloud Storage Pool.
      - Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando la hora de ingesta como referencia.
      - Al menos una de las instrucciones de colocación debe ser "para siempre".
12. Consulta el diagrama de retención para confirmar las instrucciones de colocación.
13. Selecciona **Continuar**.

    Aparece el paso 3 (Select ingest behavior).

14. Selecciona la opción de ingestión que quieres usar y selecciona **Crear**.

Gestiona las políticas de ILM

Conoce las políticas ILM en StorageGRID

Una política de gestión del ciclo de vida de la información (ILM) es un conjunto ordenado de reglas de ILM que determina cómo el sistema StorageGRID gestiona los datos de objetos a lo largo del tiempo.

> Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irrecuperable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Política predeterminada de ILM

Al instalar StorageGRID y añadir sitios, se crea automáticamente una política de ILM predeterminada, como sigue:

- Si tu grid contiene un único sitio, la política predeterminada incluye una regla predeterminada que replica dos copias de cada objeto en ese sitio.
- Si tu grid contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

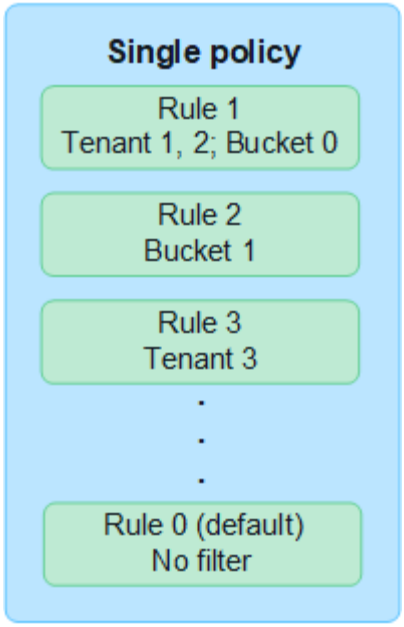
Si la política predeterminada no cumple con los requisitos de almacenamiento, puedes crear tus propias reglas y políticas. Consulta "Crear una regla de ILM" y "Crear una política de ILM".

¿Una o varias políticas de ILM activas?

Puedes tener una o varias políticas de ILM activas a la vez.

Una política

Si tu grid va a utilizar un esquema sencillo de protección de datos con pocas reglas específicas para cada tenant y cada bucket, utiliza una única política de ILM activa. Las reglas de ILM pueden incluir filtros para gestionar diferentes buckets o tenants.



Cuando solo tienes una política y cambian los requisitos de un inquilino, debes crear una nueva política de ILM o clonar la política existente para aplicar los cambios, simular y luego activar la nueva política de ILM. Los cambios en la política de ILM podrían provocar movimientos de objetos que podrían durar varios días y causar latencia en el sistema.

Varias políticas

Para ofrecer diferentes opciones de calidad de servicio a los inquilinos, puedes tener más de una política activa a la vez. Cada política puede gestionar inquilinos, buckets de S3 y objetos específicos. Cuando aplicas o modificas una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

Etiquetas de políticas de ILM

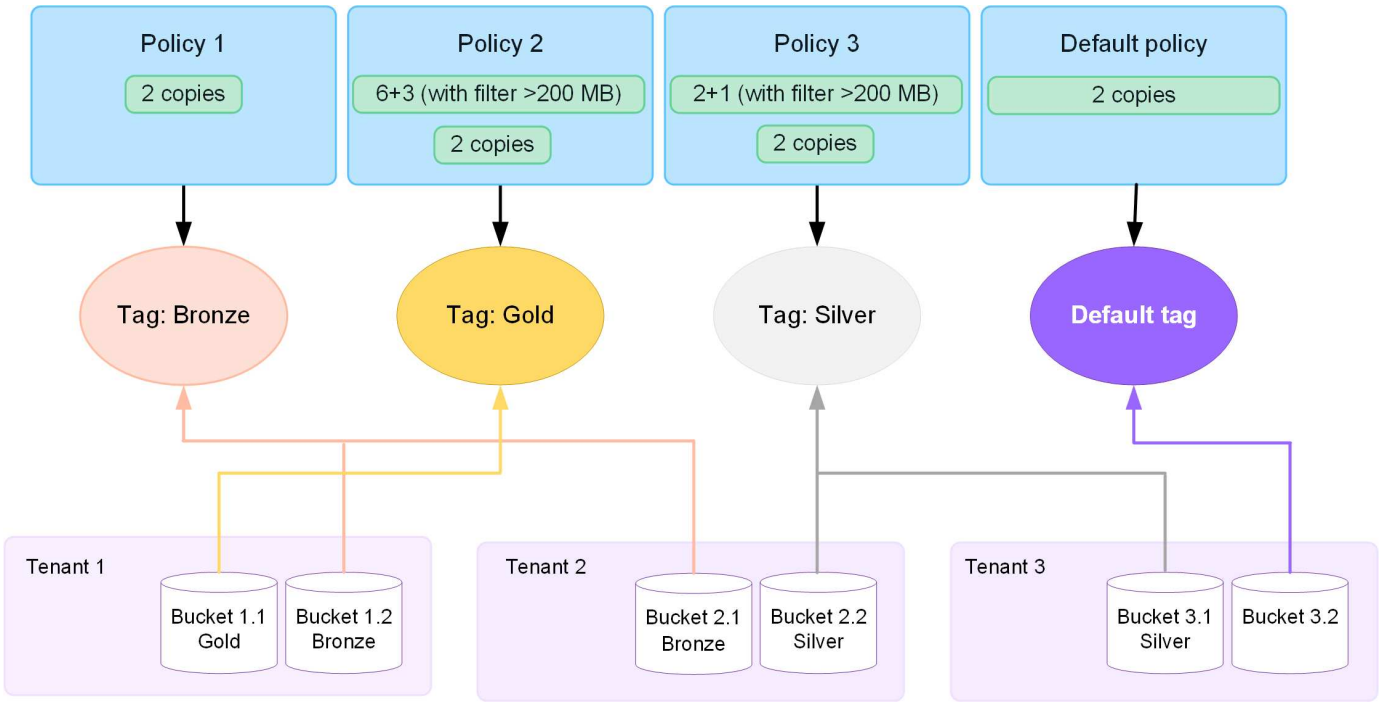
Si deseas permitir que los clientes cambien fácilmente entre varias políticas de protección de datos para cada bucket, utiliza varias políticas de ILM con *etiquetas de política de ILM*. Asignas cada política de ILM a una etiqueta, luego los clientes etiquetan un bucket para aplicar la política a ese bucket. Solo puedes configurar etiquetas de política de ILM en buckets de S3.

Por ejemplo, podrías tener tres etiquetas llamadas Gold, Silver y Bronze. Puedes asignar una política de ILM a cada etiqueta, según cuánto tiempo y dónde esa política almacene los objetos. Los tenants pueden elegir qué política usar etiquetando sus buckets. Un bucket etiquetado como Gold se gestiona mediante la política Gold y recibe el nivel Gold de protección de datos y rendimiento.

Puedes "crear un máximo de 10 etiquetas de política" para tu grid.

Etiqueta de política ILM predeterminada

Al instalar StorageGRID, se crea automáticamente una etiqueta de política ILM predeterminada. Cada grid debe tener una política activa asignada a la etiqueta Default. La política predeterminada se aplica a cualquier bucket de S3 sin etiqueta.



¿Cómo evalúa una política de ILM los objetos?

Una política de ILM activa controla la ubicación, la duración y la protección de datos de los objetos.

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan según el conjunto ordenado de reglas de ILM de la política, de la siguiente manera:

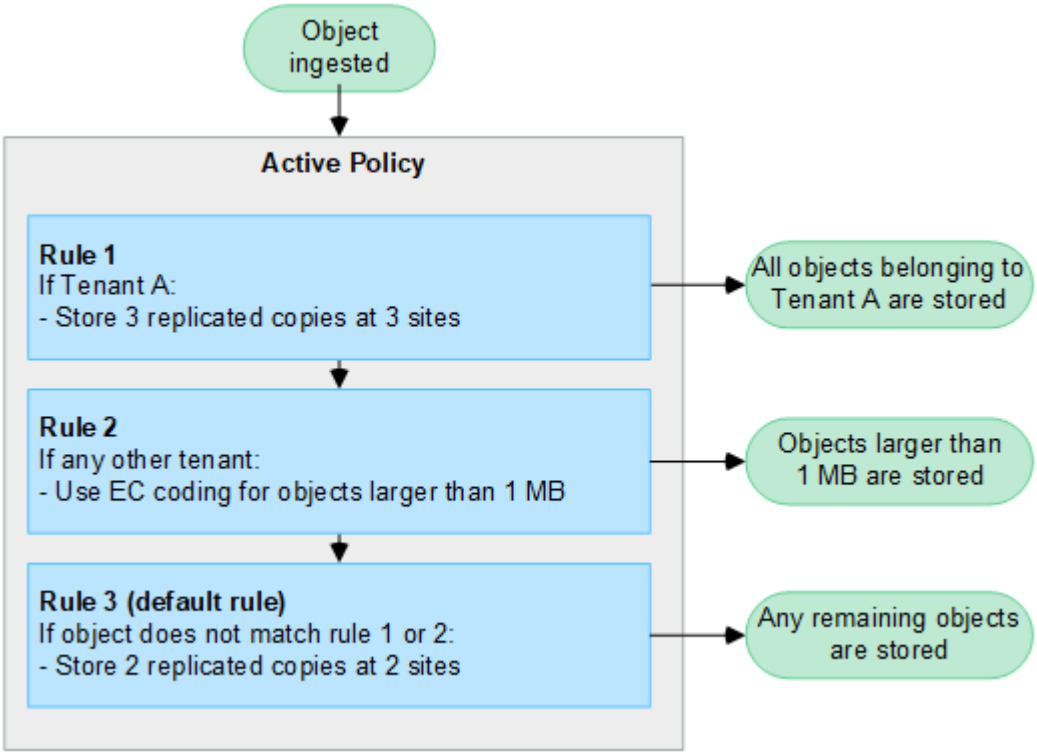
1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se incorpora según el comportamiento de incorporación de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa con cada una de las reglas siguientes de la política hasta que se encuentre una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican el comportamiento de ingesta y las instrucciones de ubicación de la regla predeterminada de la política. La regla predeterminada es la última regla de una política. La regla predeterminada debe aplicarse a todos los tenants, todos los buckets de S3 y todas las versiones de los objetos, y no puede usar ningún filtro avanzado.

Ejemplo de política de ILM

A modo de ejemplo, una política de ILM podría contener tres reglas de ILM que especifiquen lo siguiente:

- **Regla 1: Copias replicadas para Tenant A**
  - Selecciona todos los objetos que pertenezcan a Tenant A.
  - Almacena estos objetos como tres copias replicadas en tres ubicaciones.
  - Los objetos que pertenecen a otros inquilinos no se ajustan a la Regla 1, así que se evalúan según la Regla 2.
- **Regla 2: código de borrado para objetos de más de 1 MB**
  - Selecciona todos los objetos de otros tenants, pero solo si superan 1 MB. Estos objetos de mayor tamaño se almacenan utilizando erasure coding 6+3 en tres sitios.

    - No coincide con los objetos de 1 MB o menos, así que estos objetos se evalúan según la Regla 3.
- **Regla 3: 2 copias 2 centros de datos** (por defecto)
    - Es la última y predeterminada regla de la política. No utiliza filtros.
    - Crea dos copias replicadas de todos los objetos que no se ajusten a la Regla 1 ni a la Regla 2 (objetos que no pertenezcan a Tenant A y que tengan un tamaño igual o inferior a 1 MB).



¿Qué son las políticas activas e inactivas?

Cada sistema StorageGRID debe tener al menos una política de ILM activa. Si quieres tener más de una política de ILM activa, creas etiquetas de política de ILM y asignas una política a cada etiqueta. Luego, los inquilinos aplican etiquetas a los buckets de S3. La política predeterminada se aplica a todos los objetos en los buckets que no tienen una etiqueta de política asignada.

Cuando creas una política de ILM por primera vez, seleccionas una o varias reglas de ILM y las ordenas en un orden específico. Después de simular la política para confirmar su comportamiento, la activas.

Al activar una política de ILM, StorageGRID utiliza dicha política para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Es posible que los objetos existentes se trasladen a nuevas ubicaciones cuando se apliquen las reglas de ILM de la nueva política.

Si activas más de una política de ILM a la vez y los inquilinos aplican etiquetas de política a los buckets de S3, los objetos de cada bucket se gestionan según la política asignada a la etiqueta.

Un sistema StorageGRID realiza un seguimiento del historial de las políticas que se han activado o desactivado.

Aspectos a tener en cuenta a la hora de crear una política de ILM

- Utiliza únicamente la política proporcionada por el sistema, Baseline 2 copies policy, en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla Make 2 Copies en esta política utiliza el

grupo de almacenamiento All Storage Nodes, que contiene todos los sitios. Si tu sistema StorageGRID tiene más de un sitio, dos copias de un objeto podrían colocarse en el mismo sitio.

> El grupo de almacenamiento All Storage Nodes se crea automáticamente durante la instalación de StorageGRID 11.6 y versiones anteriores. Si actualizas a una versión posterior de StorageGRID, el grupo All Storage Nodes seguirá existiendo. Si instalas StorageGRID 11.7 o una versión posterior como nueva instalación, no se crea el grupo All Storage Nodes.

- Al diseñar una nueva política, ten en cuenta todos los diferentes tipos de objetos que podrían incorporarse a tu grid. Asegúrate de que la política incluya reglas para identificar y ubicar estos objetos según sea necesario.
- Mantén la política de ILM lo más sencilla posible. De este modo se evitan situaciones potencialmente peligrosas en las que los datos de los objetos no estén protegidos como se pretende cuando se realicen cambios en el sistema StorageGRID con el paso del tiempo.
- Asegúrate de que las reglas de la política estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan según las reglas en el orden en que aparecen, empezando por la primera. Por ejemplo, si la primera regla de una política coincide con un objeto, ese objeto no será evaluado por ninguna otra regla.
- La última regla de cada política de ILM es la regla predeterminada de ILM, que no puede utilizar ningún filtro. Si un objeto no ha sido coincidido por otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se retiene.
- Antes de activar una nueva política, revisa cualquier cambio que la política haga en la ubicación de los objetos existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales con los recursos cuando se evalúen y apliquen las nuevas ubicaciones.

Crea políticas ILM en StorageGRID

Crea una o varias políticas de ILM para cumplir con tus requisitos de calidad de servicio.

Contar con una política de ILM activa te permite aplicar las mismas reglas de ILM a todos los tenants y buckets.

Disponer de varias políticas de ILM activas te permite aplicar las reglas de ILM adecuadas a tenants y buckets específicos para cumplir diversos requisitos de calidad de servicio.

Crear una política de ILM

Acerca de esta tarea

Antes de crear tu propia política, verifica que la "política de ILM predeterminada" no cumpla con tus requisitos de almacenamiento.

> Utiliza únicamente las políticas proporcionadas por el sistema, 2 copies Policy (para grids de un solo sitio) o 1 Copy per Site (para grids de varios sitios), en sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla predeterminada en esta política utiliza el grupo de almacenamiento All Storage Nodes, que contiene todos los sitios. Si tu sistema StorageGRID tiene más de un sitio, dos copias de un objeto podrían colocarse en el mismo sitio.

Si el "Se ha activado la configuración global de S3 Object Lock", debes asegurarte de que la política de ILM cumpla con los requisitos de los buckets que tienen habilitado S3 Object Lock. En esta sección, sigue las instrucciones que mencionan tener S3 Object Lock habilitado.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permisos de acceso necesarios".
- Tienes "reglas de ILM creadas" según si S3 Object Lock está activado.

  S3 Object Lock no está activado

  - Tienes "creó las normas de ILM" que quieres añadir a la política. Según sea necesario, puedes guardar una política, crear reglas adicionales y luego editar la política para añadir las nuevas reglas.
  - Tienes "creaste una regla ILM predeterminada" que no contiene ningún filtro.

  S3 Object Lock activado

  - El "La configuración global de S3 Object Lock ya está activada" para el sistema StorageGRID.
  - Tienes "creaste las reglas de ILM conformes y no conformes" que quieres añadir a la política. Según sea necesario, puedes guardar una política, crear reglas adicionales y luego editar la política para añadir las nuevas reglas.
  - Tienes "creaste una regla ILM predeterminada" para la política que cumple con los requisitos.

- Opcionalmente, has visto el vídeo:

Resumen de las políticas de ILM

Véase también "Usa políticas de ILM".

Pasos

1. Selecciona **ILM** > **Policies**.

   Si la configuración global de S3 Object Lock está activada, la página de políticas de ILM indica qué reglas de ILM cumplen.

2. Decide cómo quieres crear la política de ILM.

   Crear nueva política

   a. Selecciona **Crear política**.

   Clonar una política existente

   a. Marca la casilla de la política con la que quieras empezar y, a continuación, selecciona **Clonar**.

   Editar política existente

   a. Si una política está inactiva, puedes editarla. Marca la casilla de la política inactiva con la que quieras empezar y luego selecciona **Editar**.

3. En el campo **Nombre de la política**, introduce un nombre único para la política.

4. Opcionalmente, en el campo **Motivo del cambio**, introduce el motivo por el que estás creando una nueva política.
5. Para añadir reglas a la política, selecciona **Seleccionar reglas**. Selecciona el nombre de una regla para ver su configuración.

   Si vas a clonar una política:

   - Se han seleccionado las reglas que utiliza la política que estás clonando.
   - Si la política que estás clonando utilizaba alguna regla sin filtros que no fuera la regla predeterminada, se te pedirá que elimines todas esas reglas excepto una.
   - Si la regla predeterminada utilizaba un filtro, se te pedirá que selecciones una nueva regla predeterminada.
   - Si la regla predeterminada no era la última regla, puedes mover la regla al final de la nueva política.

S3 Object Lock no está activado

a. Selecciona una regla predeterminada para la política. Para crear una nueva regla predeterminada, selecciona **ILM rules page**.

   La regla por defecto se aplica a cualquier objeto que no coincida con otra regla de la política. La regla por defecto no puede usar ningún filtro y siempre se evalúa al final.

> No utilices la regla Make 2 Copies como regla predeterminada para una política. La regla Make 2 Copies utiliza un único grupo de almacenamiento, All Storage Nodes, que contiene todos los sitios. Si tu sistema StorageGRID tiene más de un sitio, dos copias de un objeto podrían almacenarse en el mismo sitio.

S3 Object Lock activado

a. Selecciona una regla predeterminada para la política. Para crear una nueva regla predeterminada, selecciona **ILM rules page**.

   La lista de reglas contiene solo las reglas que cumplen los requisitos y no utilizan ningún filtro.

> No utilices la regla «Make 2 Copies» como regla predeterminada para una política. La regla «Make 2 Copies» utiliza un único grupo de almacenamiento, «All Storage Nodes», que contiene todos los sitios. Si utilizas esta regla, varias copias de un objeto podrían colocarse en el mismo sitio.

b. Si necesitas una regla «predeterminada» diferente para los objetos en los buckets de S3 que no cumplen los requisitos, selecciona **Incluir una regla sin filtros para los buckets de S3 que no cumplen los requisitos** y selecciona una regla para estos buckets que no utilice ningún filtro.

   Por ejemplo, es posible que quieras utilizar un Cloud Storage Pool para almacenar objetos en buckets en los que no esté habilitado S3 Object Lock.

> Solo puedes seleccionar una regla que no cumpla los requisitos y que no utilice un filtro.

Véase también "Ejemplo 7: política de ILM compatible con S3 Object Lock".

6. Cuando hayas terminado de seleccionar la regla predeterminada, selecciona **Continuar**.
7. En el paso «Otras reglas», selecciona cualquier otra regla que desees añadir a la política. Estas reglas utilizan al menos un filtro (cuenta de inquilino, nombre del bucket, filtro avanzado o el tiempo de referencia no actual). Luego selecciona **Seleccionar**.

   La ventana «Crear una política» muestra ahora las reglas que has seleccionado. La regla predeterminada aparece al final, con el resto de reglas por encima de ella.

   Si S3 Object Lock está activado y además has seleccionado una regla «predeterminada» que no cumple los requisitos, dicha regla se añade como la penúltima regla de la política.

   > Aparecerá una advertencia si alguna regla no conserva los objetos de forma permanente. Al activar esta política, debes confirmar que quieres que StorageGRID elimine los objetos cuando caduquen las instrucciones de ubicación de la regla predeterminada (a menos que un ciclo de vida de bucket mantenga los objetos durante un periodo de tiempo más largo).

8. Arrastra las filas correspondientes a las reglas no predeterminadas para determinar el orden en el que se evaluarán dichas reglas.

   No puedes mover la regla predeterminada. Si S3 Object Lock está habilitado, tampoco puedes mover la regla "predeterminada" que no cumpla los requisitos, si se seleccionó alguna.

   > Debes comprobar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan según las reglas en el orden indicado, empezando por la parte superior.

9. Según sea necesario, selecciona **Select rules** para añadir o eliminar reglas.
10. Cuando hayas terminado, selecciona **Guardar**.
11. Repite estos pasos para crear políticas de ILM adicionales.
12. Simula una política de ILM. Siempre debes simular una política antes de activarla para asegurarte de que funciona como se espera.

Simular una política

Simula una política en objetos de prueba antes de activarla y aplicarla a tus datos de producción.

Antes de empezar

- Conoces el bucket de S3 y la clave de objeto de cada objeto que quieres probar.

Pasos

1. Utiliza un cliente S3 o la "Consola de S3" para cargar los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, marca la casilla correspondiente a la política y luego selecciona **Simular**.
3. En el campo **Objeto**, introduce el S3 `bucket/object-key` para un objeto de prueba. Por ejemplo, `bucket-01/filename.png`.
4. Si está activada la función de versiones de S3, puedes introducir, si lo deseas, un ID de versión para el objeto en el campo **Version ID**.
5. Selecciona **Simular**.
6. En la sección de resultados de la simulación, confirma que cada objeto se haya asignado a la regla correcta.

7. Para determinar qué grupo de almacenamiento o qué perfil de código de borrado está activo, selecciona el nombre de la regla correspondiente para acceder a la página de detalles de la regla.

> Revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales con los recursos mientras se evalúan y se implementan las nuevas ubicaciones.

Resultados

Cualquier modificación en las reglas de la política se reflejará en los resultados de la simulación y mostrará la nueva coincidencia y la coincidencia anterior. La ventana Simular policy conserva los objetos que probaste hasta que selecciones **Clear all** o el icono de eliminar para cada objeto en la lista de resultados de la simulación.

Información relacionada

"Ejemplos de simulaciones de políticas de ILM"

Activar una política

Al activar una única política nueva de ILM, tanto los objetos existentes como los recién incorporados se gestionan según dicha política. Al activar varias políticas, las etiquetas de política de ILM asignadas a los buckets determinan los objetos que se van a gestionar.

Antes de activar una nueva política:

1. Simula la directiva para confirmar que se comporta como esperas.
2. Revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales con los recursos mientras se evalúan y se implementan las nuevas ubicaciones.

> Los errores en una política de ILM pueden provocar una pérdida de datos irrecuperable.

Acerca de esta tarea

Al activar una política de ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva política activa no entre en vigor hasta que todos los nodos de la red estén disponibles para recibir la nueva política. En algunos casos, el sistema espera antes de aplicar una nueva política activa para asegurarse de que los objetos de la red no se eliminen accidentalmente. En concreto:

- Si realizas cambios en las políticas que **aumenten la redundancia o la durabilidad de los datos**, dichos cambios se aplican de forma inmediata. Por ejemplo, si activas una nueva política que incluye una regla de tres copias en lugar de una de dos, dicha política se aplicará de inmediato, ya que aumenta la redundancia de los datos.
- Si realizas cambios en las políticas que **pudieran reducir la redundancia o la durabilidad de los datos**, dichos cambios no se aplicarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activas una nueva política que utiliza una regla de dos copias en lugar de una de tres, la nueva política aparecerá en la pestaña Active policy pero no entrará en vigor hasta que todos los nodos estén en línea y disponibles.

Pasos

Sigue los pasos para activar una o varias políticas:

Activa una política

Sigue estos pasos si solo vas a tener una política activa. Si ya tienes una o más políticas activas y vas a activar políticas adicionales, sigue los pasos para activar varias políticas.

1. Cuando estés listo para activar una política, selecciona **ILM** > **Políticas**.

   También puedes activar una única política desde la página **ILM** > **Policy tags**.

2. En la pestaña «Políticas», marca la casilla correspondiente a la política que quieras activar y luego selecciona **Activar**.
3. Sigue el paso correspondiente:
   - Si aparece un mensaje de advertencia pidiéndote que confirmes que quieres activar la política, selecciona **OK**.
   - Si aparece un mensaje de advertencia con información sobre la política:
     i. Revisa los detalles para asegurarte de que la política gestione los datos como esperas.
     ii. Si la regla predeterminada almacena los objetos durante un número limitado de días, revisa el diagrama de retención y luego escribe ese número de días en el cuadro de texto.
     iii. Si la regla predeterminada almacena los objetos indefinidamente, pero hay una o varias reglas más con un plazo de conservación limitado, escribe **sí** en el cuadro de texto.
     iv. Selecciona **Activar política**.

Activar varias políticas

Para activar varias políticas, debes crear etiquetas de política y asignar una política a cada etiqueta. Puedes crear un máximo de 10 etiquetas de política para tu grid.

Cuando se utilizan varias etiquetas de política, si los inquilinos reasignan con frecuencia etiquetas de política a los buckets, el rendimiento del grid podría verse afectado. Si tienes inquilinos no confiables, considera usar solo la etiqueta de política Default.

1. Selecciona **ILM** > **Etiquetas de política**.
2. Selecciona **Crear**.
3. En el cuadro de diálogo «Crear etiqueta de política», escribe un nombre para la etiqueta y, opcionalmente, una descripción para la etiqueta.

Los nombres y las descripciones de las etiquetas son visibles para los inquilinos. Elige valores que ayuden a los inquilinos a tomar una decisión informada cuando seleccionen las etiquetas de política que van a asignar a sus buckets. Por ejemplo, si la política asignada va a eliminar objetos después de un periodo de tiempo, podrías comunicar eso en la descripción. No incluyas información confidencial en estos campos.

4. Selecciona **Crear etiqueta**.
5. En la tabla de etiquetas de políticas de ILM, utiliza el menú desplegable para seleccionar una política que quieras asignar a la etiqueta.
6. Si aparecen advertencias en la columna «Limitaciones de la política», selecciona **Ver detalles de la política** para revisar la política.

7. Asegúrate de que cada política gestione los datos como esperas.
8. Selecciona **Activar políticas asignadas**. O selecciona **Borrar cambios** para eliminar la asignación de políticas.
9. En el cuadro de diálogo «Activar políticas con nuevas etiquetas», revisa las descripciones de cómo cada etiqueta, política y regla gestionará los objetos. Haz los cambios que necesites para asegurarte de que las políticas gestionen los objetos como esperas.
10. Cuando estés seguro de que quieres activar las políticas, escribe **sí** en el cuadro de texto y luego selecciona **Activar políticas**.

Información relacionada

"Ejemplo 6: cambio de una política de ILM"

Ejemplos de simulaciones de políticas ILM en StorageGRID

Los ejemplos de simulaciones de políticas de ILM ofrecen pautas para estructurar y modificar simulaciones para tu entorno.

Ejemplo 1: verifica las reglas al simular una política de ILM

Este ejemplo describe cómo verificar las reglas al simular una política.

En este ejemplo, la **política ILM de ejemplo** se está simulando con los objetos importados en dos buckets. La política incluye tres reglas, como sigue:

- La primera regla, **Dos copias, dos años para bucket-a**, solo se aplica a los objetos en bucket-a.
- La segunda regla, **Objetos EC > 1 MB**, se aplica a todos los buckets pero filtra los objetos que superan 1 MB.
- La tercera regla, **Dos copias, dos centros de datos**, es la regla predeterminada. No incluye ningún filtro y no utiliza el tiempo de referencia Noncurrent.

Después de simular la política, confirma que cada objeto fue asignado a la regla correcta.

En este ejemplo:

- `bucket-a/bucket-a object.pdf` coincidió correctamente con la primera regla, que filtra los objetos

en `bucket-a`.

- `bucket-b/test object greater than 1 MB.pdf` se encuentra en `bucket-b`, por lo que no coincidía con la primera regla. En cambio, coincidía correctamente con la segunda regla, que filtra los objetos de más de 1 MB.
- `bucket-b/test object less than 1 MB.pdf` no coincidía con los filtros de las dos primeras reglas, así que se colocará según la regla predeterminada, que no incluye ningún filtro.

Ejemplo 2: reordena las reglas al simular una política de ILM

Este ejemplo muestra cómo puedes reordenar las reglas para cambiar los resultados al simular una política.

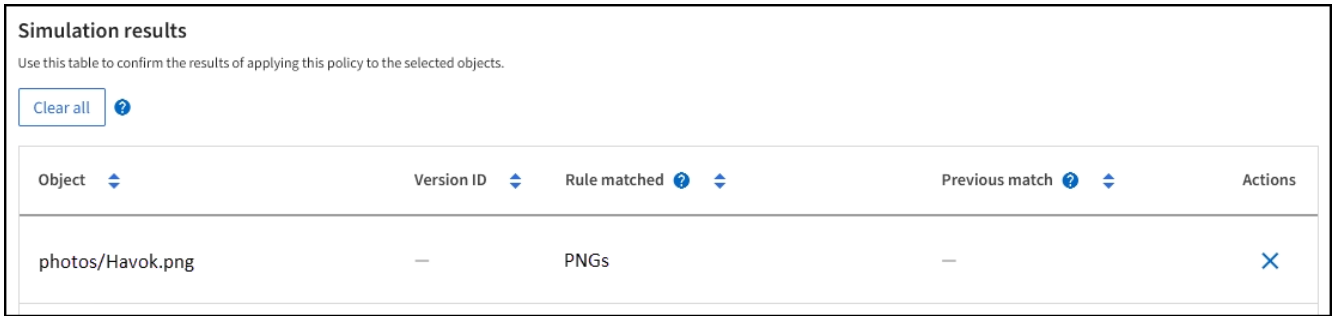
En este ejemplo, se simula la política **Demo**. Esta política, cuyo objetivo es localizar objetos que tengan metadatos de usuario series=x-men, incluye tres reglas, como sigue:

- La primera regla, **PNGs**, filtra los nombres de claves que terminan en `.png`.
- La segunda regla, **X-men**, se aplica únicamente a los objetos del inquilino A y filtra los metadatos de usuario para `series=x-men`.
- La última regla, **Dos copias en dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.

Pasos

1. Una vez añadidas las reglas y guardada la política, selecciona **Simular**.
2. En el campo **Objeto**, introduce el bucket/object-key de S3 para un objeto de prueba y selecciona **Simular**.

   Aparecen los resultados de la simulación, mostrando que el objeto `Havok.png` fue coincidido por la regla **PNGs**.

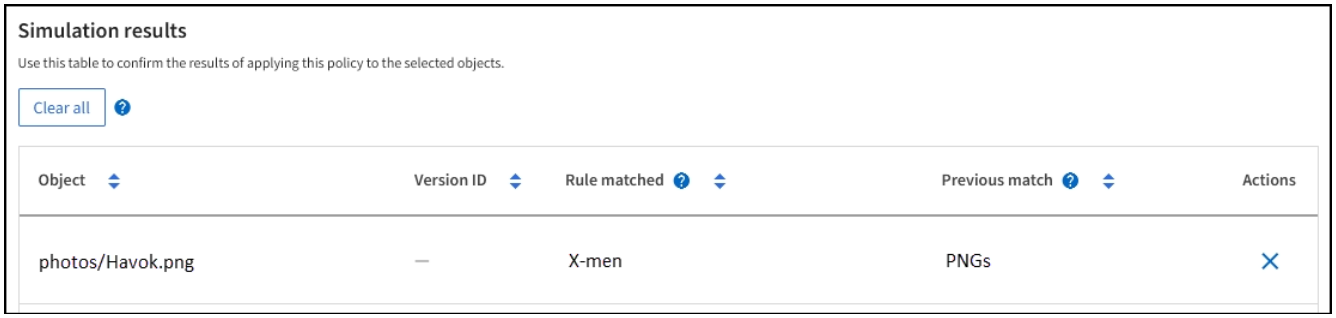


   Sin embargo, `Havok.png` estaba destinado a probar la regla de **X-men**.

3. Para resolver el problema, cambia el orden de las reglas.
   a. Selecciona **Finalizar** para cerrar la ventana Simular política de ILM.
   b. Selecciona **Editar** para editar la política.
   c. Arrastra la regla **X-men** hasta la parte superior de la lista.
   d. Selecciona **Guardar**.
4. Selecciona **Simular**.

   Los objetos que se habían comprobado anteriormente se vuelven a evaluar según la política actualizada y se muestran los nuevos resultados de la simulación. En el ejemplo, la columna «Regla coincidente» muestra que el objeto `Havok.png` ahora cumple la regla de metadatos «X-men», como se esperaba. La

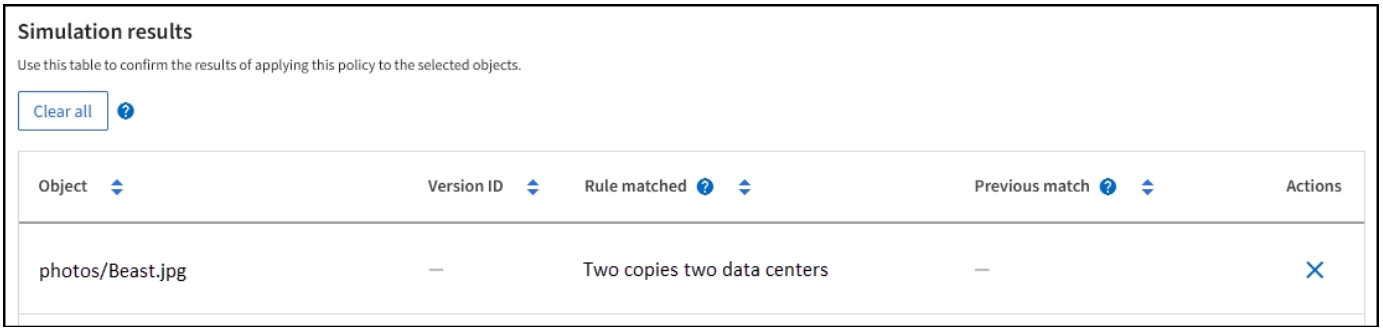
columna «Coincidencia anterior» muestra que la regla «PNGs» coincidía con el objeto en la simulación anterior.



Ejemplo 3: corregir una regla al simular una política de ILM

Este ejemplo muestra cómo simular una política, corregir una regla en la política y continuar la simulación.

En este ejemplo, se está simulando la política **Demo**. Esta política está pensada para encontrar objetos que tengan `series=x-men` metadatos de usuario. Sin embargo, se produjeron resultados inesperados al simular esta política con el objeto `Beast.jpg`. En lugar de coincidir con la regla de metadatos X-men, el objeto coincidió con la regla predeterminada, Two copies two data centers.



Cuando un objeto de prueba no se ajusta a la regla prevista en la política, debes revisar cada regla en la política y corregir cualquier error.

Pasos

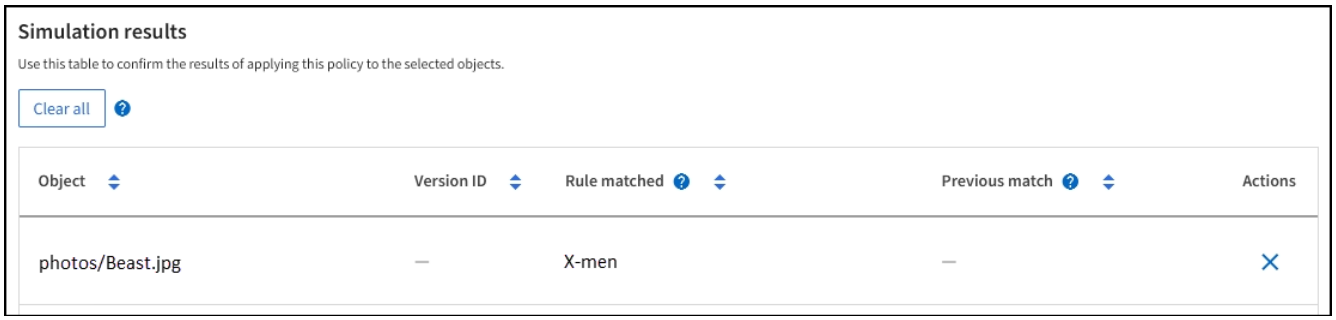
1. Selecciona **Finalizar** para cerrar el cuadro de diálogo Simulate policy. En la página de detalles de la política, selecciona **Retention diagram**. Luego selecciona **Expandir todo** o **Ver detalles** para cada regla según lo necesites.
2. Revisa la cuenta de inquilino de la regla, el periodo de referencia y los criterios de filtrado.

   Por ejemplo, supón que los metadatos para la regla X-men se ingresaron como "x-men01" en vez de "x-men".

3. Para solucionar el error, corrige la regla de la siguiente manera:
   - Si la regla forma parte de la política, puedes clonarla o eliminar la regla de la política y luego editarla.
   - Si la regla forma parte de la política activa, debes clonarla. No puedes editar ni eliminar una regla de la política activa.
4. Vuelve a realizar la simulación.

   En este ejemplo, la regla «X-men» corregida ahora coincide con el `Beast.jpg` objeto según los

`series=x-men` metadatos de usuario, como se esperaba.



Administra las etiquetas de políticas ILM en StorageGRID

Puedes consultar los detalles de una etiqueta de política de ILM, editar una etiqueta o eliminar una etiqueta.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permisos de acceso necesarios".

Ver detalles de la etiqueta de política de ILM

Para ver los detalles de una etiqueta:

1. Selecciona **ILM** > **Etiquetas de política**.
2. Selecciona el nombre de la política en la tabla. Aparece la página de detalles de la etiqueta.
3. En la página de detalles, consulta el historial anterior de las políticas asignadas.
4. Ver una política seleccionándola.

Editar etiqueta de política de ILM

> Los nombres y las descripciones de las etiquetas son visibles para los inquilinos. Elige valores que ayuden a los inquilinos a tomar una decisión informada cuando seleccionen las etiquetas de política que van a asignar a sus buckets. Por ejemplo, si la política asignada va a eliminar objetos después de un periodo de tiempo, podrías comunicar eso en la descripción. No incluyas información confidencial en estos campos.

Para editar la descripción de una etiqueta ya existente:

1. Selecciona **ILM** > **Etiquetas de política**.
2. Marca la casilla de selección correspondiente a la etiqueta y luego selecciona **Editar**.

   También puedes seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta y puedes seleccionar **Editar** en esa página.

3. Modifica la descripción de la etiqueta según sea necesario
4. Selecciona **Guardar**.

Eliminar la etiqueta de la política de ILM

Al eliminar una etiqueta de política, cualquier bucket al que se le haya asignado esa etiqueta tendrá aplicada la política predeterminada.

Para eliminar una etiqueta:

1. Selecciona **ILM** > **Etiquetas de política**.
2. Marca la casilla de selección correspondiente a la etiqueta y luego selecciona **Eliminar**. Aparece un cuadro de diálogo de confirmación.

   También puedes seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta y puedes seleccionar **Eliminar** en esa página.

3. Selecciona **Sí** para eliminar la etiqueta.

Información relacionada

"Conoce cómo crear etiquetas de políticas de ILM"

Verifica una política ILM con búsqueda de metadatos de objetos en StorageGRID

Una vez que hayas activado una política de ILM, introduce objetos de prueba representativos en el sistema StorageGRID y luego realiza una búsqueda de metadatos de los objetos para confirmar que las copias se están creando como se espera y se están ubicando en los lugares correctos.

Antes de empezar

Tienes un identificador de objeto, que puede ser uno de:

- **UUID**: El identificador único universal del objeto.
- **CBID**: El identificador único del objeto dentro de StorageGRID. Puedes obtener el CBID de un objeto a partir del registro de auditoría. Introduce el CBID en mayúsculas.
- **Depósito S3 y clave de objeto**: Cuando se importa un objeto a través de la interfaz de S3, la aplicación cliente utiliza una combinación de depósito y clave de objeto para almacenar e identificar el objeto. Si el depósito S3 está versionado y deseas buscar una versión específica de un objeto S3 utilizando el depósito y la clave de objeto, dispones del **ID de versión**.

Pasos

1. Ingiere el objeto.
2. Selecciona **ILM** > **Búsqueda de metadatos de objetos**.
3. Escribe el identificador del objeto en el campo **Identificador**. Puedes introducir un UUID, un CBID o una clave de bucket/objeto de S3.
4. Si lo deseas, introduce un identificador de versión para el objeto (solo S3).
5. Selecciona **Buscar**.

   Aparecen los resultados de la búsqueda de metadatos del objeto. Esta página muestra los siguientes tipos de información:

   - Metadatos del sistema, como el ID del objeto (UUID), el tipo de resultado (objeto, marcador de eliminación, S3 bucket) y el tamaño lógico del objeto. Consulta la captura de pantalla de ejemplo que

aparece a continuación para obtener más detalles.

- Cualquier par clave-valor de metadatos de usuario personalizados asociados al objeto.
- Para los objetos de S3, cualquier par clave-valor de etiquetas asociado con el objeto.
- En el caso de las copias replicadas de objetos, la ubicación de almacenamiento actual de cada copia.
- ${post_edited_translations.segment}
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluyendo el nombre del bucket externo y el identificador único del objeto.
- En el caso de los objetos segmentados y los objetos compuestos, una lista de los segmentos del objeto que incluye los identificadores de los segmentos y los tamaños de los datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
- Todos los metadatos de los objetos en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema cuya persistencia no está garantizada de una versión a otra.

6. Confirma que el objeto esté almacenado en la ubicación o ubicaciones correctas y que sea el tipo de copia correcto.

   Si la opción de auditoría está activada, también puedes supervisar el registro de auditoría para ver el mensaje "ORLM Object Rules Met". El mensaje de auditoría ORLM puede darte más información sobre el estado del proceso de evaluación de ILM, pero no puede darte información sobre la corrección de la ubicación de los datos del objeto ni sobre la integridad de la política de ILM. Debes evaluarlo tú mismo. Para más detalles, consulta "Revisar los registros de auditoría".

El siguiente ejemplo muestra los resultados de la consulta de metadatos de un objeto de prueba de S3 almacenado en dos copias replicadas.

> La siguiente captura de pantalla es un ejemplo. Tus resultados variarán dependiendo de tu versión de StorageGRID.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Información relacionada

"Usa la API de REST de S3"

Trabaja con políticas ILM y reglas ILM en StorageGRID

A medida que cambian tus requisitos de almacenamiento, puede que necesites aplicar políticas adicionales o modificar las reglas de ILM asociadas a una política. Puedes consultar las métricas de ILM para determinar el rendimiento del sistema.

Antes de empezar

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

Ver las políticas de ILM

Para consultar las políticas de ILM activas e inactivas y el historial de activación de políticas:

1. Selecciona **ILM** > **Policies**.
2. Selecciona **Policies** para ver una lista de las políticas activas e inactivas. La tabla muestra el nombre de cada política, las etiquetas a las que está asignada y si está activa o inactiva.
3. Selecciona **Historial de activación** para ver una lista de las fechas de inicio y fin de la activación de las políticas.
4. Selecciona el nombre de una política para ver los detalles de la política.

> Si consultas los detalles de una política cuyo estado sea «Editado» o «Eliminado», aparecerá un mensaje en el que se explica que estás viendo la versión de la política que estuvo activa durante el periodo de tiempo especificado y que, desde entonces, ha sido editada o eliminada.

Editar una política de ILM

Solo puedes editar una política inactiva. Si quieres editar una política activa, desactívala o crea un clon y edita el clon.

Para editar una política:

1. Selecciona **ILM** > **Policies**.
2. Marca la casilla de la política que quieras editar y luego selecciona **Editar**.
3. Modifica la política siguiendo las instrucciones en "${post_edited_translations.segment}".
4. Simula la política antes de volver a activarla.

> Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irrecuperable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Clonar una política de ILM

Para clonar una política de ILM:

1. Selecciona **ILM** > **Policies**.
2. Marca la casilla de la política que quieres clonar y luego selecciona **Clonar**.
3. Crea una nueva política a partir de la que has clonado siguiendo las instrucciones en "${post_edited_translations.segment}".

> Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irrecuperable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Eliminar una política de ILM

Solo puedes eliminar una política de ILM si está inactiva. Para eliminar una política:

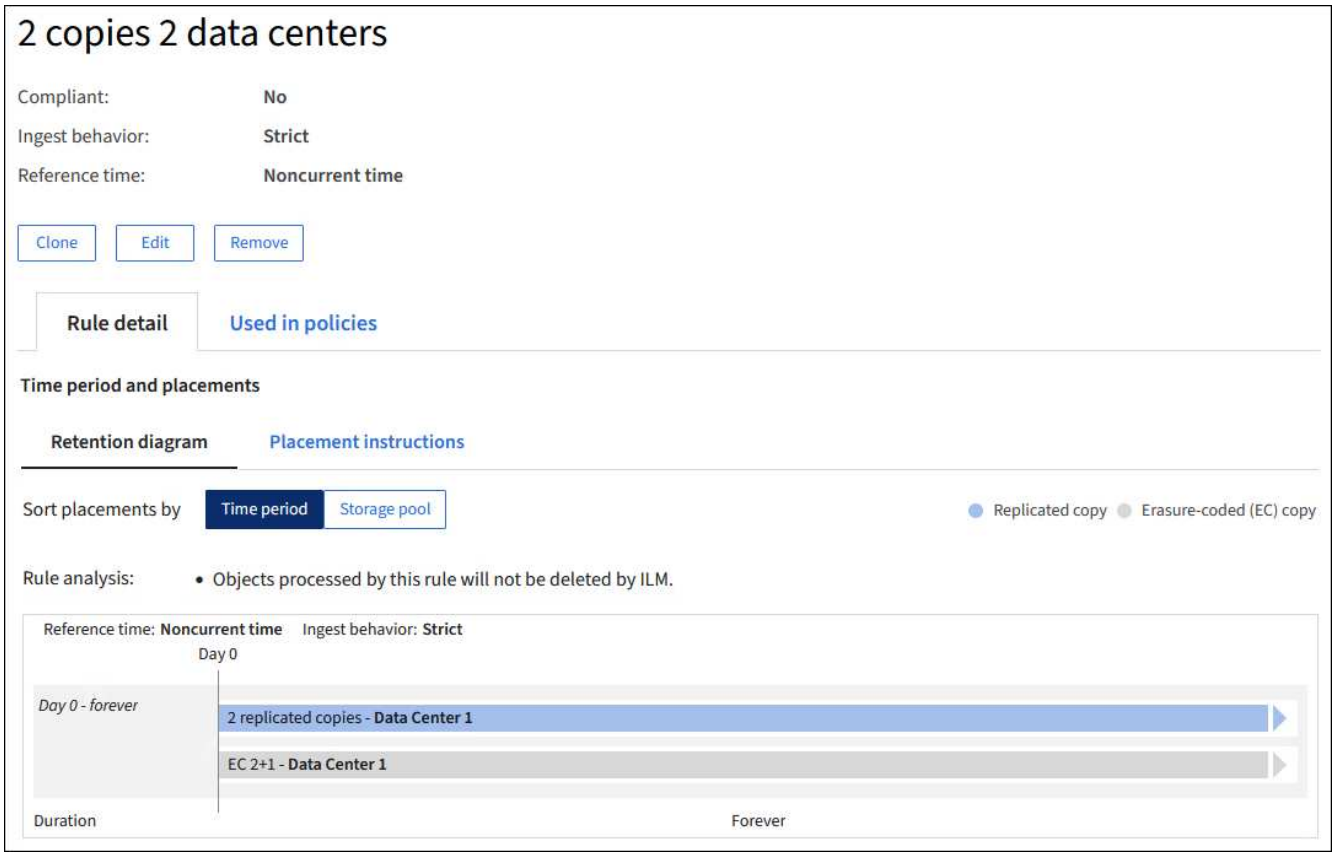
1. Selecciona **ILM** > **Policies**.

2. Marca la casilla de la política inactiva que quieras eliminar.
3. Selecciona **Eliminar**.

Ver detalles de la regla ILM

Para consultar los detalles de una regla ILM, incluido el diagrama de retención y las instrucciones de ubicación de la regla:

1. Selecciona **ILM** > **Reglas**.
2. Selecciona el nombre de la regla cuyos detalles quieras consultar. Ejemplo:



Además, puedes utilizar la página de detalles para clonar, editar o eliminar una regla. No puedes editar ni eliminar una regla si se utiliza en alguna política.

Clonar una regla de ILM

Puedes clonar una regla existente si quieres crear una nueva regla que use algunos de los ajustes de la regla existente. Si necesitas editar una regla que se usa en alguna política, clona la regla y haz los cambios en la copia. Después de hacer los cambios en la copia, puedes quitar la regla original de la política y reemplazarla por la versión modificada según sea necesario.

No puedes clonar una regla de ILM si se creó con StorageGRID versión 10.2 o anterior.

Pasos

1. Selecciona **ILM** > **Reglas**.

2. Marca la casilla de la regla que quieras clonar y luego selecciona **Clonar**. O bien, selecciona el nombre de la regla y luego selecciona **Clonar** en la página de detalles de la regla.
3. Actualiza la regla clonada siguiendo los pasos para Editar una regla ILM y "uso de filtros avanzados en las reglas de ILM".

   Al clonar una regla ILM, debes introducir un nuevo nombre.

Editar una regla de ILM

Es posible que tengas que modificar una regla de ILM para cambiar un filtro o una instrucción de ubicación.

No puedes editar una regla si se utiliza en alguna política de ILM. En su lugar, puedes clonar la regla y realizar los cambios necesarios en la copia clonada.

> ⚠ Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irrecuperable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Confirma que la regla que deseas editar no se use en ninguna política de ILM.
3. Si la regla que deseas editar no está en uso, marca la casilla correspondiente a dicha regla y selecciona **Acciones** > **Editar**. O bien, selecciona el nombre de la regla y luego selecciona **Editar** en la página de detalles de la regla.
4. Sigue los pasos del asistente para editar reglas de ILM. Si es necesario, sigue los pasos para "crear una regla de ILM" y "uso de filtros avanzados en las reglas de ILM".

   Al editar una regla de ILM, no puedes cambiar su nombre.

Eliminar una regla de ILM

Para que la lista de reglas de ILM actuales sea más manejable, elimina aquellas reglas de ILM que probablemente no vayas a utilizar.

Pasos

Para eliminar una regla de ILM que se esté utilizando actualmente en una política activa:

1. Clona la política.
2. Elimina la regla ILM del clon de la política.
3. Guarda, simula y activa la nueva política para asegurarte de que los objetos estén protegidos tal y como se espera.
4. Ve a los pasos para eliminar una regla de ILM que se está usando en una política inactiva.

Para eliminar una regla de ILM que se está utilizando actualmente en una política inactiva:

1. Selecciona la política inactiva.
2. Elimina la regla ILM de la política o eliminar la política.

3. Sigue los pasos para eliminar una regla de ILM que no se esté utilizando actualmente.

Para eliminar una regla de ILM que no se está utilizando actualmente:

1. Selecciona **ILM** > **Reglas**.
2. Confirma que la regla que deseas eliminar no se use en ninguna política.
3. Si la regla que deseas eliminar no está en uso, selecciónala y elige **Acciones** > **Eliminar**. Puedes seleccionar varias reglas y eliminarlas todas a la vez.
4. Selecciona **Sí** para confirmar que deseas eliminar la regla de ILM.

Ver métricas de ILM

Puedes consultar métricas de ILM, como el número de objetos en la cola y la tasa de evaluación. Puedes supervisar estas métricas para determinar el rendimiento del sistema. Una cola o una tasa de evaluación elevadas podrían indicar que el sistema no es capaz de seguir el ritmo de la tasa de consumo, que la carga de las aplicaciones cliente es excesiva o que existe alguna situación anómala.

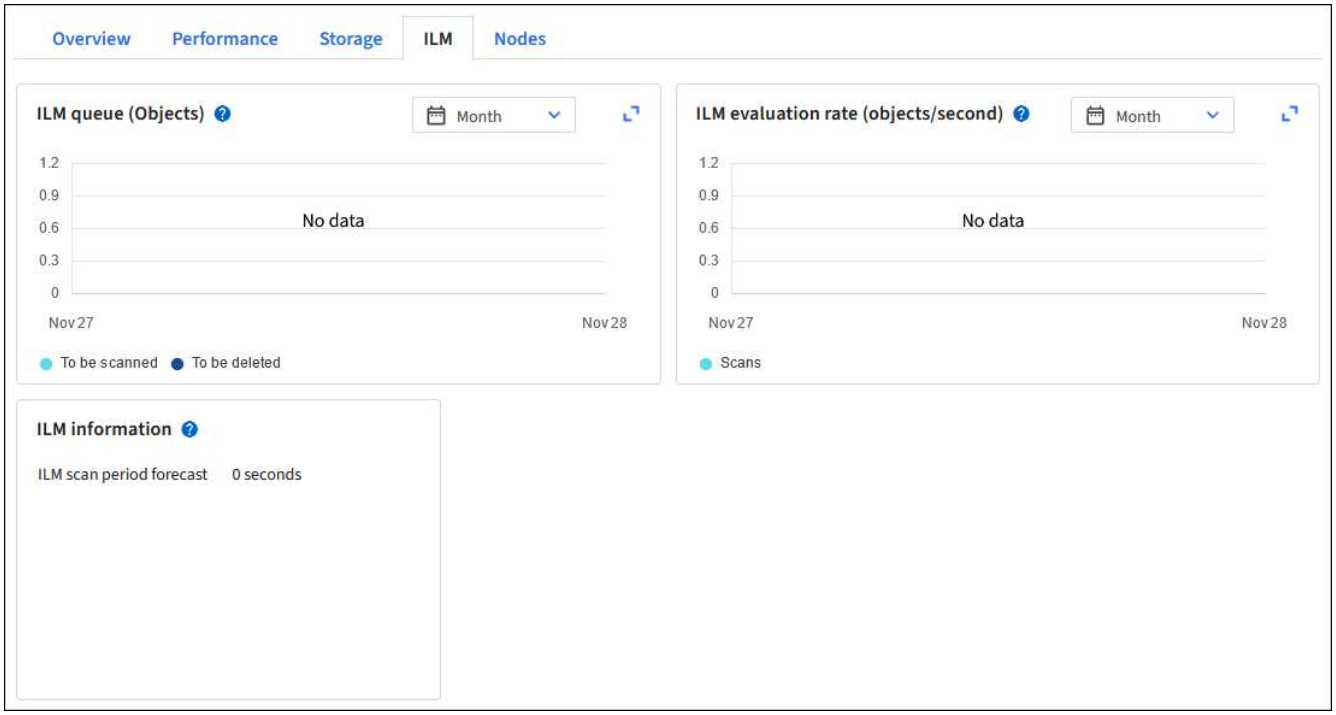
Pasos

1. Selecciona **Dashboard** > **ILM**.

> Dado que el panel de control se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervisa las métricas en la pestaña «ILM».

   Puedes hacer clic en el signo de interrogación (?) para ver una descripción de los elementos de la pestaña ILM.



Usa S3 Object Lock

Cómo S3 Object Lock protege los objetos en StorageGRID

Como administrador de la grid, puedes habilitar S3 Object Lock para tu sistema StorageGRID e implementar una política de ILM compatible para ayudar a garantizar que los objetos en buckets específicos de S3 no se eliminen ni se sobrescriban durante un periodo de tiempo especificado.

¿Qué es S3 Object Lock?

La función S3 Object Lock de StorageGRID es una solución de protección de objetos equivalente a S3 Object Lock en Amazon Simple Storage Service (Amazon S3).

Cuando la configuración global de S3 Object Lock está habilitada para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear buckets con o sin S3 Object Lock habilitado. Si un bucket tiene S3 Object Lock habilitado, el control de versiones de buckets es obligatorio y se habilita automáticamente.

Un bucket sin S3 Object Lock solo puede tener objetos sin una configuración de retención especificada. Ningún objeto ingerido tendrá configuración de retención.

Un bucket con S3 Object Lock puede tener objetos con y sin ajustes de retención especificados por las aplicaciones cliente de S3. Algunos objetos incorporados tendrán ajustes de retención.

Un bucket con S3 Object Lock y la retención predeterminada configurada puede contener objetos cargados con ajustes de retención especificados y nuevos objetos sin ajustes de retención. Los nuevos objetos usan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

Efectivamente, todos los objetos recién ingeridos tienen ajustes de retención cuando se configura la retención predeterminada. Los objetos existentes sin ajustes de retención de objetos no se ven afectados.

Modos de retención

La función Object Lock de StorageGRID S3 admite dos modos de retención para aplicar distintos niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
  - El objeto no se puede eliminar hasta que se alcance su fecha de retención.
  - ${post_edited_translations.segment}
  - La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha.
- En modo de gobernanza:
  - Los usuarios con permisos especiales pueden utilizar un encabezado de omisión en las solicitudes para modificar determinados ajustes de retención.
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}

Configuración de retención para las versiones de los objetos

Si se crea un depósito con S3 Object Lock activado, los usuarios pueden usar la aplicación cliente de S3 para

especificar de forma opcional los siguientes parámetros de retención para cada objeto que se añada al depósito:

- **Modo de retención**: cumplimiento normativo o gobernanza.
- **Fecha límite de conservación**: Si la fecha límite de conservación de una versión de un objeto es posterior a la fecha actual, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: Al aplicar una retención legal a la versión de un objeto, dicho objeto queda bloqueado de inmediato. Por ejemplo, podrías necesitar aplicar una retención legal a un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de caducidad, sino que permanece vigente hasta que se elimine de forma explícita. Las retenciones legales son independientes de la retain-until-date.

  ${post_edited_translations.segment}

  Para obtener detalles sobre la configuración de los objetos, consulta "Utiliza la API de REST de S3 para configurar S3 Object Lock".

${post_edited_translations.segment}

Si se crea un bucket con S3 Object Lock activado, los usuarios pueden, si lo desean, especificar los siguientes ajustes predeterminados para el bucket:

- **Modo de retención predeterminado**: cumplimiento o gobernanza.
- ${post_edited_translations.segment}

La configuración predeterminada del depósito solo se aplica a los objetos nuevos que no tienen su propia configuración de retención. Los objetos existentes en el depósito no se ven afectados cuando añades o cambias esta configuración predeterminada.

Consulta "Crear un depósito de S3" y "Actualizar la retención predeterminada de S3 Object Lock".

Comparación entre S3 Object Lock y Compliance tradicional

La función S3 Object Lock sustituye a la función Compliance que estaba disponible en versiones anteriores de StorageGRID. Porque la función S3 Object Lock cumple con los requisitos de Amazon S3, deja de utilizarse la función Compliance propia de StorageGRID, que ahora se denomina "legacy Compliance".

La configuración global de Compliance está obsoleta. Si activaste esta configuración usando una versión anterior de StorageGRID, la configuración de S3 Object Lock se activa automáticamente. Puedes seguir usando StorageGRID para gestionar la configuración de los buckets conformes existentes; sin embargo, no puedes crear nuevos buckets conformes. Para más detalles, consulta "NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5".

Si usaste la función heredada de Compliance en una versión anterior de StorageGRID, consulta la siguiente tabla para saber cómo se compara con la función S3 Object Lock en StorageGRID.

	Bloqueo de objetos de S3	Cumplimiento (legacy)
¿Cómo se activa la función a nivel global?	En el Grid Manager, selecciona **Configuración** > **Sistema** > **S3 Object Lock**.	Ya no es compatible.
¿Cómo se activa la función en un bucket?	Los usuarios deben habilitar S3 Object Lock al crear un nuevo bucket mediante el Tenant Manager, la Tenant Management API o la API de REST de S3.	Ya no es compatible.
¿Se admite el versionado de los buckets?	Sí. El control de versiones del bucket es obligatorio y se activa automáticamente cuando S3 Object Lock está habilitado para el bucket.	No.
¿Cómo se configura la retención de objetos?	Los usuarios pueden establecer una fecha de retención para cada versión de objeto, o pueden establecer un periodo de retención predeterminado para cada bucket.	Los usuarios deben establecer un periodo de retención para todo el bucket. El periodo de retención se aplica a todos los objetos del bucket.
¿Se puede cambiar el periodo de retención?	• En el modo de cumplimiento, la fecha límite de conservación de una versión de un objeto se puede aumentar, pero nunca disminuir. • En el modo de governance, los usuarios con permisos especiales pueden reducir o incluso eliminar la configuración de retención de un objeto.	El periodo de retención de un bucket puede aumentarse, pero nunca reducirse.
¿Dónde se controla la retención legal?	Los usuarios pueden aplicar o levantar una retención legal para cualquier versión de objeto en el bucket.	Se aplica una retención legal al bucket y afecta a todos los objetos en el bucket.

	Bloqueo de objetos de S3	Cumplimiento (legacy)
¿Cuándo se pueden eliminar los objetos?	• En el modo de cumplimiento, una versión de objeto puede eliminarse después de que se alcance la fecha de retención, siempre que el objeto no esté bajo retención legal. • En el modo de gobernanza, los usuarios con permisos especiales pueden eliminar un objeto antes de que se alcance su retain-until-date, siempre que el objeto no esté bajo legal hold.	Un objeto se puede eliminar una vez que haya vencido el periodo de retención, siempre que el bucket no esté bajo retención legal. Los objetos se pueden eliminar automáticamente o manualmente.
¿Se admite la configuración del ciclo de vida de los buckets?	Sí	No

Flujo de trabajo de S3 Object Lock en StorageGRID

Como administrador de la grid, debes coordinarte estrechamente con los usuarios de los tenants para garantizar que los objetos estén protegidos de forma que se cumplan sus requisitos de retención.

${post_edited_translations.segment}

Las siguientes listas para administradores de grid y usuarios de inquilinos contienen las tareas a grandes rasgos para usar la función S3 Object Lock.

Administrador de grid

- Activa la configuración global de S3 Object Lock para todo el sistema StorageGRID.
- Asegúrate de que las políticas de gestión del ciclo de vida de la información (ILM) sean *conformes*; es decir, que cumplan con "Requisitos de los buckets con S3 Object Lock activado".
- Si es necesario, permite que un inquilino utilice Compliance como modo de retención. De lo contrario, solo se permite el modo Governance.
- Si es necesario, establece un periodo máximo de retención para un tenant.

Usuario arrendatario

- Revisa las consideraciones para los buckets y objetos con S3 Object Lock.
- Si es necesario, ponte en contacto con el administrador de grid para activar la configuración global de S3 Object Lock y establecer los permisos.
- ${post_edited_translations.segment}
- Opcionalmente, configura los ajustes de retención predeterminados para un bucket:
  - Modo de retención predeterminado: Governance o Compliance, si lo permite el administrador del grid.
  - Período de retención predeterminado: debe ser menor o igual al período máximo de retención

establecido por el administrador de grid.

- ${post_edited_translations.segment}
  - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la grid.
  - Fecha de retención: debe ser menor o igual a lo permitido por el periodo máximo de retención establecido por el administrador de grid.

Requisitos de S3 Object Lock en StorageGRID

Debes revisar los requisitos para habilitar la configuración global de S3 Object Lock, los requisitos para crear reglas de ILM y políticas de ILM compatibles, y las restricciones que StorageGRID impone a los buckets y objetos que usan S3 Object Lock.

Requisitos para usar la configuración global de S3 Object Lock

- Debes activar la configuración global de S3 Object Lock usando el Grid Manager o la Grid Management API antes de que cualquier tenant de S3 pueda crear un bucket con S3 Object Lock activado.
- Al habilitar la configuración global de S3 Object Lock, todas las cuentas de inquilinos de S3 pueden crear buckets con S3 Object Lock habilitado.
- Una vez que hayas activado la configuración global de S3 Object Lock, no podrás desactivarla.
- No puedes habilitar S3 Object Lock a nivel global a menos que la regla predeterminada de todas las políticas de ILM activas sea *conforme* (es decir, la regla predeterminada debe cumplir con los requisitos de los buckets con S3 Object Lock habilitado).
- Cuando la configuración global de S3 Object Lock está activada, no puedes crear una nueva política de ILM ni activar una política de ILM existente a menos que la regla predeterminada de la política sea compatible. Después de que la configuración global de S3 Object Lock se haya activado, las páginas de reglas de ILM y políticas de ILM indican qué reglas de ILM son compatibles.

Requisitos para reglas de ILM compatibles

Si deseas habilitar la configuración global de S3 Object Lock, debes asegurarte de que la regla predeterminada de todas las políticas de ILM activas sea compatible. Una regla compatible satisface los requisitos tanto de los buckets con S3 Object Lock habilitado como de cualquier bucket existente que tenga habilitado el cumplimiento heredado:

- Debe crear al menos dos copias replicadas de objetos o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante toda la duración de cada línea en las instrucciones de ubicación.
- Las copias de objetos no se pueden guardar en un Cloud Storage Pool.
- Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando **Hora de ingesta** como hora de referencia.
- Al menos una de las instrucciones de colocación debe ser "para siempre".

Requisitos para las políticas de ILM

Cuando la configuración global de S3 Object Lock está activada, las políticas de ILM activas e inactivas pueden incluir tanto reglas que cumplen los requisitos como reglas que no los cumplen.

- La regla predeterminada en una política de ILM activa o inactiva debe ser compatible.

- Las reglas de incumplimiento solo se aplican a los objetos en los buckets que no tienen habilitado S3 Object Lock o que no tienen habilitada la función de cumplimiento heredada.
- Las reglas de cumplimiento pueden aplicarse a los objetos de cualquier bucket; no es necesario que el bucket tenga activado S3 Object Lock ni el cumplimiento heredado.

"Ejemplo de una política de ILM conforme para S3 Object Lock"

Requisitos para los buckets con S3 Object Lock activado

- Si la configuración global de S3 Object Lock está habilitada para el sistema StorageGRID, puedes usar el Tenant Manager, la API de gestión de inquilinos o la API de REST de S3 para crear buckets con S3 Object Lock habilitado.
- Si tienes pensado utilizar S3 Object Lock, debes habilitar S3 Object Lock al crear el bucket. No puedes habilitar S3 Object Lock en un bucket ya existente.
- Cuando se habilita S3 Object Lock para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar S3 Object Lock ni suspender el control de versiones para el bucket.
- Si lo deseas, puedes especificar un modo de retención y un periodo de retención predeterminados para cada bucket usando el Tenant Manager, la Tenant Management API o la API de REST de S3. La configuración de retención predeterminada del bucket solo se aplica a los nuevos objetos añadidos al bucket que no tengan su propia configuración de retención. Puedes anular esta configuración predeterminada especificando un modo de retención y una retain-until-date para cada versión del objeto cuando se suba.
- ${post_edited_translations.segment}
- CloudMirror replication no es compatible con los buckets con S3 Object Lock habilitado.

Requisitos para los objetos en buckets con S3 Object Lock activado

- Para proteger una versión de un objeto, puedes especificar ajustes de retención predeterminados para el bucket, o puedes especificar ajustes de retención para cada versión del objeto. Los ajustes de retención a nivel de objeto se pueden especificar usando la aplicación cliente de S3 o la API de REST de S3.
- Los ajustes de retención se aplican a las versiones individuales de los objetos. Una versión de un objeto puede tener tanto una configuración de «retención hasta una fecha» como una de «retención legal», una de ellas pero no la otra, o ninguna de las dos. Al especificar una configuración de «retención hasta una fecha» o de «retención legal» para un objeto, solo se protege la versión especificada en la solicitud. Puedes crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en los buckets con S3 Object Lock activado

Cada objeto que se guarda en un bucket con S3 Object Lock activado pasa por estas etapas:

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - Si especificas la configuración de retención para el objeto, se aplica la configuración a nivel de objeto. Se ignora cualquier configuración predeterminada del bucket.
   - Si no se especifican ajustes de retención para el objeto, se aplican los ajustes predeterminados del bucket, si existen.

- Si no se especifican ajustes de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

Si se aplican los parámetros de retención, quedan protegidos tanto el objeto como cualquier metadato definido por el usuario en S3.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el periodo de retención especificado. El número exacto y el tipo de copias de objeto y las ubicaciones de almacenamiento se determinan por las reglas de cumplimiento en las políticas de ILM activas. Si un objeto protegido puede eliminarse antes de que se alcance su fecha de retención depende de su modo de retención.

   - ${post_edited_translations.segment}

Información relacionada

- "Crear un depósito de S3"
- "Actualizar la retención predeterminada de S3 Object Lock"
- "Utiliza la API de REST de S3 para configurar S3 Object Lock"
- "Ejemplo 7: política de ILM compatible con S3 Object Lock"

Habilita el bloqueo de objetos S3 a nivel global en StorageGRID

Si una cuenta de inquilino de S3 debe cumplir con los requisitos normativos a la hora de guardar datos de objetos, debes habilitar S3 Object Lock para todo tu sistema StorageGRID. Al habilitar la configuración global de S3 Object Lock, cualquier usuario de inquilino de S3 podrá crear y gestionar buckets y objetos con S3 Object Lock.

Antes de empezar

- Tienes el "Permiso de acceso raíz".
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Has revisado el flujo de trabajo de S3 Object Lock y entiendes las consideraciones.
- Has confirmado que la regla predeterminada de la política de ILM activa cumple con los requisitos. Consulta "Crear una regla de ILM predeterminada" para más detalles.

Acerca de esta tarea

El administrador de grid debe activar la configuración global de S3 Object Lock para permitir que los usuarios inquilinos creen nuevos buckets con S3 Object Lock activado. Una vez activada esta configuración, no se puede desactivar.

Revisa la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de S3 Object Lock. Cuando habilitas esta configuración, los ajustes de S3 Object Lock por inquilino dependen de la versión de StorageGRID vigente en el momento en que se creó el inquilino.

> La configuración global de Compliance está obsoleta. Si activaste esta configuración usando una versión anterior de StorageGRID, la configuración de S3 Object Lock se activa automáticamente. Puedes seguir usando StorageGRID para gestionar la configuración de los buckets conformes existentes; sin embargo, no puedes crear nuevos buckets conformes. Para más detalles, consulta "NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5".

Pasos

1. Selecciona **Configuración** > **Sistema** > **S3 Object Lock**.

   Aparece la página «Configuración de S3 Object Lock».

2. Selecciona **Habilitar bloqueo de objetos S3**.
3. Selecciona **Aplicar**.

   Aparece un cuadro de diálogo de confirmación que te recuerda que no puedes desactivar S3 Object Lock después de que se haya activado.

4. Si estás seguro de que quieres activar de forma permanente S3 Object Lock para todo tu sistema, selecciona **OK**.

   Cuando seleccionas **OK**:

   - Si la regla predeterminada de la política de ILM activa cumple con los requisitos, S3 Object Lock queda habilitado para toda la grid y no se puede desactivar.
   - Si la regla predeterminada no cumple los requisitos, aparece un error. Debes crear y activar una nueva política de ILM que incluya una regla que cumpla los requisitos como regla predeterminada. Selecciona **OK**. Luego, crea una nueva política, simúlala y actívala. Consulta "Crear política de ILM" para ver las instrucciones.

Resuelve errores de consistencia al actualizar la configuración de S3 Object Lock o legacy Compliance en StorageGRID

Si un centro de datos o varios nodos de almacenamiento de una misma ubicación dejan de estar disponibles, es posible que tengas que ayudar a los usuarios de S3 a aplicar cambios en la configuración de S3 Object Lock o en la configuración de cumplimiento heredada.

Los usuarios de un inquilino que tengan buckets con S3 Object Lock (o Compliance heredado) activado pueden cambiar ciertos ajustes. Por ejemplo, un usuario de un inquilino que use S3 Object Lock podría necesitar poner una versión de un objeto bajo retención legal.

Cuando un usuario de un inquilino actualiza la configuración de un bucket de S3 o la versión de un objeto, StorageGRID intenta actualizar inmediatamente los metadatos del bucket o del objeto en toda la grid. Si el sistema no puede actualizar los metadatos porque un data center o varios Storage Nodes no están disponibles, devuelve un error:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Para solucionar este error, sigue estos pasos:

1. Intenta que todos los nodos de almacenamiento o sitios vuelvan a estar disponibles lo antes posible.
2. Si no puedes poner a disposición un número suficiente de nodos de almacenamiento en cada sitio, ponte en contacto con el soporte técnico, que te ayudará a recuperar los nodos y a garantizar que los cambios

se apliquen de forma coherente en toda la grid.

3. Una vez resuelto el problema subyacente, recuerda al usuario del tenant que vuelva a intentar aplicar los cambios de configuración.

Información relacionada

- "Utiliza una cuenta de inquilino"
- "Usa la API de REST de S3"
- "Recuperar y mantener"

Ejemplos de reglas y políticas de ILM

Reglas y políticas de ILM para la protección y retención básica de objetos en StorageGRID

Puedes usar las siguientes reglas y políticas de ejemplo como punto de partida al definir una política de ILM que se ajuste a tus requisitos de protección y retención de objetos.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

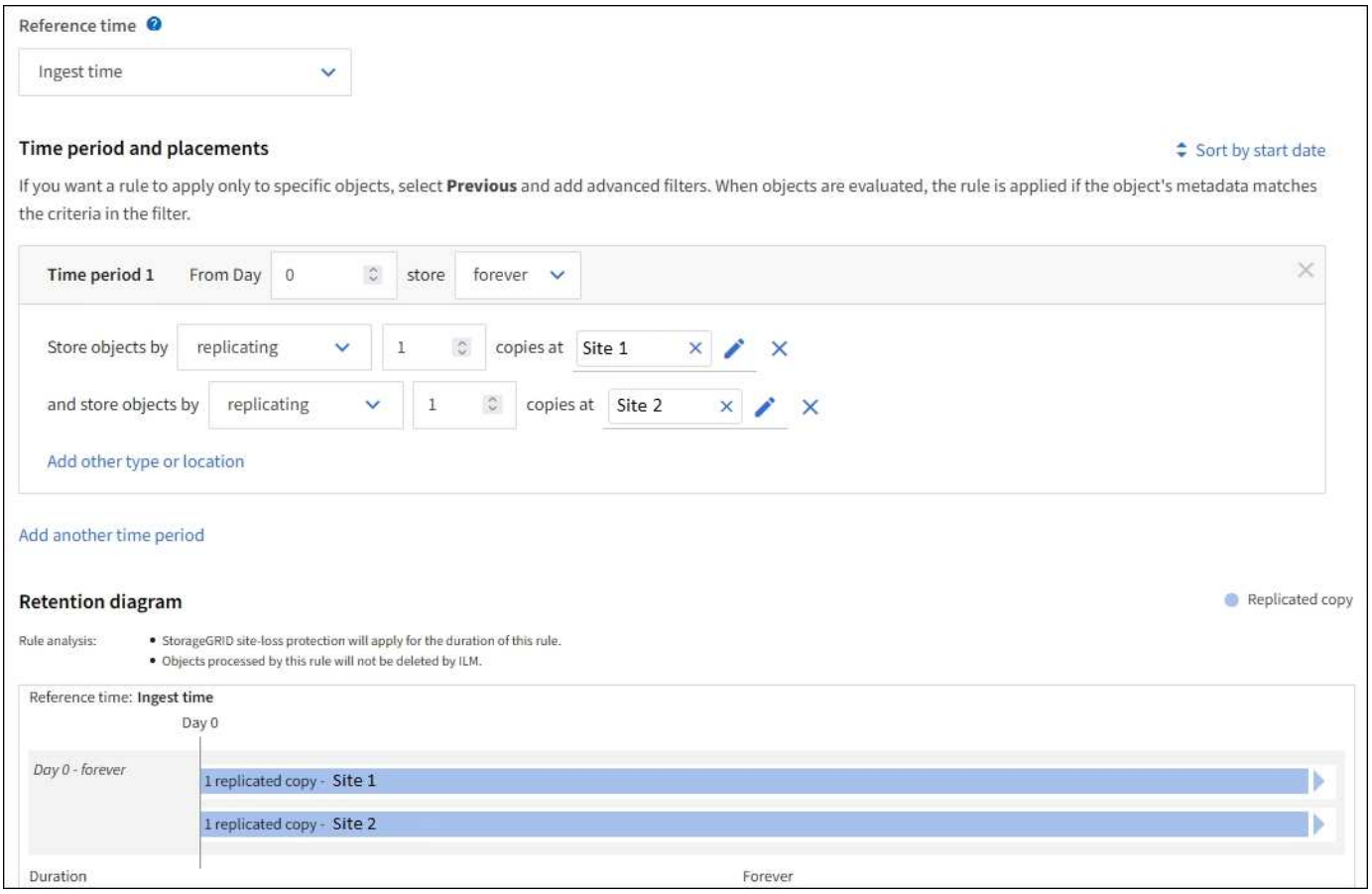
Regla 1 de ILM para el ejemplo 1: Copia los datos de los objetos en dos sitios

Esta regla de ILM de ejemplo copia los datos de los objetos a grupos de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Grupos de almacenamiento en un único sitio	Dos grupos de almacenamiento, cada uno con diferentes sitios, llamados Site 1 y Site 2.
Nombre de la regla	Dos copias dos sitios
Hora de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 hasta siempre, mantén una copia replicada en el sitio 1 y otra copia replicada en el sitio 2.

La sección de análisis de reglas del diagrama de retención dice:

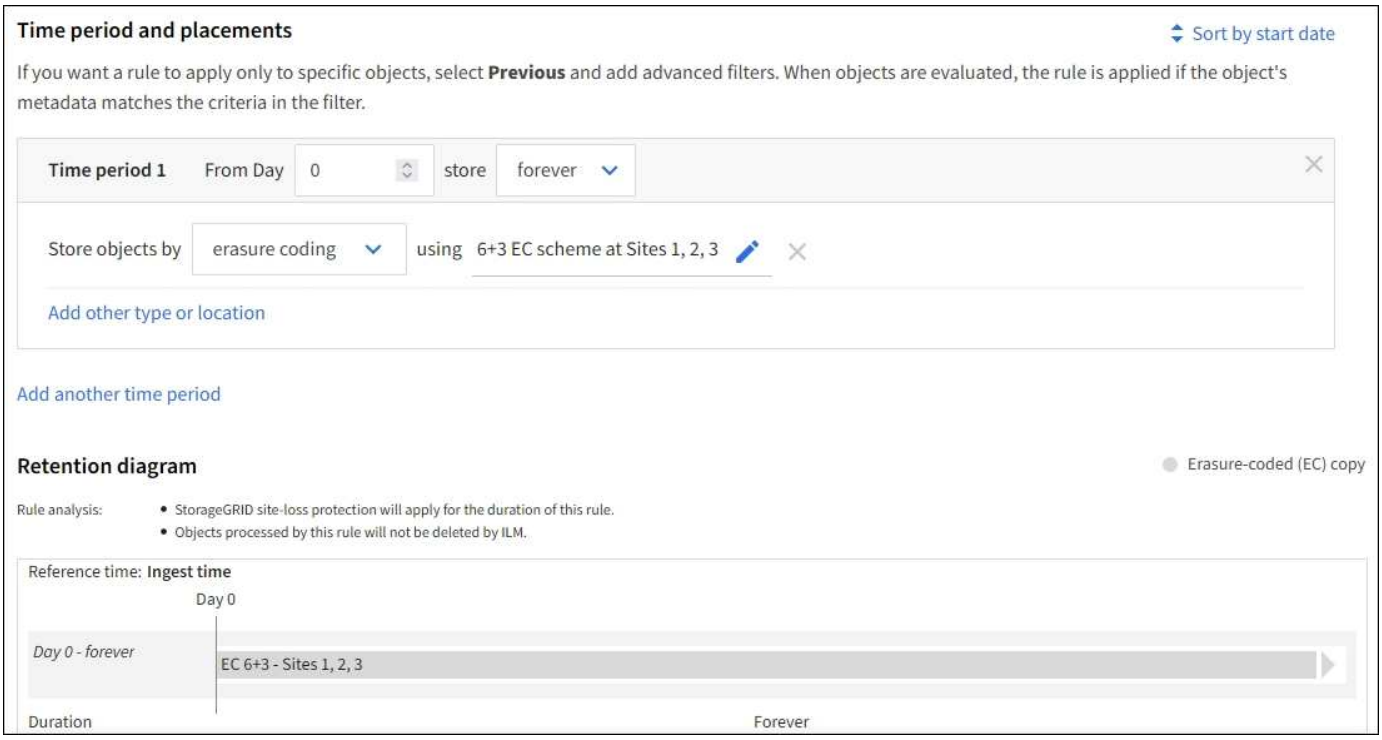
- La protección contra la pérdida de un sitio de StorageGRID se aplicará mientras esté vigente esta regla.
- Los objetos procesados por esta regla no serán eliminados por ILM.



Regla 2 de ILM para el ejemplo 1: perfil de código de borrado con coincidencia de bucket

Esta regla de ILM de ejemplo utiliza un perfil de código de borrado y un bucket de S3 para determinar dónde y durante cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Grupo de almacenamiento con múltiples emplazamientos	• Un grupo de almacenamiento que abarca tres sitios (sitios 1, 2 y 3) • Utiliza el esquema de codificación de borrado 6+3
Nombre de la regla	Bucket S3 finance-records
Hora de referencia	Tiempo de ingesta
Ubicaciones	Para los objetos del bucket S3 llamado finance-records, crea una copia con código de borrado en el pool especificado por el perfil de erasure-coding. Conserva esta copia para siempre.

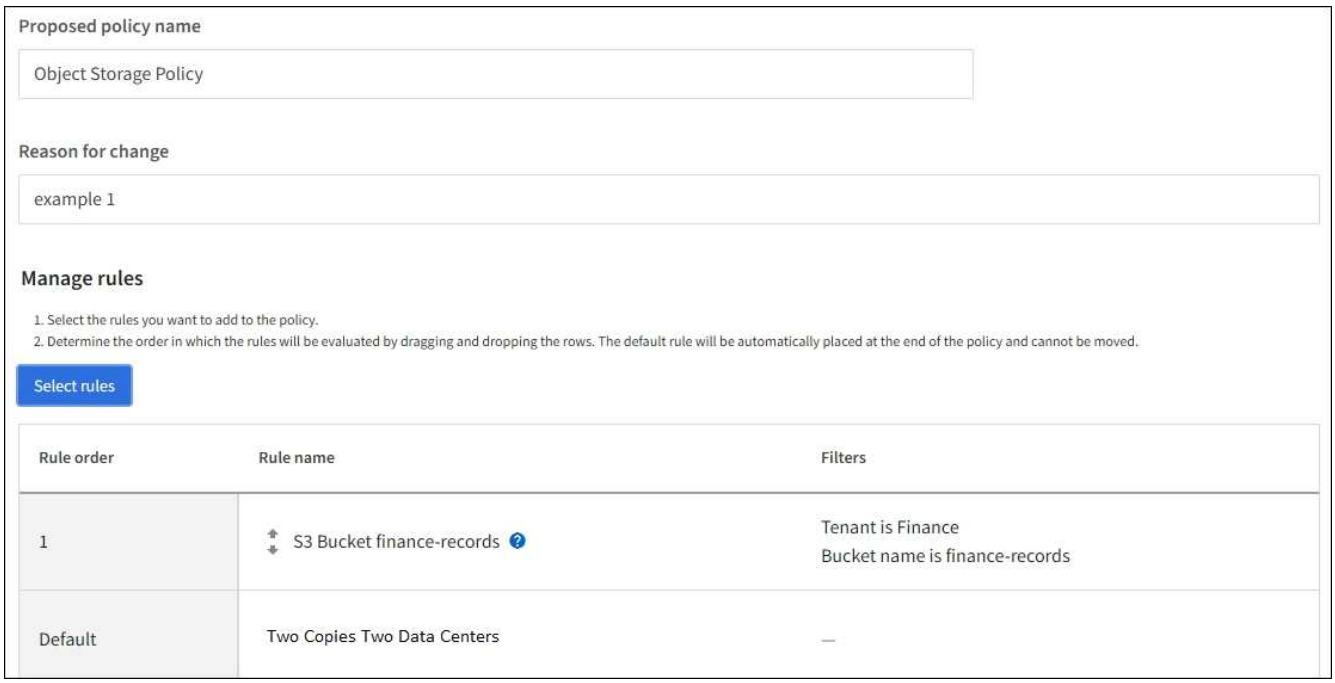


Política de ILM para el ejemplo 1

En la práctica, la mayoría de las políticas de ILM son sencillas, aunque el sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas.

Una política típica de ILM para una red con múltiples emplazamientos podría incluir reglas de ILM como las siguientes:

- Durante la importación, almacena todos los objetos pertenecientes al bucket de S3 llamado `finance-records` en un pool de almacenamiento que contenga tres sitios. Utiliza codificación de borrado 6+3.
- Si un objeto no cumple con la primera regla de ILM, usa la regla de ILM predeterminada de la política, Two Copies Two Data Centers, para almacenar una copia de ese objeto en Site 1 y otra copia en Site 2.



Información relacionada

- "Usa políticas de ILM"
- "${post_edited_translations.segment}"

Reglas y política de ILM para el filtrado de tamaño de objetos EC en StorageGRID

Puedes usar las siguientes reglas y políticas de ejemplo como punto de partida para definir una política de ILM que filtre según el tamaño de los objetos para cumplir los requisitos recomendados de EC.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Regla 1 de ILM para el ejemplo 2: usa EC para objetos mayores de 1 MB

Esta regla de ILM de ejemplo aplica códigos de borrado a los objetos que son mayores de 1 MB.

> El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Solo objetos EC > 1 MB
Hora de referencia	Tiempo de ingesta
Filtro avanzado por tamaño del objeto	Tamaño del objeto superior a 1 MB

Definición de regla	Valor de ejemplo
Ubicaciones	Crea una copia con código de borrado 2+1 usando tres sitios

Regla de ILM 2 para el ejemplo 2: dos copias replicadas

Esta regla de ILM de ejemplo crea dos copias replicadas y no filtra por tamaño de objeto. Esta regla es la regla predeterminada de la política. Dado que la primera regla descarta todos los objetos de más de 1 MB, esta regla solo se aplica a los objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas
Hora de referencia	Tiempo de ingesta
Filtro avanzado por tamaño del objeto	Ninguno
Ubicaciones	Desde el día 0 hasta siempre, mantén una copia replicada en el sitio 1 y otra copia replicada en el sitio 2.

Política de ILM para el ejemplo 2: usar EC para objetos de más de 1 MB

Esta política de ILM de ejemplo incluye dos reglas de ILM:

- La primera regla aplica códigos de borrado a todos los objetos que son mayores de 1 MB.
- La segunda regla de ILM (predeterminada) crea dos copias replicadas. Dado que la regla 1 ha filtrado los objetos de más de 1 MB, la regla 2 solo se aplica a los objetos de 1 MB o menos.

Reglas ILM y política para proteger archivos de imagen en StorageGRID

Puedes utilizar las siguientes reglas y la política de ejemplo para garantizar que las imágenes de más de 1 MB se codifiquen con código de borrado y que se creen dos copias de las imágenes más pequeñas.

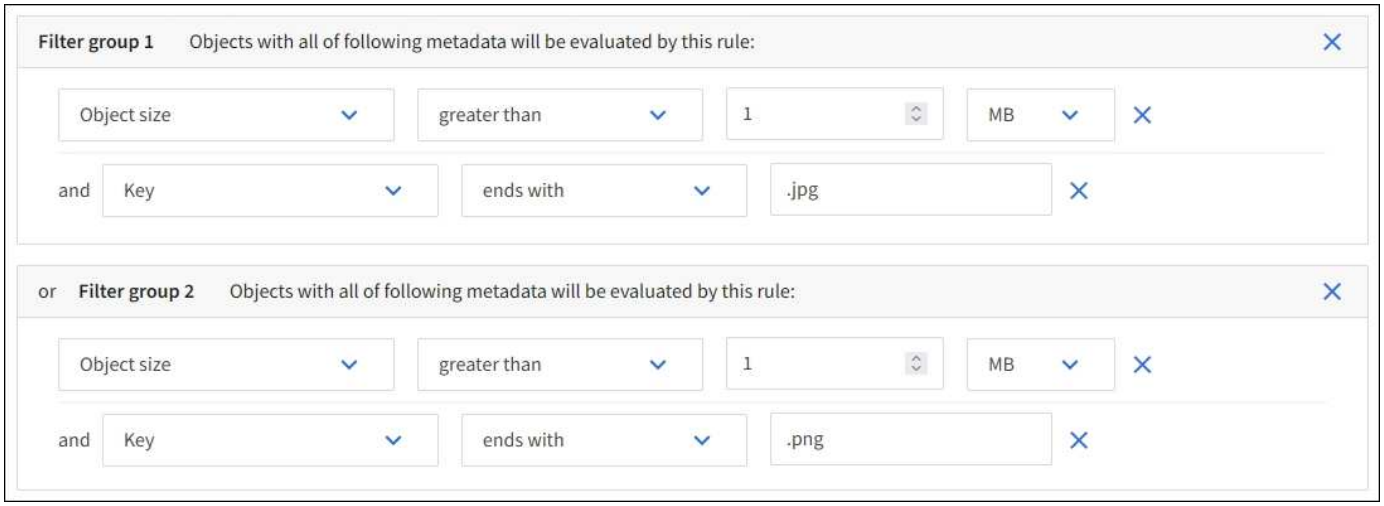
> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Regla 1 de ILM para el ejemplo 3: usa EC para los archivos de imagen mayores de 1 MB

Este ejemplo de regla de ILM utiliza un filtrado avanzado para aplicar el código de borrado a todos los archivos de imagen de más de 1 MB.

> El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Archivos de imagen EC > 1 MB
Hora de referencia	Tiempo de ingesta
Filtro avanzado por tamaño del objeto	Tamaño del objeto superior a 1 MB
Filtros avanzados para Key	• Termina en .jpg • Termina en .png
Ubicaciones	Crea una copia con código de borrado 2+1 usando tres sitios



Dado que esta regla está configurada como la primera de la política, la instrucción de ubicación del código de borrado solo se aplica a los archivos .jpg y .png que superan 1 MB.

Regla 2 de ILM para el ejemplo 3: crea 2 copias replicadas de todos los archivos de imagen restantes

Esta regla de ILM de ejemplo utiliza un filtrado avanzado para especificar que se repliquen los archivos de imagen más pequeños. Porque la primera regla de la política ya ha seleccionado los archivos de imagen de más de 1 MB, esta regla se aplica a los archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	2 copias para los archivos de imagen

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Filtros avanzados para Key	• Termina en .jpg • Termina en .png
Ubicaciones	Crear 2 copias replicadas en dos grupos de almacenamiento

Política de ILM para el ejemplo 3: mejor protección para los archivos de imagen

Esta política de ILM de ejemplo incluye tres reglas:

- La primera regla codifica mediante códigos de borrado todos los archivos de imagen de más de 1 MB.
- La segunda regla crea dos copias de los archivos de imagen restantes (es decir, las imágenes de 1 MB o menos).
- La regla por defecto se aplica a todos los demás objetos (es decir, a cualquier archivo que no sea una imagen).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Reglas y políticas ILM para versiones no actuales de objetos S3 en StorageGRID

Si tienes un bucket de S3 con el versionado activado, puedes gestionar las versiones de objetos no actuales incluyendo reglas en tu política de ILM que usen "Noncurrent time" como tiempo de referencia.

> Si especificas un plazo de retención limitado para los objetos, estos se eliminarán de forma definitiva una vez transcurrido dicho plazo. Asegúrate de entender durante cuánto tiempo se conservarán los objetos.

Como muestra este ejemplo, puedes controlar la cantidad de almacenamiento que ocupan los objetos versionados usando diferentes instrucciones de ubicación para las versiones no actuales de los objetos.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Para realizar una simulación de la política de ILM en una versión no actual de un objeto, debes conocer el UUID o el CBID de la versión del objeto. Para encontrar el UUID y el CBID, usa "búsqueda de metadatos de objetos" mientras el objeto siga siendo actual.

Información relacionada

"Cómo se eliminan los objetos"

Regla 1 de ILM para el ejemplo 4: guardar tres copias durante 10 años

Esta regla de ILM de ejemplo almacena una copia de cada objeto en tres ubicaciones durante 10 años.

Esta regla se aplica a todos los objetos, tengan o no versión.

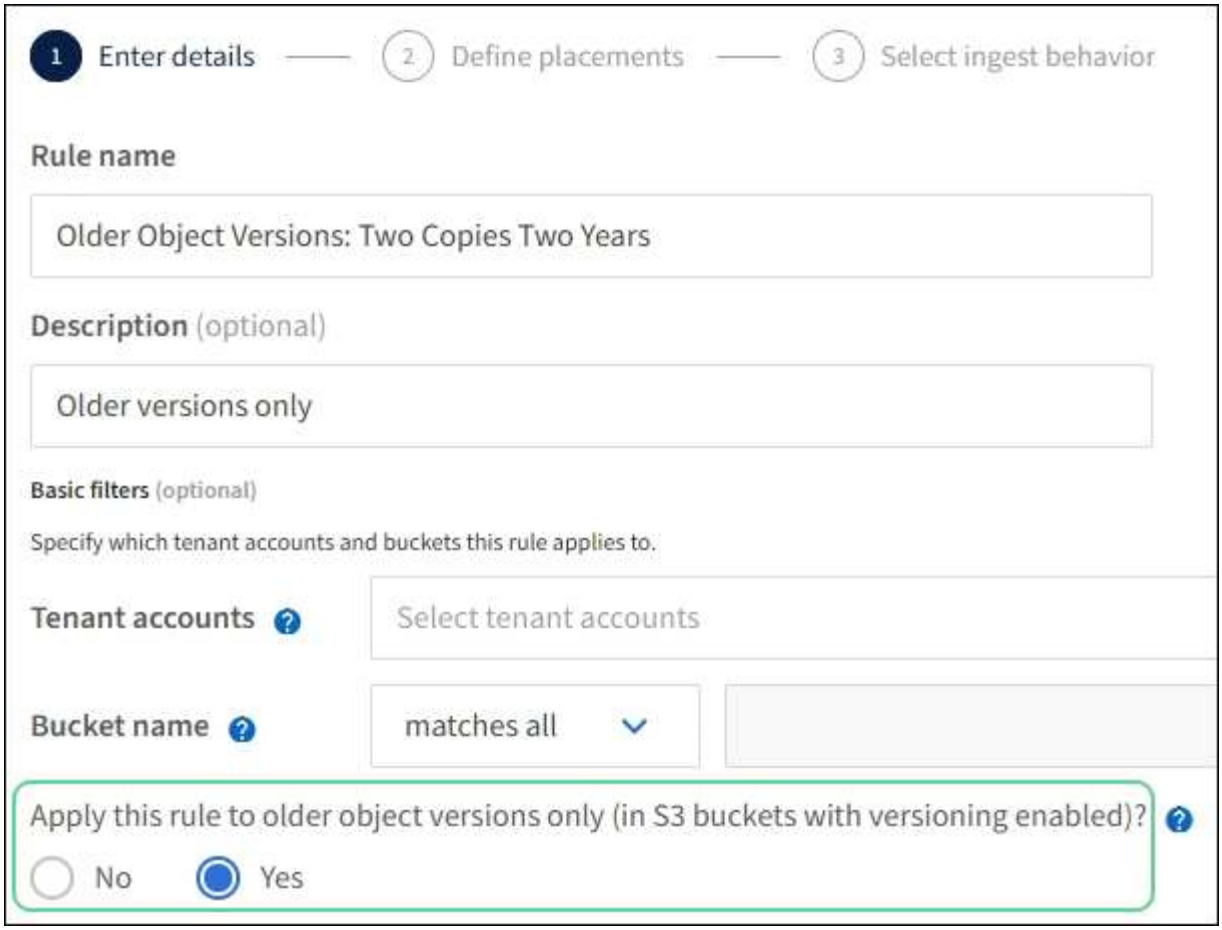
Definición de regla	Valor de ejemplo
Grupos de almacenamiento	Tres grupos de almacenamiento, cada uno compuesto por diferentes centros de datos, llamados Site 1, Site 2 y Site 3.
Nombre de la regla	Tres copias diez años
Hora de referencia	Tiempo de ingesta
Ubicaciones	El día 0, conserva tres copias replicadas durante 10 años (3,652 días), una en el sitio 1, una en el sitio 2 y una en el sitio 3. Al cabo de 10 años, elimina todas las copias del objeto.

Regla 2 de ILM para el ejemplo 4: guarda dos copias de las versiones no actuales durante 2 años

Esta regla de ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto con versiones de S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debes crear otra regla para filtrar cualquier versión que no sea la actual.

Para crear una regla que utilice «Tiempo no actual» como tiempo de referencia, selecciona **Sí** en la pregunta «¿Aplicar esta regla solo a versiones antiguas de objetos (en buckets de S3 con control de versiones activado)?» en el Paso 1 (Introducir detalles) del asistente para crear una regla de ILM. Cuando seleccionas **Sí**, *Tiempo no actual* se selecciona automáticamente como tiempo de referencia y no puedes seleccionar un tiempo de referencia diferente.



En este ejemplo, solo se almacenan dos copias de las versiones no actuales, y dichas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Grupos de almacenamiento	Dos grupos de almacenamiento, cada uno en un centro de datos diferente, Sitio 1 y Sitio 2.
Nombre de la regla	Versiones no actuales: dos copias dos años
Hora de referencia	Tiempo no corriente Se selecciona automáticamente cuando eliges **Sí** en la pregunta, «¿Aplicar esta regla solo a las versiones anteriores de los objetos (en buckets de S3 con control de versiones activado)?» en el asistente para crear una regla de ILM.
Ubicaciones	En el día 0 con respecto al tiempo no actual (es decir, a partir del día en que la versión del objeto pasa a ser la versión no actual), conserva dos copias replicadas de las versiones no actuales del objeto durante 2 años (730 días), una en Site 1 y otra en Site 2. Al cabo de 2 años, elimina las versiones no actuales.

Política de ILM para el ejemplo 4: objetos con versiones de S3

Si deseas gestionar las versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilicen "Noncurrent time" como momento de referencia deben aparecer en la política de ILM antes que las reglas que se aplican a la versión actual del objeto.

Una política de ILM para objetos versionados de S3 podría incluir reglas de ILM como las siguientes:

- Conserva las versiones antiguas (no actuales) de cada objeto durante 2 años, a partir del día en que la versión se volvió no actual.

> Las reglas de «Tiempo no actual» deben aparecer en la política antes que las reglas que se aplican a la versión actual del objeto. De lo contrario, las versiones no actuales del objeto nunca se ajustarán a la regla de «Tiempo no actual».

- En el momento de la importación, crea tres copias replicadas y almacena una copia en cada uno de los tres sitios. Conserva las copias de la versión actual del objeto durante 10 años.

Cuando simulas la política de ejemplo, esperarías que los objetos de prueba se evaluaran de la siguiente manera:

- Cualquier versión de objeto no actual se ajustaría a la primera regla. Si una versión de objeto no actual tiene más de dos años, ILM la elimina de forma permanente (se eliminan de la grid todas las copias de la versión no actual).
- La versión actual del objeto se ajustaría a la segunda regla. Cuando la versión actual del objeto lleva almacenada 10 años, el proceso ILM añade un marcador de eliminación como la versión actual del objeto y convierte la versión anterior del objeto en "no actual". La próxima vez que se realice una evaluación de ILM, esta versión no actual se ajusta a la primera regla. Como resultado, se elimina la copia en el Sitio 3 y las dos copias en el Sitio 1 y el Sitio 2 se almacenan durante 2 años más.

Reglas y política de ILM para el comportamiento de ingesta estricto en StorageGRID

Puedes utilizar un filtro de ubicación y el comportamiento de ingesta Strict en una regla para evitar que se guarden objetos en una ubicación concreta del centro de datos.

En este ejemplo, un cliente con sede en París no desea almacenar algunos objetos fuera de la UE por motivos normativos. El resto de objetos, incluidos todos los de otras cuentas de cliente, pueden almacenarse tanto en el centro de datos de París como en el de EE. UU.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Información relacionada

- "Opciones de ingesta"
- "Crear regla de ILM: seleccionar comportamiento de ingesta"

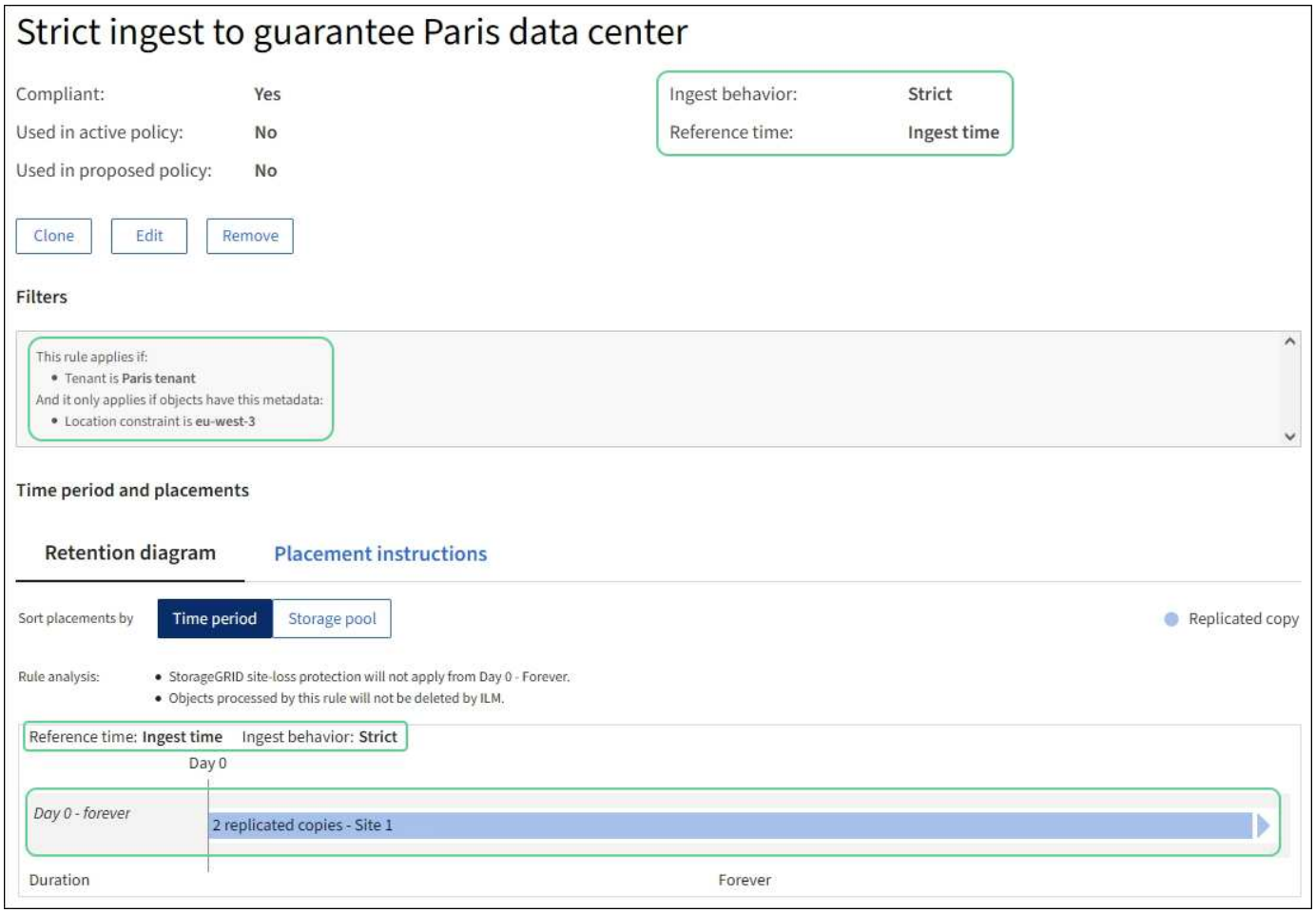
Regla 1 de ILM para el ejemplo 5: ingesta estricta para garantizar el centro de datos de París

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta estricto para garantizar que los objetos guardados por un cliente con sede en París en buckets de S3 con la región configurada como eu-west-3

(París) nunca se almacenen en el centro de datos de EE. UU.

Esta regla se aplica a los objetos que pertenecen al inquilino Paris y que tienen la región del bucket S3 configurada como eu-west-3 (Paris).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Arrendatario de Paris
Filtro avanzado	La restricción de ubicación es eu-west-3
Grupos de almacenamiento	Sede 1 (Paris)
Nombre de la regla	Ingesta estricta para garantizar el centro de datos de París
Hora de referencia	Tiempo de ingesta
Ubicaciones	El día 0, mantén dos copias replicadas para siempre en Site 1 (Paris)
Comportamiento de ingesta	Estricta. Utiliza siempre las ubicaciones de esta regla durante la ingesta. La ingesta falla si no es posible almacenar dos copias del objeto en el centro de datos de París.



Regla 2 de ILM para el ejemplo 5: captura equilibrada para otros objetos

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta equilibrado para ofrecer una eficiencia óptima de ILM para cualquier objeto que no se ajuste a la primera regla. Se almacenarán dos copias de todos los objetos que se ajusten a esta regla: una en el centro de datos de EE. UU. y otra en el centro de datos de París. Si la regla no se puede cumplir de inmediato, se almacenan copias provisionales en cualquier ubicación disponible.

Esta regla se aplica a los objetos que pertenecen a cualquier inquilino y a cualquier región.

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtro avanzado	*No especificado*
Grupos de almacenamiento	Sede 1 (París) y Sede 2 (US)
Nombre de la regla	2 copias 2 centros de datos
Hora de referencia	Tiempo de ingesta
Ubicaciones	El día 0, mantén dos copias replicadas para siempre en dos centros de datos
Comportamiento de ingesta	Equilibrado. Los objetos que cumplen esta regla se colocan según las instrucciones de colocación de la misma, si es posible. De lo contrario, se crean copias provisionales en cualquier ubicación disponible.

Política de ILM para el ejemplo 5: combinación de comportamientos de ingesta

La política de ILM de ejemplo incluye dos reglas que presentan comportamientos de ingesta diferentes.

Una política de ILM que utilice dos comportamientos de ingesta distintos podría incluir reglas de ILM como las siguientes:

- Almacena los objetos que pertenezcan al tenant de Paris y cuya región del bucket de S3 esté configurada como eu-west-3 (Paris) únicamente en el centro de datos de Paris. Falla la ingesta si el centro de datos de Paris no está disponible.
- Almacena todos los demás objetos (incluidos aquellos que pertenecen al inquilino de París pero que tienen una región de bucket diferente) tanto en el centro de datos de EE. UU. como en el centro de datos de París. Realiza copias provisionales en cualquier ubicación disponible si no se puede cumplir la instrucción de ubicación.

Cuando simulas la política de ejemplo, esperas que los objetos de prueba se evalúen de la siguiente manera:

- Cualquier objeto que pertenezca al inquilino de París y cuya región del bucket S3 esté configurada como eu-west-3 se ajusta a la primera regla y se almacena en el centro de datos de París. Porque la primera regla usa Strict ingest, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los Storage Nodes del centro de datos de París no están disponibles, la ingesta falla.

- El resto de objetos se ajustan a la segunda regla, incluidos aquellos que pertenecen al inquilino de Paris y que no tienen la región del bucket de S3 configurada como eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, porque la segunda regla usa Balanced ingest, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Cómo cambiar una política ILM afecta el rendimiento de StorageGRID

Si necesitas cambiar la protección de tus datos o añades nuevos sitios, puedes crear y activar una nueva política de ILM.

Antes de modificar una política, debes comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente el rendimiento general de un sistema StorageGRID.

En este ejemplo, se ha añadido un nuevo sitio de StorageGRID como parte de una ampliación, y es necesario implementar una nueva política ILM activa para almacenar datos en el nuevo sitio. Para implementar una nueva política activa, primero "crear una política". Después, debes "simular" y luego "activar" la nueva política.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Cómo afecta al rendimiento el cambio de una política de ILM

Al activar una nueva política de ILM, el rendimiento de tu sistema StorageGRID podría verse afectado temporalmente, sobre todo si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se trasladen a nuevas ubicaciones.

Al activar una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Antes de activar una nueva política de ILM, revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado ya existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales de recursos mientras se evalúan y se implementan las nuevas ubicaciones.

Para garantizar que una nueva política de ILM no afecte la ubicación de los objetos replicados y con código de borrado ya existentes, puedes "crear una regla de ILM con un filtro de hora de ingesta". Por ejemplo, **Ingest time *is on or after <date and time>***, así que la nueva regla solo se aplica a los objetos incorporados en o después de la fecha y hora especificadas.

Los tipos de cambios en las políticas de ILM que pueden afectar temporalmente el rendimiento de StorageGRID incluyen los siguientes:

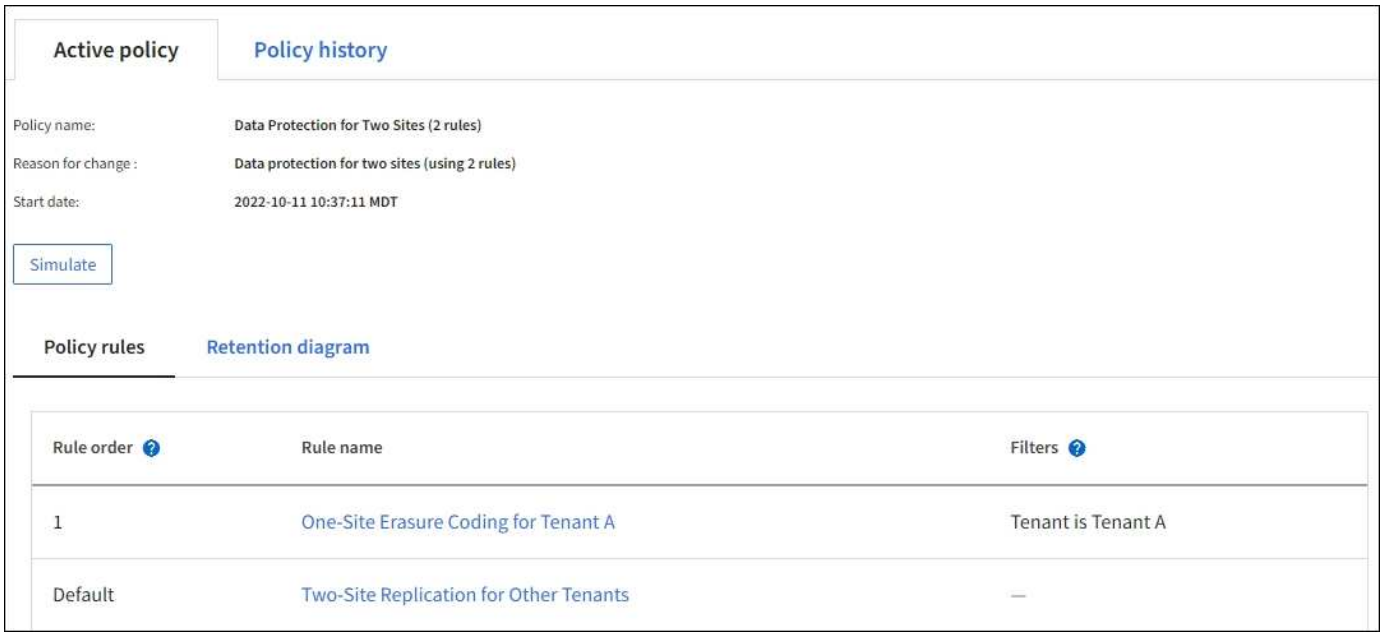
- Aplicar un perfil de código de borrado diferente a los objetos de código de borrado existentes.

  > StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

- Modificar el tipo de copias requeridas para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados a objetos con código de borrado.
- Trasladar copias de objetos existentes a una ubicación completamente diferente; por ejemplo, trasladar un gran número de objetos hacia o desde un Cloud Storage Pool o hacia o desde una sede remota.

Política de ILM activa para el ejemplo 6: protección de datos en dos emplazamientos

En este ejemplo, la política de ILM activa se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas de ILM.



En esta política de ILM, los objetos pertenecientes a Tenant A están protegidos mediante código de borrado 2+1 en un único sitio, mientras que los objetos pertenecientes a todos los demás tenants están protegidos en dos sitios usando replicación de 2 copias.

Regla 1: código de borrado en un solo sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado en un solo sitio para el inquilino A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Sitio 1
Ubicaciones	Codificación de borrado 2+1 en Site 1 desde el día 0 para siempre

Regla 2: replicación en dos sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Replicación en dos sitios para otros tenants
Cuenta de inquilino	Ignorar
Grupos de almacenamiento	Sitio 1 y Sitio 2

Definición de regla	Valor de ejemplo
Ubicaciones	Dos copias replicadas desde el día 0 hasta siempre: una copia en Site 1 y una copia en Site 2.

Política de ILM para el ejemplo 6: protección de datos en tres sedes

En este ejemplo, la política de ILM se está sustituyendo por una nueva política para un sistema StorageGRID de tres sitios.

Tras realizar una ampliación para añadir el nuevo sitio, el administrador de la red creó dos nuevos grupos de almacenamiento: un grupo de almacenamiento para el Sitio 3 y un grupo de almacenamiento que incluye los tres sitios (que no es lo mismo que el grupo de almacenamiento predeterminado All Storage Nodes). Luego, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM, que está diseñada para proteger los datos en los tres sitios.

Cuando se active esta nueva política de ILM, los objetos pertenecientes a Tenant A estarán protegidos mediante código de borrado 2+1 en tres sitios, mientras que los objetos pertenecientes a otros tenants (y los objetos más pequeños pertenecientes a Tenant A) estarán protegidos en tres sitios usando replicación de 3 copias.

Regla 1: código de borrado en tres ubicaciones para Tenant A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado en tres sitios para el tenant A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Las tres sedes (incluye la sede 1, la sede 2 y la sede 3)
Ubicaciones	Codificación de borrado 2+1 en los 3 sitios desde el día 0 para siempre

Regla 2: replicación en tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Replicación en tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Grupos de almacenamiento	Sitio 1, Sitio 2 y Sitio 3
Ubicaciones	Tres copias replicadas desde el día 0 hasta el infinito: una copia en Site 1, una copia en Site 2 y una copia en Site 3.

Activar la política de ILM para el ejemplo 6

Al activar una nueva política de ILM, es posible que los objetos existentes se trasladen a nuevas ubicaciones

o que se creen nuevas copias de los objetos existentes, según las instrucciones de ubicación que figuren en las reglas nuevas o actualizadas.

> Los errores en una política de ILM pueden provocar una pérdida irrecuperable de datos. Revisa detenidamente y simula la política antes de activarla para confirmar que funcionará como esperas.

> Al activar una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Antes de activar una nueva política de ILM, revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado ya existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales de recursos mientras se evalúan y se implementan las nuevas ubicaciones.

¿Qué pasa cuando cambian las instrucciones de codificación de borrado?

En la política de ILM actualmente activa para este ejemplo, los objetos pertenecientes a Tenant A están protegidos mediante código de borrado 2+1 en el sitio 1. En la nueva política de ILM, los objetos pertenecientes a Tenant A estarán protegidos mediante código de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se llevan a cabo las siguientes operaciones de ILM:

- Los nuevos objetos incorporados por Tenant A se dividen en dos fragmentos de datos y se añade un fragmento de paridad. Luego, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen a Tenant A se reevalúan durante el proceso de análisis de ILM en curso. Porque las instrucciones de ubicación de ILM usan un nuevo perfil de código de borrado, se crean fragmentos con código de borrado completamente nuevos y se distribuyen en los tres sitios.

> Los fragmentos 2+1 existentes en el sitio 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

¿Qué ocurre cuando cambian las instrucciones de replicación?

En la política de ILM actualmente activa para este ejemplo, los objetos que pertenecen a otros inquilinos se protegen mediante dos copias replicadas en los grupos de almacenamiento de los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenecen a otros inquilinos se protegerán mediante tres copias replicadas en los grupos de almacenamiento de los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se llevan a cabo las siguientes operaciones de ILM:

- Cuando cualquier inquilino que no sea Tenant A incorpora un nuevo objeto, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Porque las copias existentes del objeto en Site 1 y Site 2 siguen cumpliendo los requisitos de replicación de la nueva regla de ILM, StorageGRID solo necesita crear una nueva copia del objeto para Site 3.

Impacto en el rendimiento de la activación de esta política

Cuando se active la política de ILM de este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles de recursos de grid superiores a los habituales para crear nuevos fragmentos con código de borrado para los objetos existentes de Tenant A y nuevas copias

replicadas en Site 3 para los objetos existentes de otros tenants.

Como consecuencia del cambio en la política de ILM, las solicitudes de lectura y escritura de los clientes podrían experimentar temporalmente latencias superiores a las normales. Las latencias volverán a los niveles normales después de que las instrucciones de ubicación se implementen por completo en toda la grid.

Para evitar problemas con los recursos al activar una nueva política de ILM, puedes usar el filtro avanzado Ingest time en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establece Ingest time en un valor mayor o igual a la hora aproximada en la que la nueva política entrará en vigor para asegurarte de que los objetos existentes no se trasladen innecesariamente.

Ponte en contacto con el soporte técnico si necesitas reducir o aumentar la velocidad a la que se procesan los objetos tras un cambio en la política de ILM.

Política ILM compatible para S3 Object Lock en StorageGRID

Puedes utilizar el depósito de S3, las reglas de ILM y la política de ILM de este ejemplo como punto de partida a la hora de definir una política de ILM que cumpla los requisitos de protección y retención de los objetos en depósitos con S3 Object Lock habilitado.

Si has utilizado la función de Compliance heredada en versiones anteriores de StorageGRID, también puedes usar este ejemplo para gestionar cualquier bucket existente que tenga activada la función de Compliance heredada.

Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Información relacionada

- "Gestiona objetos con S3 Object Lock"
- "Crear una política de ILM"

Bucket y objetos para el ejemplo de S3 Object Lock

En este ejemplo, una cuenta de inquilino de S3 llamada Bank of ABC ha usado el Tenant Manager para crear un bucket con S3 Object Lock activado para guardar registros bancarios críticos.

Definición de bucket	Valor de ejemplo
Nombre de la cuenta del inquilino	Banco ABC
Nombre del bucket	registros bancarios
Región de bucket	us-east-1 (predeterminado)

Cada objeto y cada versión de objeto que se añada al bucket bank-records usará los siguientes valores para `retain-until-date` y `legal hold`.

Configuración de cada objeto	Valor de ejemplo
`retain-until-date`	«2030-12-30T23:59:59Z» (30 de diciembre de 2030) Cada versión de objeto tiene su propio `retain-until-date` valor. Este valor se puede aumentar, pero no disminuir.
`legal hold`	"OFF" (No está en vigor) Se puede aplicar o levantar una retención legal sobre cualquier versión de un objeto en cualquier momento durante el periodo de retención. Si un objeto está sujeto a una retención legal, no se puede eliminar aunque se haya alcanzado el `retain-until-date`.

Regla 1 de ILM para S3 Object Lock: perfil de código de borrado con coincidencia de buckets

Esta regla de ILM de ejemplo se aplica únicamente a la cuenta de cliente de S3 denominada Bank of ABC. Coincide con cualquier objeto en el bucket `bank-records` y luego utiliza el código de borrado para almacenar el objeto en los Storage Nodes de tres sitios de centros de datos usando un perfil de código de borrado 6+3. Esta regla cumple los requisitos de los buckets con S3 Object Lock habilitado: se mantiene una copia en los Storage Nodes desde el día 0 para siempre, usando la hora de ingesta como referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla de cumplimiento: Objetos EC en el bucket bank-records - Bank of ABC
Cuenta de inquilino	Banco ABC
Nombre del bucket	`bank-records`
Filtro avanzado	Tamaño del objeto (MB) superior a 1 **Nota:** Este filtro garantiza que no se utilice el código de borrado para los objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 almacena para siempre
Perfil de código de borrado	• Crea una copia con código de borrado en los nodos de almacenamiento en tres centros de datos • Utiliza un esquema de código de borrado 6+3

Regla n.º 2 de ILM para el ejemplo de S3 Object Lock: regla no conforme

Esta regla ILM de ejemplo almacena inicialmente dos copias replicadas del objeto en Storage Nodes. Después de un año, almacena una copia en un Cloud Storage Pool para siempre. Como esta regla usa un Cloud Storage Pool, no cumple y no se aplicará a los objetos en los buckets con S3 Object Lock habilitado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla incumplida: usar Cloud Storage Pool
${post_edited_translations.segment}	No especificado
Nombre del bucket	No se especifica, pero solo se aplicará a los buckets que no tengan activado S3 Object Lock (o la función heredada de Compliance).
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Ubicaciones	• El día 0, mantén dos copias replicadas en los nodos de almacenamiento en Data Center 1 y Data Center 2 durante 365 días • Después de 1 año, conserva una copia replicada en un Cloud Storage Pool para siempre

Regla 3 de ILM para S3 Object Lock: regla predeterminada

Esta regla de ILM de ejemplo copia los datos de los objetos a grupos de almacenamiento en dos centros de datos. Esta regla conforme está diseñada para ser la regla predeterminada en la política de ILM. No incluye ningún filtro, no utiliza el tiempo de referencia Noncurrent y cumple los requisitos de los buckets con S3 Object Lock habilitado: se conservan dos copias de los objetos en los Storage Nodes desde el día 0 hasta siempre, utilizando Ingest como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla de cumplimiento predeterminada: dos copias en dos centros de datos
Cuenta de inquilino	No especificado
Nombre del bucket	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 y de forma permanente, mantén dos copias replicadas: una en los nodos de almacenamiento en Data Center 1 y otra en los nodos de almacenamiento en Data Center 2.

Ejemplo de política de ILM conforme a los requisitos para S3 Object Lock

Para crear una política de ILM que proteja de forma eficaz todos los objetos de tu sistema, incluidos los que se encuentran en buckets con S3 Object Lock activado, debes seleccionar reglas de ILM que cumplan los requisitos de almacenamiento de todos los objetos. Luego, tienes que simular y activar la política.

Agrega reglas a la política

En este ejemplo, la política de ILM incluye tres reglas de ILM, en el siguiente orden:

1. Una regla conforme que utiliza código de borrado para proteger objetos de más de 1 MB en un bucket específico con S3 Object Lock activado. Los objetos se almacenan en Storage Nodes desde el día 0 hasta siempre.
2. Una regla no conforme que crea dos copias replicadas de un objeto en Storage Nodes durante un año y luego mueve una copia del objeto a un Cloud Storage Pool para siempre. Esta regla no se aplica a los buckets con S3 Object Lock habilitado porque utiliza un Cloud Storage Pool.
3. La regla de cumplimiento predeterminada que crea dos copias replicadas de objetos en los Storage Nodes desde el día 0 y para siempre.

Simular la política

Una vez que hayas añadido reglas a tu política, hayas elegido una regla de cumplimiento predeterminada y hayas organizado el resto de reglas, debes simular la política probando objetos del bucket en el que se ha habilitado S3 Object Lock y de otros buckets. Por ejemplo, al simular la política de ejemplo, esperarías que los objetos de prueba se evaluaran de la siguiente manera:

- La primera regla solo coincidirá con los objetos de prueba que sean mayores de 1 MB en el bucket bank-records para el inquilino Bank of ABC.
- La segunda regla coincidirá con todos los objetos en todos los buckets no conformes de todas las demás cuentas de inquilino.
- La regla predeterminada coincidirá con estos objetos:
  - Objetos de 1 MB o menos en el bucket bank-records para el tenant Bank of ABC.
  - Objetos en cualquier otro depósito que tenga S3 Object Lock activado para todas las demás cuentas de inquilino.

Activa la política

Cuando estés completamente seguro de que la nueva política protege los datos de los objetos como esperabas, puedes activarla.

Cómo interactúan el ciclo de vida de los buckets S3 y la política ILM en StorageGRID

En función de la configuración del ciclo de vida, los objetos siguen los parámetros de retención del ciclo de vida del bucket de S3 o de una política de ILM.

Ejemplo de cómo el ciclo de vida de un bucket tiene prioridad sobre la política de ILM

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conserva X copias durante 20 días
- Regla basada en la referencia de la hora de ingesta (por defecto): el día 0, conserva X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Se ha importado un objeto denominado "docs/text". Coincide con el filtro de ciclo de vida del bucket que tiene el prefijo "docs/".
  - Después de 100 días se crea un marcador de eliminación y "docs/text" pasa a ser no actual.
  - Después de 5 días, es decir, un total de 105 días desde la incorporación, "docs/text" se elimina.
  - Después de 95 días, un total de 200 días desde la ingestión y 100 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación caducado.
- Se ha importado un objeto denominado "video/movie". No coincide con el filtro y utiliza la política de retención de ILM.
  - Después de 50 días, se crea un marcador de eliminación y "video/movie" pasa a estar no actual.
  - Después de 20 días, es decir, un total de 70 días desde la ingesta, "video/movie" se elimina.
  - Después de 30 días, es decir, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, el marcador de eliminación caducado se elimina.

Ejemplo de ciclo de vida de un bucket que, de forma implícita, se mantiene indefinidamente

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conserva X copias durante 20 días
- Regla basada en la referencia de la hora de ingesta (por defecto): el día 0, conserva X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Resultado

- Se ha importado un objeto denominado "docs/text". Coincide con el filtro de ciclo de vida del bucket que tiene el prefijo "docs/".

  La acción `Expiration` solo se aplica a los marcadores de eliminación caducados, lo que implica conservar todo lo demás para siempre (empezando por "docs/").

Los marcadores de eliminación que empiezan por "docs/" se eliminan cuando caducan.

- Se ha importado un objeto denominado "video/movie". No coincide con el filtro y utiliza la política de retención de ILM.
  - Después de 50 días, se crea un marcador de eliminación y "video/movie" pasa a estar no actual.
  - Después de 20 días, es decir, un total de 70 días desde la ingesta, "video/movie" se elimina.
  - Después de 30 días, es decir, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, el marcador de eliminación caducado se elimina.

Ejemplo de cómo utilizar el ciclo de vida de los buckets para duplicar el ILM y eliminar los marcadores de eliminación caducados

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conserva X copias durante 20 días
- Regla basada en la referencia de la hora de importación (por defecto): el día 0, conserva X copias para siempre

Ciclo de vida del bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- La política de ILM se duplica en el ciclo de vida del bucket.
  - La regla «para siempre» de la política ILM está diseñada para eliminar objetos manualmente y limpiar las versiones obsoletas al cabo de 20 días. Por consiguiente, la regla basada en la fecha de ingesta conservará para siempre los marcadores de eliminación caducados.
  - El ciclo de vida del bucket reproduce el comportamiento de la política de ILM mientras añade `"ExpiredObjectDeleteMarker": true`, que elimina los marcadores de eliminación una vez que han caducado
- Se ingiere un objeto. La ausencia de filtro significa que el ciclo de vida del bucket se aplica a todos los objetos y anula la configuración de retención de ILM.
  - Cuando un inquilino envía una solicitud de eliminación de un objeto, se crea un marcador de eliminación y el objeto pasa a estar no actual.
  - Después de 20 días, el objeto no actual se elimina y el marcador de eliminación caduca.
  - Poco después, se elimina el marcador de eliminación caducado.