# Administrar objetos con ILM

StorageGRID software

NetApp
December 03, 2025

# Tabla de contenidos

# Administrar objetos con ILM

## Administrar objetos con ILM

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

### Acerca de estas instrucciones

El diseño y la implementación de reglas y políticas de ILM requieren una planificación cuidadosa. Debe comprender sus requisitos operativos, la topología de su sistema StorageGRID , sus 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.

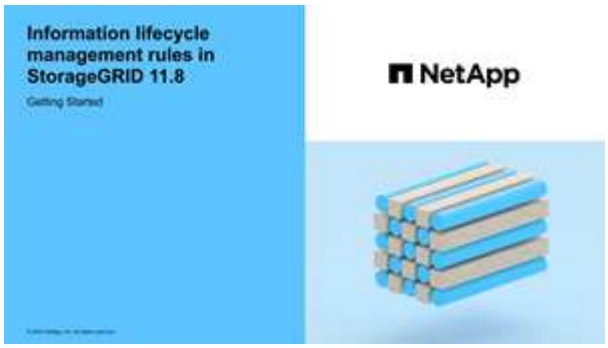
Utilice estas instrucciones para:

- Obtenga más información sobre StorageGRID ILM, incluido"Cómo funciona ILM a lo largo de la vida de un objeto" .
- Aprenda a configurar"grupos de almacenamiento" ,"Grupos de almacenamiento en la nube" , y"Reglas de ILM" .
- Aprenda cómo"crear, simular y activar una política ILM" que protegerá los datos de los objetos en uno o más sitios.
- Aprenda cómo"Administrar objetos con S3 Object Lock" , lo que ayuda a garantizar que los objetos en depósitos S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo específico.

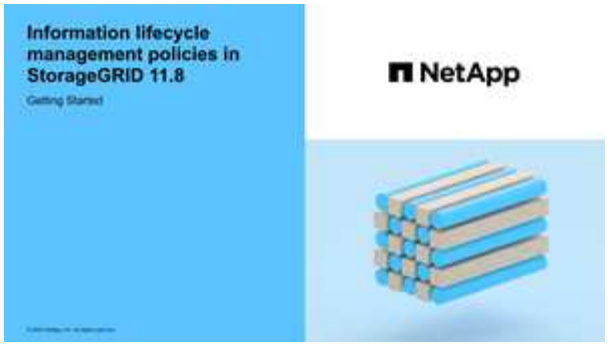
### Más información

Para obtener más información, revise estos videos:

- "Vídeo: Resumen de las reglas de ILM" .




- "Vídeo: Resumen de las políticas de ILM"




# ILM y ciclo de vida de los objetos

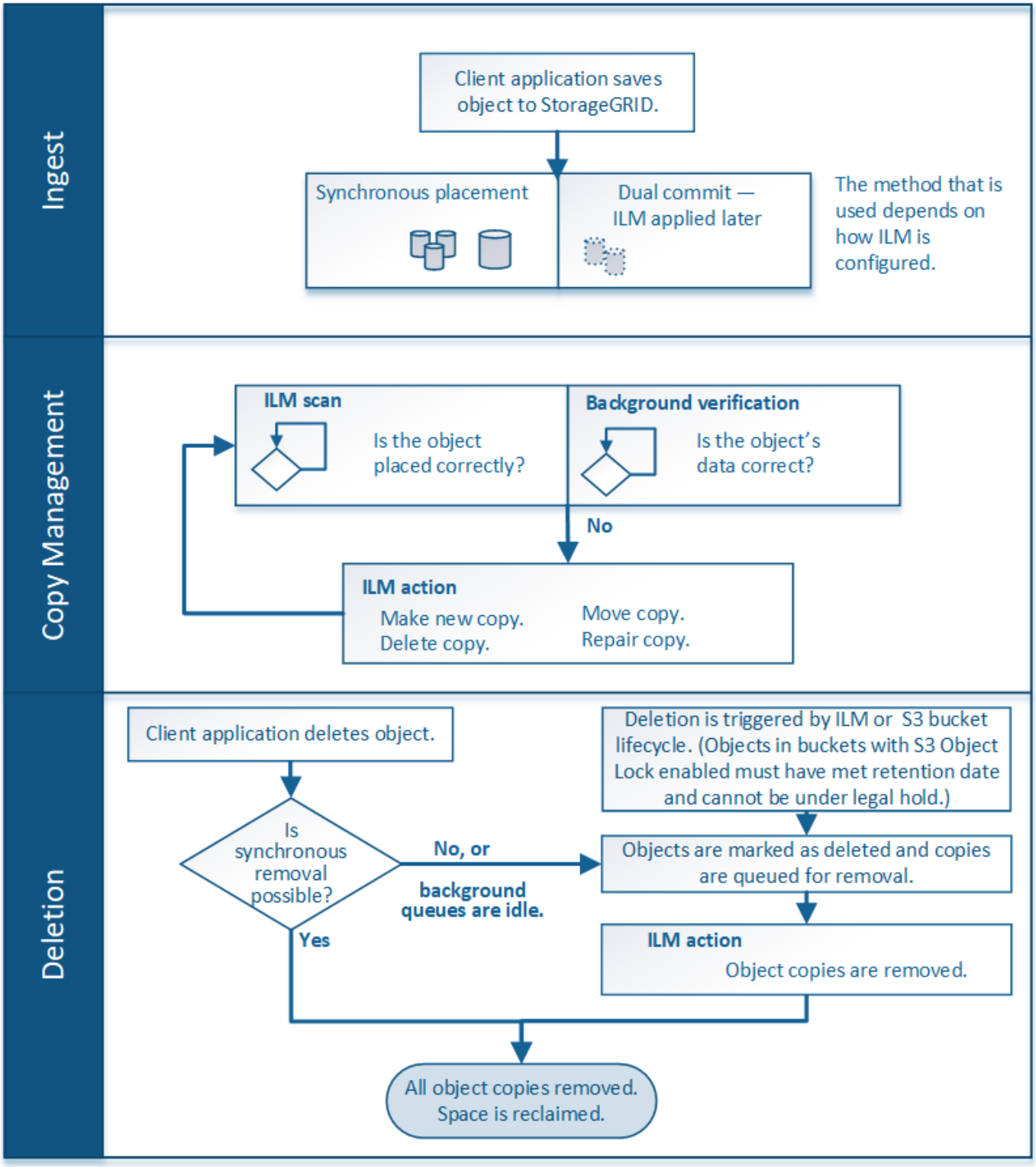
## Cómo funciona ILM a lo largo de la vida de un objeto

Comprender cómo StorageGRID utiliza ILM para administrar objetos durante cada etapa de su vida puede ayudarlo a diseñar una política más efectiva.

- **Ingesta**: la ingesta comienza cuando una aplicación cliente S3 establece una conexión para guardar un objeto en el sistema StorageGRID y se completa cuando StorageGRID devuelve un mensaje de "ingesta exitosa" al cliente. Los datos de los objetos se protegen durante la ingesta ya sea aplicando instrucciones ILM inmediatamente (colocación sincrónica) o creando copias provisionales y aplicando ILM más tarde (confirmación dual), dependiendo de cómo se especificaron los requisitos de ILM.
- **Administración de copias**: después de crear la cantidad y el tipo de copias de objetos que se especifican en las instrucciones de ubicación de ILM, StorageGRID administra las ubicaciones de los objetos y los protege contra pérdidas.
  - **Escaneo y evaluación de ILM**: StorageGRID escanea continuamente la lista de objetos almacenados en la red y verifica si las copias actuales cumplen con los requisitos de ILM. Cuando se requieren diferentes tipos, números o ubicaciones de copias de objetos, StorageGRID crea, elimina o mueve copias según sea necesario.
  - **Verificación en segundo plano**: StorageGRID realiza continuamente una verificación en segundo plano para comprobar la integridad de los datos de los objetos. Si se encuentra un problema, StorageGRID crea automáticamente una nueva copia del objeto o un fragmento de objeto con código de borrado de reemplazo en una ubicación que cumpla con los requisitos ILM actuales. Ver "Verificar la integridad del objeto" .
- **Eliminación de objetos**: la administración de un objeto finaliza cuando se eliminan todas las copias del sistema StorageGRID . Los objetos se pueden eliminar como resultado de una solicitud de eliminación por parte de un cliente, o como resultado de una eliminación por parte de ILM o una eliminación causada por la expiración del ciclo de vida de un bucket de S3.

> ⓘ Los objetos de un bucket que tiene habilitado el bloqueo de objetos S3 no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención pero aún no se cumple.

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




## Cómo se ingieren los objetos

### Opciones de ingesta

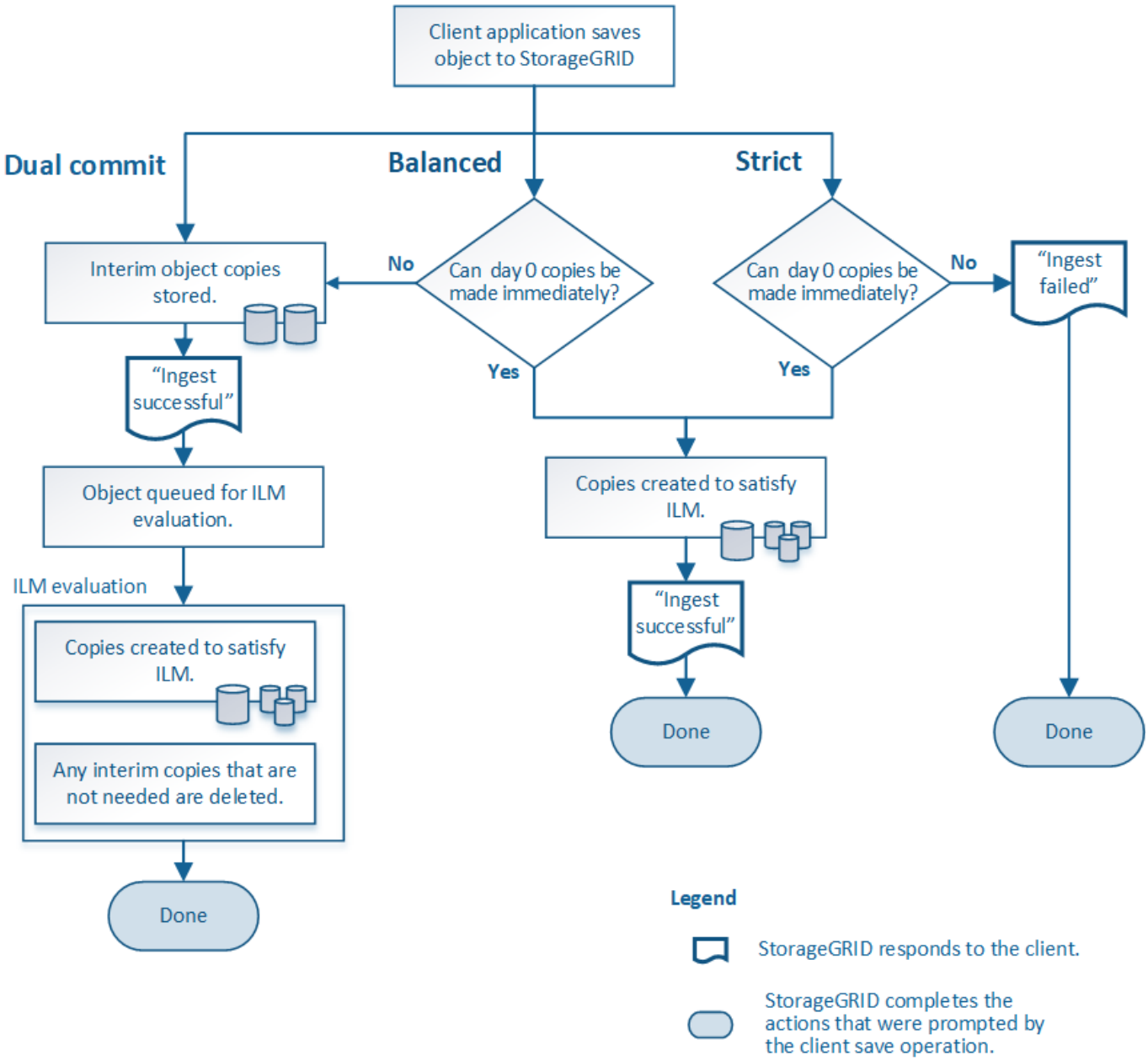
Cuando crea una regla ILM, especifica una de tres opciones para proteger objetos durante la ingesta: Confirmación dual, Estricta o Equilibrada.

Según su elección, StorageGRID realiza copias provisionales y pone en cola los objetos para una evaluación

ILM posterior, o utiliza la ubicación sincrónica y realiza copias inmediatamente para cumplir con los requisitos de ILM.

#### Diagrama de flujo de opciones de ingesta

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




#### Compromiso dual

Cuando selecciona la opción de confirmación dual, StorageGRID realiza inmediatamente copias de objetos provisionales en dos nodos de almacenamiento diferentes y devuelve un mensaje de "ingesta exitosa" al cliente. El objeto se pone en cola para la evaluación de ILM y luego se realizan copias que cumplen con las instrucciones de ubicación de la regla. Si la política ILM no se puede procesar inmediatamente después de la confirmación dual, la protección contra pérdida del sitio podría llevar tiempo.

Utilice la opción de confirmación dual en cualquiera de estos casos:

- Está utilizando reglas ILM de múltiples sitios y la latencia de ingesta del cliente es su consideración principal. Al usar la confirmación dual, debe asegurarse de que su cuadrícula pueda realizar el trabajo adicional de crear y eliminar las copias de confirmación dual si no satisfacen ILM. Específicamente:
  - La carga en la red debe ser lo suficientemente baja para evitar un retraso en la ILM.
  - La red debe tener recursos de hardware excedentes (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Está utilizando reglas ILM de varios sitios y la conexión WAN entre los sitios generalmente tiene alta latencia o ancho de banda limitado. En este escenario, el uso de la opción de confirmación dual puede ayudar a evitar tiempos de espera del cliente. Antes de elegir la opción de confirmación dual, debe probar la aplicación cliente con cargas de trabajo realistas.

#### Equilibrado (predeterminado)

Cuando selecciona la opción Equilibrado, StorageGRID también utiliza la ubicación sincrónica en la ingesta y realiza inmediatamente todas las copias especificadas en las instrucciones de ubicación de la regla. A diferencia de la opción Estricta, si StorageGRID no puede realizar todas las copias inmediatamente, utiliza la confirmación dual en su lugar. Si la política ILM utiliza ubicaciones en varios sitios y no se puede lograr una protección inmediata contra pérdida de sitios, se activa la alerta **Ubicación ILM inalcanzable**.

Utilice la opción Equilibrado para lograr la mejor combinación de protección de datos, rendimiento de la red y éxito de ingesta. Equilibrado es la opción predeterminada en el asistente Crear regla ILM.

#### Estricto

Cuando selecciona la opción Estricto, StorageGRID utiliza la ubicación sincrónica en la ingesta y realiza inmediatamente todas las copias de objetos especificadas en las instrucciones de ubicación de la regla. La ingesta falla si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento requerida no está disponible temporalmente. El cliente debe volver a intentar la operación.

Utilice la opción Estricto si tiene un requisito operativo o reglamentario para almacenar inmediatamente objetos solo en las ubicaciones descritas en la regla ILM. Por ejemplo, para satisfacer un requisito reglamentario, es posible que necesite utilizar la opción Estricto y un filtro avanzado de Restricción de ubicación para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Ver "Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto" .

### Ventajas, desventajas y limitaciones de las opciones de ingesta

Comprender las ventajas y desventajas de cada una de las tres opciones para proteger datos en la ingesta (equilibrada, estricta o confirmación dual) puede ayudarlo a decidir cuál seleccionar para una regla ILM.

Para obtener una descripción general de las opciones de ingesta, consulte"Opciones de ingesta" .

#### Ventajas de las opciones Equilibrada y Estricta

En comparación con la confirmación dual, que crea copias provisionales durante la ingesta, las dos opciones de ubicación sincrónica pueden proporcionar las siguientes ventajas:

- **Mejor seguridad de los datos**: los datos de los objetos se protegen inmediatamente como se especifica en las instrucciones de ubicación de las reglas ILM, que se pueden configurar para proteger contra una amplia variedad de condiciones de falla, incluida la falla de más de una ubicación de almacenamiento. La confirmación dual solo puede proteger contra la pérdida de una única copia local.

- **Operación de red más eficiente**: cada objeto se procesa solo una vez, a medida que se ingiere. Debido a que el sistema StorageGRID no necesita rastrear ni eliminar copias provisionales, hay menos carga de procesamiento y se consume menos espacio de base de datos.
- **(Equilibrado) Recomendado**: La opción Equilibrada proporciona una eficiencia ILM óptima. Se recomienda usar la opción Equilibrado a menos que se requiera un comportamiento de ingesta estricto o la cuadrícula cumpla con todos los criterios para usar la confirmación dual.
- **(Estricta) Certeza sobre las ubicaciones de los objetos**: La opción Estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de ubicación de la regla ILM.

#### Desventajas de las opciones equilibrada y estricta

En comparación con la confirmación dual, las opciones equilibrada y estricta tienen algunas desventajas:

- **Ingestas de cliente más prolongadas**: las latencias de ingesta de cliente pueden ser más prolongadas. Cuando se utilizan las opciones Equilibrado o Estricto, no se devuelve un mensaje de "ingesta exitosa" al cliente hasta que se crean y almacenan todos los fragmentos codificados de borrado o copias replicadas. Sin embargo, lo más probable es que los datos de los objetos lleguen a su ubicación final mucho más rápido.
- **(Estricto) Mayores tasas de errores de ingesta**: con la opción Estricto, la ingesta falla siempre que StorageGRID no pueda realizar inmediatamente todas las copias especificadas en la regla ILM. Es posible que observe altas tasas de errores de ingesta si una ubicación de almacenamiento requerida está temporalmente fuera de línea o si los problemas de red causan demoras en la copia de objetos entre sitios.
- **(Estricto) Las ubicaciones de carga multiparte de S3 podrían no ser las esperadas en algunas circunstancias**: con Estricto, se espera que los objetos se coloquen como lo describe la regla ILM o que la ingesta falle. Sin embargo, con una carga multiparte de S3, ILM se evalúa para cada parte del objeto a medida que se ingiere y para el objeto como un todo cuando se completa la carga multiparte. En las siguientes circunstancias, esto podría dar lugar a ubicaciones diferentes a las esperadas:
  - **Si ILM cambia mientras una carga multiparte de S3 está en progreso**: debido a que cada parte se coloca de acuerdo con la regla que está activa cuando se ingiere la parte, es posible que algunas partes del objeto no cumplan con los requisitos actuales de ILM cuando se complete la carga multiparte. En estos casos la ingesta del objeto no falla. En cambio, cualquier pieza que no esté colocada correctamente se pone en cola para una reevaluación de ILM y se mueve a la ubicación correcta más tarde.
  - **Cuando las reglas ILM filtran por tamaño**: al evaluar ILM para una pieza, StorageGRID filtra por el tamaño de la pieza, no por el tamaño del objeto. Esto significa que partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su totalidad. 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 momento de la ingesta 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 mueven a DC1.
- **(Estricto) La ingesta no falla cuando se actualizan las etiquetas o los metadatos de los objetos y no se pueden realizar las nuevas ubicaciones requeridas**: con Estricto, se espera que los objetos se coloquen como lo describe la regla ILM o que la ingesta falle. Sin embargo, cuando se actualizan los metadatos o las etiquetas de un objeto que ya está almacenado en la cuadrícula, el objeto no se vuelve a ingerir. Esto significa que cualquier cambio en la ubicación de los objetos que se active mediante la actualización no se realiza de inmediato. Los cambios de ubicación se realizan cuando el ILM se vuelve a evaluar mediante procesos ILM en segundo plano normales. Si no se pueden realizar los cambios de ubicación requeridos (por ejemplo, porque la nueva ubicación requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que sea posible realizar los cambios de ubicación.

#### Limitaciones en la ubicación de objetos con las opciones Equilibrado y Estricto

Las opciones Equilibrado o Estricto no se pueden usar para reglas ILM que tengan alguna de estas instrucciones de ubicación:

- Ubicación en un grupo de almacenamiento en la nube el día 0.
- Ubicaciones en un grupo de almacenamiento en la nube cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones existen porque StorageGRID no puede realizar copias de manera sincrónica a un grupo de almacenamiento en la nube, y un tiempo de creación definido por el usuario podría resolverse en el presente.

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

Tanto su regla ILM como su elección de consistencia afectan cómo se protegen los objetos. Estas configuraciones pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla ILM afecta la ubicación inicial de las copias de objetos, mientras que la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto. Debido a que StorageGRID requiere acceso a los datos y 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 brindar una mejor protección de datos inicial y respuestas del sistema más predecibles.

A continuación se muestra un breve resumen de los valores de consistencia disponibles en StorageGRID:

- **Todos**: Todos los nodos reciben metadatos del objeto inmediatamente o la solicitud fallará.
- **Fuerte-global**: Los metadatos de los objetos se distribuyen inmediatamente a todos los sitios. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
- **Sitio fuerte**: los metadatos del objeto se distribuyen inmediatamente a otros nodos del sitio. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
- **Lectura después de nueva escritura**: proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los buckets S3, úselo solo cuando sea necesario (por ejemplo, para un bucket que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

> Antes de seleccionar un valor de consistencia,"Lea la descripción completa de la consistencia" . Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

#### Ejemplo de cómo la consistencia y las reglas ILM pueden interactuar

Supongamos que tiene una cuadrícula de dos sitios con la siguiente regla ILM y la siguiente consistencia:

- **Regla ILM**: Crea dos copias de objetos, una en el sitio local y otra en un sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia**: Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en la red, StorageGRID realiza copias de los objetos y distribuye metadatos a ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra pérdida en el momento del mensaje de ingesta exitosa. Por ejemplo, si el sitio local se pierde poco después de la ingesta, aún existen copias de los datos del objeto y de los metadatos del objeto en el sitio remoto. El objeto es completamente recuperable.

Si, en cambio, utilizara la misma regla ILM y la consistencia del sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se repliquen en el sitio remoto 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. No se puede recuperar el objeto.

La interrelación entre la consistencia y las reglas ILM puede ser compleja. Comuníquese con NetApp si necesita ayuda.

**Información relacionada**

"Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"

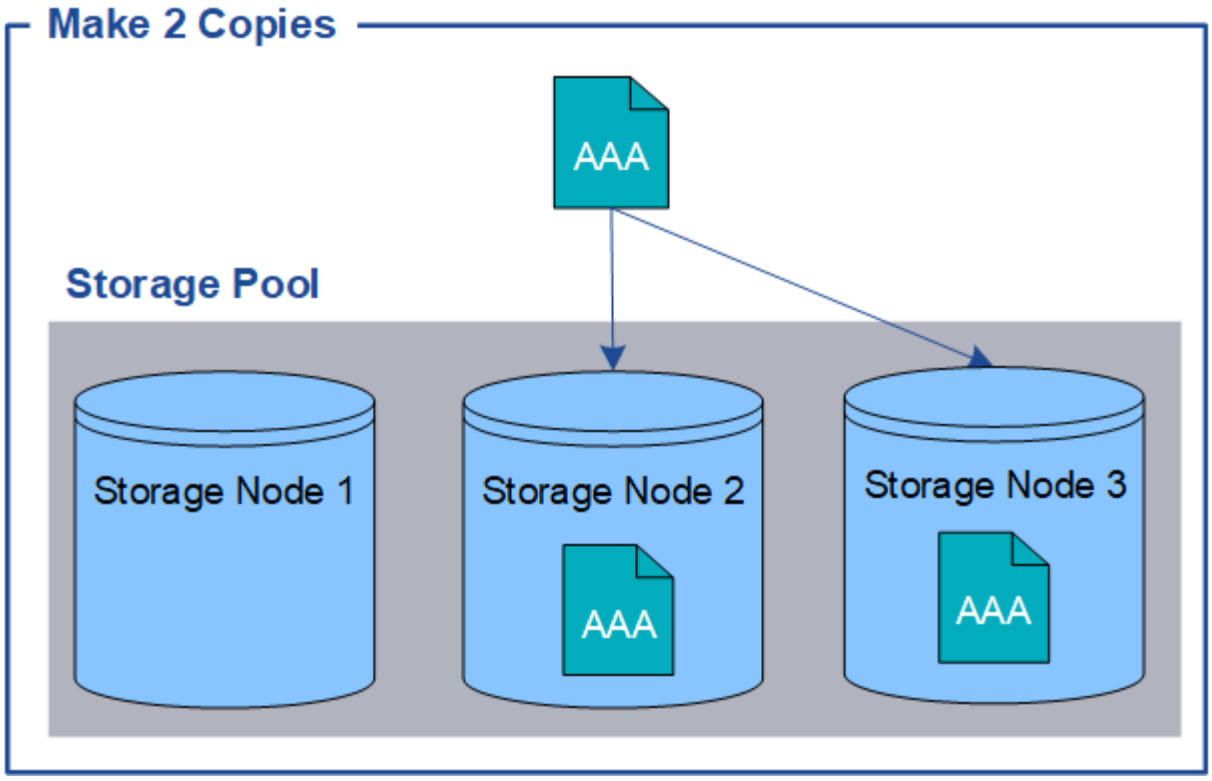
## Cómo se almacenan los objetos (codificación de replicación o borrado)

### ¿Qué es la replicación?

La replicación es uno de los dos métodos utilizados por StorageGRID para almacenar datos de objetos (la codificación de borrado es el otro método). Cuando los objetos coinciden con una regla ILM que utiliza replicación, el sistema crea copias exactas de los datos de los objetos y almacena las copias en los nodos de almacenamiento.

Cuando configura una regla ILM para crear copias replicadas, especifica cuántas copias se deben crear, dónde se deben colocar esas copias y durante cuánto tiempo se deben almacenar las copias en cada ubicación.

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




Cuando StorageGRID hace coincidir objetos con esta regla, crea dos copias del objeto y coloca cada copia en un nodo de almacenamiento diferente en el grupo de almacenamiento. Las dos copias se pueden colocar en cualquiera de los dos de los tres nodos de almacenamiento disponibles. En este caso, la regla colocó copias de objetos en los nodos de almacenamiento 2 y 3. Dado que hay dos copias, el objeto se puede recuperar si alguno de los nodos del grupo de almacenamiento falla.

> StorageGRID solo puede almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento determinado. Si su red incluye tres nodos de almacenamiento y crea una regla ILM de 4 copias, solo se realizarán tres copias: una copia para cada nodo de almacenamiento. La alerta **Colocación ILM inalcanzable** se activa para indicar que la regla ILM no se pudo aplicar por completo.

**Información relacionada**

- "¿Qué es la codificación de borrado?"
- "¿Qué es un pool de almacenamiento?"
- "Habilite la protección contra pérdida de sitios mediante codificación de replicación y borrado"

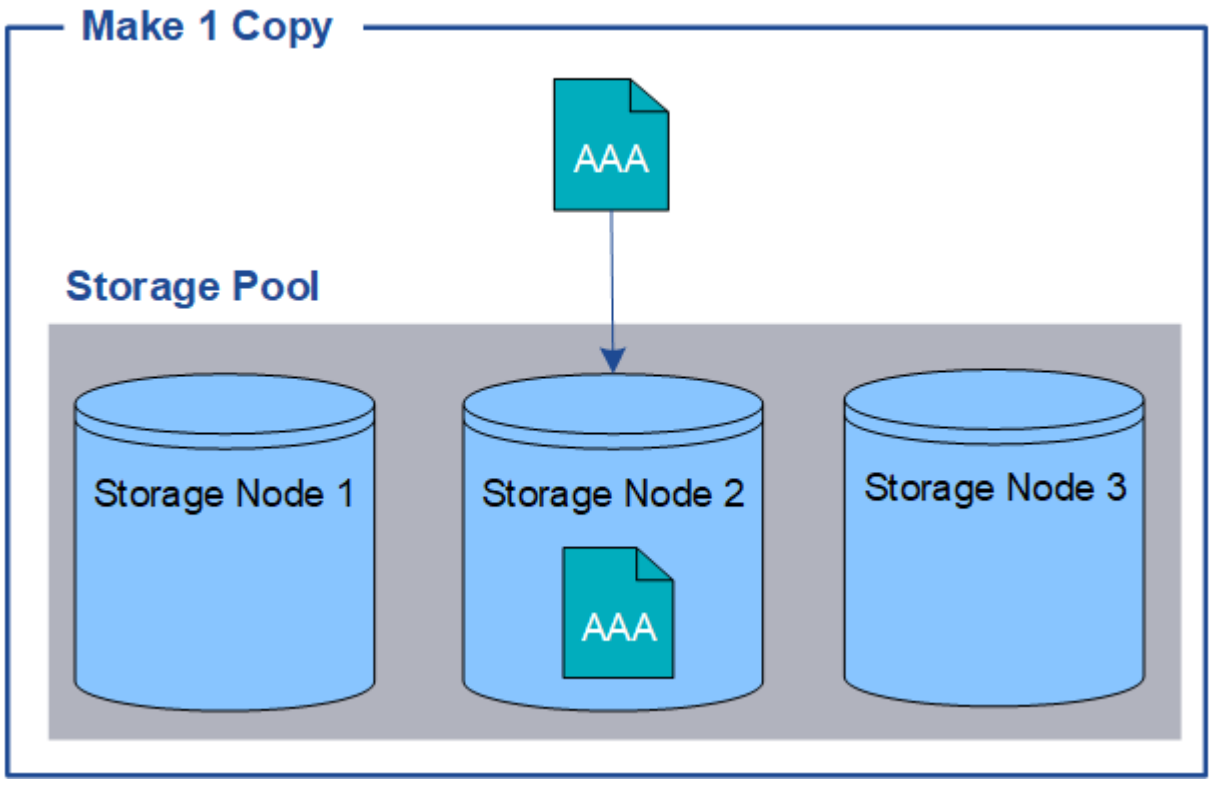
**Por qué no debería utilizar la replicación de copia única**

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

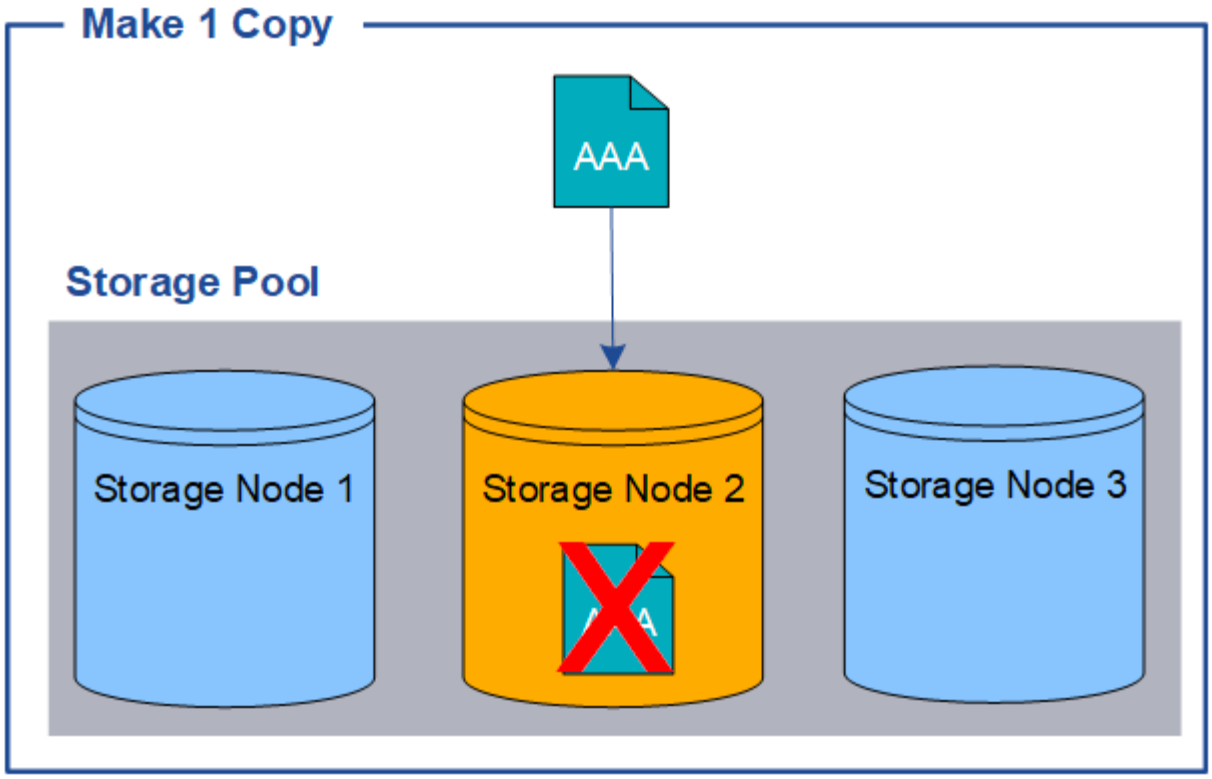
> No utilice una regla ILM que cree solo una copia replicada por un período de tiempo determinado. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

En el siguiente ejemplo, la regla ILM Realizar 1 copia especifica que una copia replicada de un objeto se

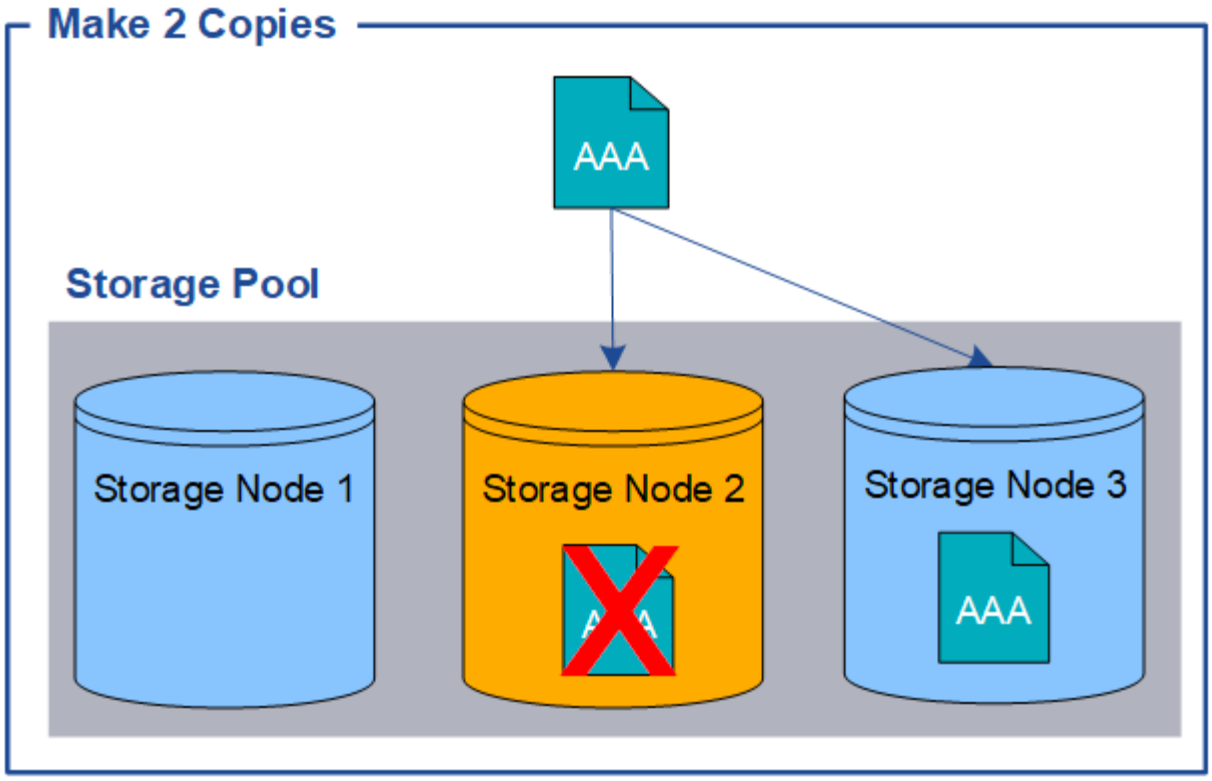
coloque en un grupo de almacenamiento que contenga tres nodos de almacenamiento. Cuando se ingiere un objeto que coincide con esta regla, StorageGRID coloca una única copia en un solo nodo de almacenamiento.




Cuando una regla 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, perderá temporalmente el acceso al objeto AAA siempre que el Nodo de almacenamiento 2 esté fuera de línea, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA por completo si falla el Nodo de almacenamiento 2.




Para evitar perder datos de objetos, siempre debe hacer al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, aún podrá acceder al objeto si un nodo de almacenamiento falla o se desconecta.



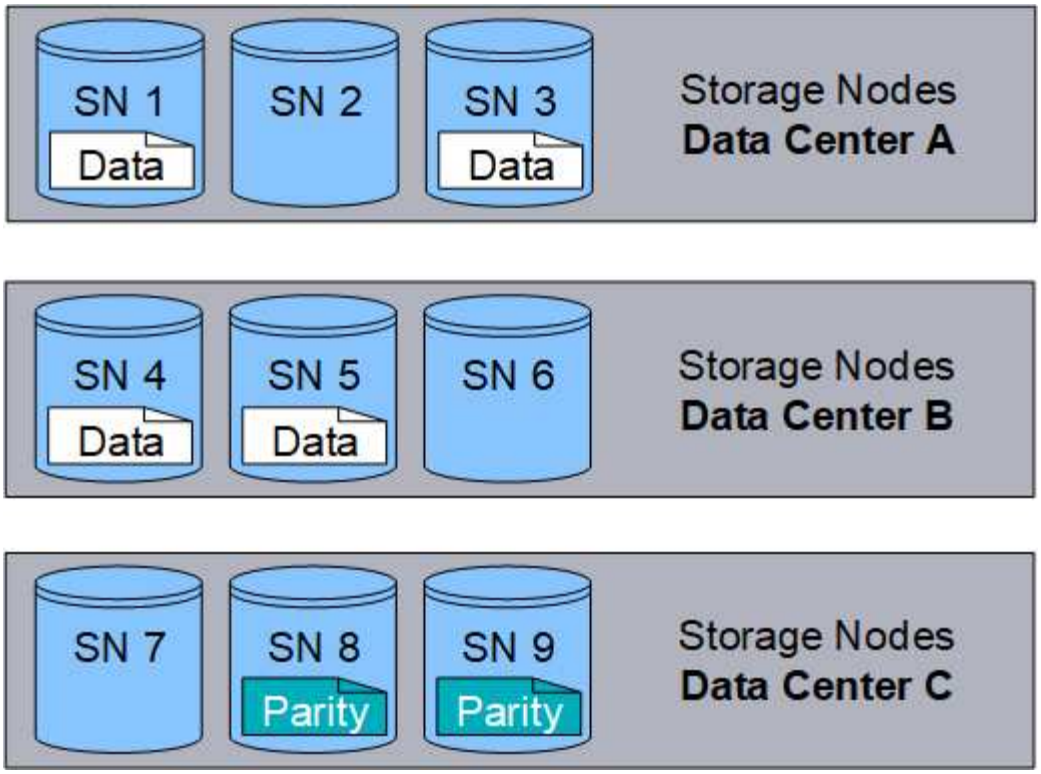

**¿Qué es la codificación de borrado?**

La codificación 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 coinciden con una regla ILM que utiliza codificación 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.

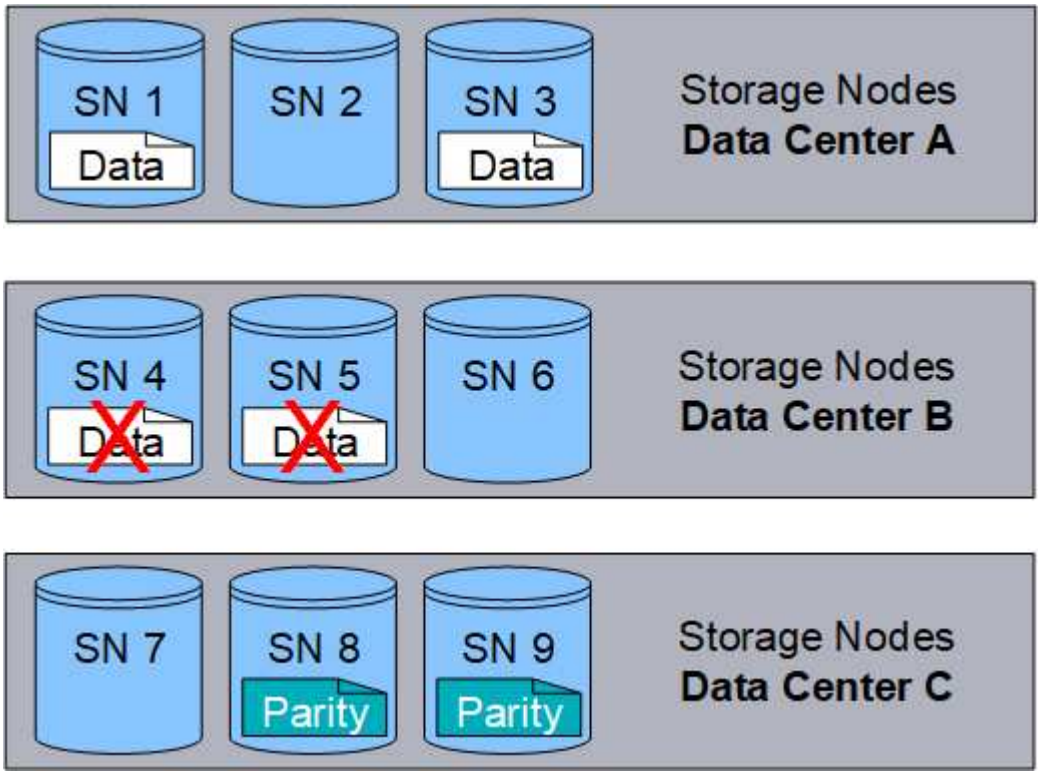
Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o de paridad se corrompe o se pierde, el algoritmo de codificación de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes.

A medida que crea reglas ILM, StorageGRID crea perfiles de codificación de borrado que admiten esas reglas. Puede ver una lista de perfiles de codificación de borrado,"cambiar el nombre de un perfil de codificación de borrado" , o"Desactivar un perfil de codificación de borrado si no se utiliza actualmente en ninguna regla ILM" .

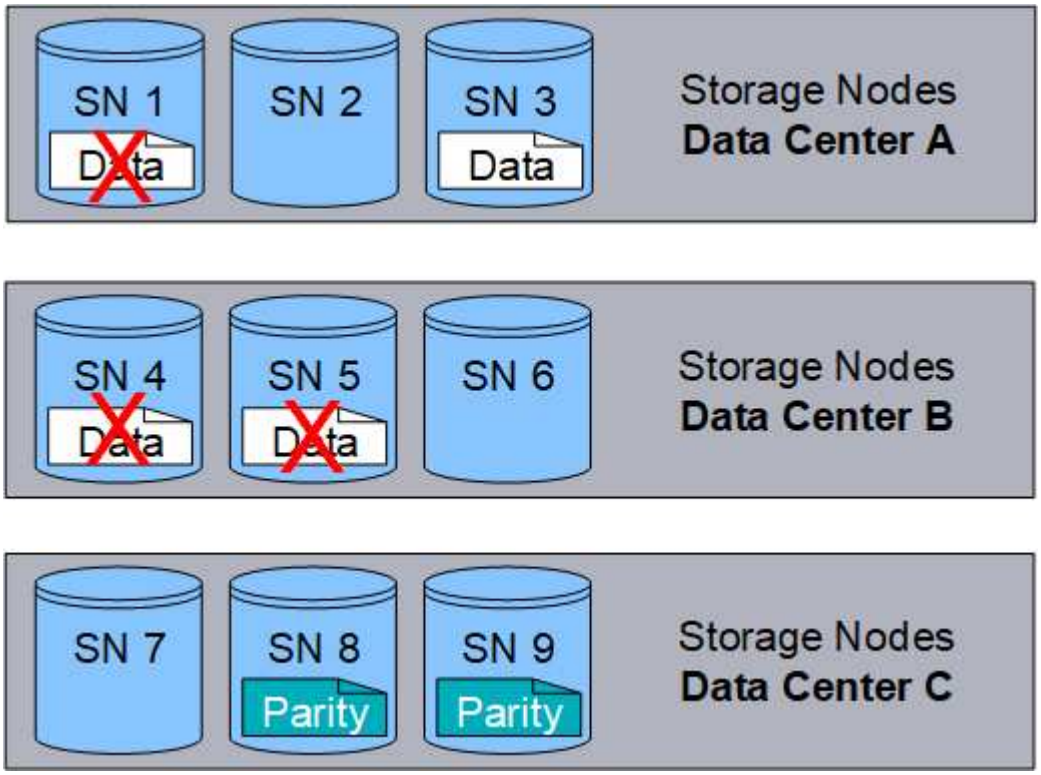
El siguiente ejemplo ilustra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los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




El esquema de codificación de borrado 4+2 se puede configurar de varias maneras. Por ejemplo, puede configurar un grupo de almacenamiento de un solo sitio que contenga seis nodos de almacenamiento. Para"protección contra pérdida de sitio" , puede utilizar un grupo de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Se puede recuperar un objeto siempre que cuatro de los seis fragmentos (datos o paridad) permanezcan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio entero, el objeto aún puede recuperarse o repararse, siempre que todos los demás fragmentos permanezcan accesibles.



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




**Información relacionada**

- "¿Qué es la replicación?"
- "¿Qué es un pool de almacenamiento?"
- "¿Qué son los esquemas de codificación de borrado?"
- "Cambiar el nombre de un perfil de codificación de borrado"
- "Desactivar un perfil de codificación de borrado"

### ¿Qué son los esquemas de codificación de borrado?

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

Cuando crea o edita una regla ILM, selecciona un esquema de codificación de borrado disponible. StorageGRID crea automáticamente esquemas de codificación de borrado en función de la cantidad de nodos de almacenamiento y sitios que conforman el grupo de almacenamiento que planea utilizar.

#### Protección de datos

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

El `k + m = n` Los fragmentos se encuentran dispersos `n` Nodos de almacenamiento para proporcionar protección de datos de la siguiente manera:

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

mayor será la tolerancia al fallo.

La mejor protección de datos la proporciona el esquema de codificación de borrado con la mayor tolerancia a fallas de nodo o volumen dentro de un grupo de almacenamiento.

#### Gastos generales de almacenamiento

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

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

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

Seleccione el esquema de codificación de borrado con el valor total más bajo de `k+m` que se ajuste a sus necesidades. Los esquemas de codificación de borrado con un menor número de fragmentos son computacionalmente más eficientes porque:

- Se crean y distribuyen (o recuperan) menos fragmentos por objeto
- Muestran un mejor rendimiento porque el tamaño del fragmento es mayor
- Pueden requerir que se agreguen menos nodos en un"expansión cuando se requiere más almacenamiento"

#### Directrices para los pools de almacenamiento

Al seleccionar el grupo de almacenamiento que se utilizará para una regla que creará una copia con código de borrado, utilice las siguientes pautas para los grupos de almacenamiento:

- El grupo de almacenamiento debe incluir tres o más sitios, o exactamente un sitio.

  > No se puede utilizar la codificación de borrado si el grupo de almacenamiento incluye dos sitios.

  - Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios
  - Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio
- No utilice un grupo de almacenamiento que incluya el sitio Todos los sitios.
- El grupo de almacenamiento debe incluir al menos *`k+m`* `+1` Nodos de almacenamiento que pueden almacenar datos de objetos.

  > Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan solo metadatos de objetos y no datos de objetos. Para obtener más información, consulte "Tipos de nodos de almacenamiento" .

  El número mínimo de nodos de almacenamiento requeridos es `k+m` . Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a prevenir fallas de ingesta o retrasos en ILM si un nodo de almacenamiento requerido no está disponible temporalmente.

#### Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios

La siguiente tabla describe los esquemas de codificación de borrado actualmente admitidos por StorageGRID para grupos de almacenamiento que incluyen tres o más sitios. Todos estos esquemas brindan protección contra pérdida de sitio. Se puede perder un sitio y el objeto seguirá siendo accesible.

Para los esquemas de codificación de borrado que brindan protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el grupo de almacenamiento excede `k+m +1` porque cada sitio requiere un mínimo de tres nodos de almacenamiento.

| Esquema de codificación 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 pérdida de sitio? | Gastos generales 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 utilizar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda utilizar cinco nodos de almacenamiento por sitio.

Al seleccionar un esquema de codificación de borrado que proporcione protección del sitio, equilibre la importancia relativa de los siguientes factores:

- **Número de fragmentos**: el rendimiento y la flexibilidad de expansión generalmente son mejores cuando el número total de fragmentos es menor.
- **Tolerancia a fallos**: La tolerancia a fallos aumenta al tener más segmentos de paridad (es decir, cuando `m` tiene un valor más alto.)
- **Tráfico de red**: Al recuperarse de fallas, se utiliza un esquema con más fragmentos (es decir, un total más alto para `k+m` ) crea más tráfico de red.
- **Gastos generales de almacenamiento**: los esquemas con mayores gastos generales requieren más espacio de almacenamiento por objeto.

Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3 (ambos tienen una sobrecarga de almacenamiento del 50 %), seleccione el esquema 6+3 si se requiere tolerancia a fallas adicional. Seleccione el esquema 4+2 si los recursos de red están limitados. Si todos los demás factores son iguales, seleccione 4+2 porque tiene un número total menor de fragmentos.

Si no está seguro de qué esquema utilizar, seleccione 4+2 o 6+3, o comuníquese con el soporte técnico.

#### Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio

Un grupo de almacenamiento de un solo sitio admite todos los esquemas de codificación de borrado definidos para tres o más sitios, siempre que el sitio tenga suficientes nodos de almacenamiento.

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

| Esquema de codificación de borrado (*k+m*) | Número mínimo de nodos de almacenamiento | Número recomendado de nodos de almacenamiento | Gastos generales 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 de la codificación de borrado

Antes de decidir si utilizar la codificación de borrado o replicación para proteger los datos de los objetos contra pérdidas, debe comprender las ventajas, desventajas y los requisitos de la codificación de borrado.

#### Ventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado ofrece mayor confiabilidad, disponibilidad y

eficiencia de almacenamiento.

- **Confiabilidad**: La confiabilidad se mide en términos de tolerancia a fallas, es decir, la cantidad de fallas simultáneas que pueden mantenerse sin pérdida de datos. Con la replicación, se almacenan múltiples copias idénticas en diferentes nodos y en distintos sitios. Con la codificación de borrado, un objeto se codifica en fragmentos de datos y paridad y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección contra fallas tanto del sitio como del nodo. En comparación con la replicación, la codificación de borrado proporciona una confiabilidad mejorada a costos de almacenamiento comparables.
- **Disponibilidad**: La disponibilidad se puede definir como la capacidad de recuperar objetos si los nodos de almacenamiento fallan o se vuelven inaccesibles. En comparación con la replicación, la codificación de borrado proporciona una mayor disponibilidad a costos de almacenamiento comparables.
- **Eficiencia de almacenamiento**: para niveles similares de disponibilidad y confiabilidad, los objetos protegidos mediante codificación de borrado consumen menos espacio en disco que los mismos objetos si estuvieran protegidos mediante replicación. Por ejemplo, un objeto de 10 MB que se replica en dos sitios consume 20 MB de espacio en disco (dos copias), mientras que un objeto que tiene un código de borrado en tres sitios con un esquema de codificación de borrado 6+3 solo consume 15 MB de espacio en disco.

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

#### Desventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado tiene las siguientes desventajas:

- Se recomienda un mayor número de nodos y sitios de almacenamiento, según el esquema de codificación de borrado. Por el contrario, si replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia. Ver"Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios" y"Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio" .
- Aumento del coste y la complejidad de las ampliaciones de almacenamiento. Para expandir una implementación que utiliza replicación, agregue capacidad de almacenamiento en cada ubicación donde se realizan copias de objetos. Para expandir una implementación que utiliza codificación de borrado, debe considerar tanto el esquema de codificación de borrado en uso como qué tan llenos están los nodos de almacenamiento existentes. Por ejemplo, si espera hasta que los nodos existentes estén 100% llenos, debe agregar al menos `k+m` Nodos de almacenamiento, pero si se expande cuando los nodos existentes están llenos al 70 %, puede agregar dos nodos por sitio y aún así maximizar la capacidad de almacenamiento utilizable. Para obtener más información, consulte "Añadir capacidad de almacenamiento para objetos con código de borrado" .
- Hay mayores latencias de recuperación cuando se utiliza codificación de borrado en sitios distribuidos geográficamente. Los fragmentos de objeto de un objeto codificado para borrado y distribuido en sitios remotos tardan más en recuperarse a través de conexiones WAN que los de un objeto replicado y disponible localmente (el mismo sitio al que se conecta el cliente).
- Cuando se utiliza codificación de borrado en sitios distribuidos geográficamente, hay un mayor uso de tráfico de red WAN para recuperaciones y reparaciones, especialmente para objetos recuperados con frecuencia o para reparaciones de objetos a través de conexiones de red WAN.
- Cuando se utiliza codificación de borrado en varios sitios, el rendimiento máximo de objetos disminuye drásticamente a medida que aumenta la latencia de la red entre los sitios. Esta disminución se debe a la disminución correspondiente en el rendimiento de la red TCP, lo que afecta la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objetos.

- Mayor uso de recursos computacionales.

#### Cuándo utilizar la codificación de borrado

La codificación de borrado es la más adecuada para los siguientes requisitos:

- Objetos de tamaño superior a 1 MB.

> La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

- Almacenamiento a largo plazo o en frío para contenido que se recupera con poca frecuencia.
- Alta disponibilidad y confiabilidad de los datos.
- Protección contra fallas completas del sitio y del nodo.
- Eficiencia de almacenamiento.
- Implementaciones de un solo sitio que requieren una protección de datos eficiente con una única copia con código de borrado en lugar de múltiples copias replicadas.
- Implementaciones de múltiples sitios donde la latencia entre sitios es inferior a 100 ms.

## Cómo se determina la retención de objetos

StorageGRID ofrece opciones para que los administradores de la red y los usuarios individuales especifiquen durante cuánto tiempo almacenar los objetos. En general, cualquier instrucción de retención proporcionada por un usuario inquilino tiene prioridad sobre las instrucciones de retención proporcionadas por el administrador de la red.

#### Cómo los usuarios inquilinos controlan la retención de objetos

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

- Si la configuración global de Bloqueo de objetos S3 está habilitada para la red, los usuarios inquilinos de S3 pueden crear depósitos con el Bloqueo de objetos S3 habilitado y luego seleccionar un **Período de retención predeterminado** para cada depósito.
- Si la configuración global de Bloqueo de objetos S3 está habilitada para la red, los usuarios inquilinos de S3 pueden crear depósitos con Bloqueo de objetos S3 habilitado y luego usar la API REST de S3 para especificar configuraciones de retención hasta la fecha y retención legal para cada versión de objeto agregada a ese depósito.
  - Una versión de un objeto que se encuentra bajo retención legal no se puede eliminar mediante ningún método.
  - Antes de que se alcance la fecha de conservación de una versión de un objeto, esa versión no se puede eliminar mediante ningún método.
  - Los objetos en depósitos con el bloqueo de objetos S3 habilitado son retenidos por ILM "para siempre". Sin embargo, una vez alcanzada su fecha de retención, una versión de un objeto puede eliminarse mediante una solicitud del cliente o mediante la expiración del ciclo de vida del depósito. Ver "Administrar objetos con S3 Object Lock" .
- Los usuarios inquilinos de S3 pueden agregar una configuración de ciclo de vida a sus depósitos que

especifique una acción de vencimiento. Si existe un ciclo de vida de depósito, StorageGRID almacena un objeto hasta que se cumpla la fecha o la cantidad de días especificados en la acción Vencimiento, a menos que el cliente elimine el objeto primero. Ver "Crear la configuración del ciclo de vida de S3" .

- Un cliente S3 puede emitir una solicitud de eliminación de objeto. StorageGRID siempre prioriza las solicitudes de eliminación del cliente sobre el ciclo de vida del bucket S3 o ILM al determinar si eliminar o conservar un objeto.

### Cómo los administradores de red controlan la retención de objetos

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

- Establezca un período máximo de retención de bloqueo de objetos S3 para cada inquilino. Luego, los usuarios inquilinos pueden establecer un período de retención predeterminado para cada uno de sus depósitos. El período máximo de retención también se aplica a cualquier objeto recién ingerido para ese depósito (fecha de retención del objeto).
- Cree instrucciones de ubicación de ILM para controlar durante cuánto tiempo se almacenan los objetos. Cuando los objetos coinciden con una regla ILM, StorageGRID almacena esos objetos hasta que transcurra el último período de tiempo de la regla ILM. Los objetos se conservan indefinidamente si se especifica "para siempre" en las instrucciones de ubicación.
- Independientemente de quién controla cuánto tiempo se conservan los objetos, las configuraciones de ILM controlan qué tipos de copias de objetos (replicadas o codificadas por borrado) se almacenan y dónde se ubican las copias (nodos de almacenamiento o grupos de almacenamiento en la nube).

### Cómo interactúan el ciclo de vida del bucket S3 y ILM

Cuando se configura un ciclo de vida de un bucket S3, las acciones de vencimiento del ciclo de vida anulan la política ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría permanecer en la cuadrícula incluso después de que hayan transcurrido las instrucciones ILM para colocar el objeto.

### Ejemplos de retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, las configuraciones del ciclo de vida del bucket, las solicitudes de eliminación de clientes e ILM, considere los siguientes ejemplos.

#### Ejemplo 1: El ciclo de vida del depósito S3 conserva los objetos durante más tiempo que ILM

**ILM**

Almacenar dos copias durante 1 año (365 días)

**Ciclo de vida del bucket**

Los objetos expiran en 2 años (730 días)

**Resultado**

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

> ⓘ Si el ciclo de vida del depósito especifica que los objetos deben conservarse durante más tiempo del especificado por ILM, StorageGRID continúa usando las instrucciones de ubicación de ILM al determinar la cantidad y el tipo de copias a almacenar. En este ejemplo, se continuarán almacenando dos copias del objeto en StorageGRID desde el día 366 al 730.

#### Ejemplo 2: El ciclo de vida del depósito S3 hace que los objetos caduquen antes que ILM

**ILM**

Conservar dos copias durante 2 años (730 días)

**Ciclo de vida del bucket**

Los objetos expiran en 1 año (365 días)

**Resultado**

StorageGRID elimina ambas copias del objeto después del día 365.

#### Ejemplo 3: La eliminación del cliente anula el ciclo de vida del depósito y el ILM

**ILM**

Almacenar dos copias en nodos de almacenamiento "para siempre"

**Ciclo de vida del bucket**

Los objetos expiran en 2 años (730 días)

**Solicitud de eliminación de cliente**

Emitido 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 S3 anula la solicitud de eliminación del cliente

**Bloqueo de objetos S3**

La fecha de conservación hasta para una versión de objeto es 2026-03-31. No está en vigor ninguna retención legal.

**Regla ILM compatible**

Almacenar dos copias en nodos de almacenamiento "para siempre"

**Solicitud de eliminación de cliente**

Emitido el 31/03/2024

**Resultado**

StorageGRID no eliminará la versión del objeto porque la fecha de conservación aún está a 2 años de distancia.

## Cómo se eliminan los 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 S3 o los requisitos de la política ILM. Comprender las diferentes formas en que se pueden eliminar objetos y cómo StorageGRID maneja las solicitudes de eliminación puede ayudarlo a administrar objetos de manera más efectiva.

StorageGRID puede utilizar uno de dos métodos para eliminar objetos:

- Eliminación sincrónica: cuando StorageGRID recibe una solicitud de eliminación de cliente, todas las copias de objetos se eliminan inmediatamente. Después de eliminar las copias se informa al cliente que la eliminación se realizó correctamente.
- Los objetos se ponen en cola para su eliminación: cuando StorageGRID recibe una solicitud de eliminación, el objeto se pone en cola para su eliminación y se informa inmediatamente al cliente que la eliminación se realizó correctamente. Las copias de objetos se eliminan más tarde mediante el procesamiento 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 más rápidamente.

La tabla resume cuándo StorageGRID utiliza cada método.

| **Método para realizar la eliminación** | **Cuando se utiliza** |
|---|---|
| Los objetos se ponen en cola para su eliminación | Cuando **cualquiera** de las siguientes condiciones sea verdadera:<br>• La eliminación automática de objetos se ha activado por uno de los siguientes eventos:<br>◦ Se alcanza la fecha de vencimiento o el número de días en la configuración del ciclo de vida de un bucket S3.<br>◦ Transcurre el último período de tiempo especificado en una regla ILM.<br>**Nota:** Los objetos en un bucket que tiene habilitado el Bloqueo de objetos S3 no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención pero aún no se cumple.<br>• Un cliente S3 solicita la eliminación y una o más de estas condiciones son verdaderas:<br>◦ Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, la ubicación de un objeto no está disponible temporalmente.<br>◦ Las colas de eliminación en segundo plano están inactivas. |
| Los objetos se eliminan inmediatamente (eliminación sincrónica) | Cuando un cliente S3 realiza una solicitud de eliminación y se cumplen **todas** las siguientes condiciones:<br>• Todas las copias se pueden eliminar en 30 segundos.<br>• Las colas de eliminación en segundo plano contienen objetos para procesar. |

Cuando los clientes S3 realizan solicitudes de eliminación, StorageGRID comienza agregando 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 que StorageGRID procese las eliminaciones de manera más eficiente, especialmente para clientes de baja concurrencia, al mismo tiempo que ayuda a prevenir retrasos en la eliminación de clientes.

**Tiempo necesario para eliminar objetos**

La forma en que StorageGRID elimina objetos puede afectar el funcionamiento aparente del sistema:

- Cuando StorageGRID realiza una eliminación sincrónica, puede tardar hasta 30 segundos en devolver un

resultado al cliente. Esto significa que puede parecer que la eliminación ocurre más lentamente, aunque en realidad las copias se eliminan más rápido que cuando StorageGRID pone en cola los objetos para su eliminación.

- Si supervisa de cerca el rendimiento de eliminación durante una eliminación masiva, es posible que observe que la tasa de eliminación parece ser lenta después de que se haya eliminado una cierta cantidad de objetos. Este cambio se produce cuando StorageGRID pasa de poner en cola objetos para su eliminación a realizar una eliminación sincrónica. La aparente reducción en la tasa de eliminación no significa que las copias de objetos se estén eliminando más lentamente. Por el contrario, indica que, en promedio, ahora se está liberando espacio más rápidamente.

Si está eliminando una gran cantidad de objetos y su prioridad es liberar espacio rápidamente, considere usar una solicitud de cliente para eliminar objetos en lugar de eliminarlos mediante ILM u otros métodos. En general, el espacio se libera más rápidamente cuando la eliminación la realizan los clientes porque StorageGRID puede usar la eliminación sincrónica.

La cantidad de tiempo necesaria para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de objetos se eliminan de forma sincrónica o se ponen en cola para su eliminación más tarde (para solicitudes de eliminación del cliente).
- Otros factores, como la cantidad de objetos en la red o la disponibilidad de recursos de la red cuando las copias de objetos se ponen en cola para su eliminación (tanto para eliminaciones de cliente como para otros métodos).

**Cómo se eliminan los objetos versionados de S3**

Cuando el control de versiones está habilitado para un bucket S3, StorageGRID sigue el comportamiento de Amazon S3 al responder a solicitudes de eliminación, ya sea que dichas solicitudes provengan de un cliente S3, la expiración del ciclo de vida de un bucket S3 o los requisitos de la política ILM.

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

Incluso 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, debido a que no se han eliminado los datos del objeto no actual, las solicitudes que especifican una versión no actual del objeto pueden tener éxito.

Para liberar espacio al eliminar objetos versionados o para quitar marcadores de eliminación, utilice una de las siguientes opciones:

- **Solicitud de cliente S3**: especifique el ID de la versión del objeto en la solicitud S3 DELETE Object(`DELETE /object?versionId=ID` ). Tenga en cuenta que esta solicitud solo elimina copias de objetos de la versión especificada (las otras versiones aún ocupan espacio).
- **Ciclo de vida del bucket**: utilice el `NoncurrentVersionExpiration` acción en la configuración del ciclo de vida del bucket. Cuando se alcanza la cantidad de NoncurrentDays especificada, StorageGRID elimina de forma permanente todas las copias de versiones de objetos no actuales. Estas versiones de objetos no se pueden recuperar.

  El `NewerNoncurrentVersions` La acción en la configuración del ciclo de vida del bucket especifica la

cantidad de versiones no actuales que se conservan en un bucket S3 versionado. Si hay más versiones no actuales que `NewerNoncurrentVersions` especifica que StorageGRID elimina las versiones anteriores cuando ha transcurrido el valor NoncurrentDays. El `NewerNoncurrentVersions` El umbral anula las reglas del ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del `NewerNoncurrentVersions` El umbral se mantiene si ILM solicita su eliminación.

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

- **ILM**:"Clonar una política activa" y agregue dos reglas ILM a la nueva política:
  - Primera regla: utilice “Tiempo no actual” como tiempo de referencia para que coincida con las versiones no actuales del objeto. En"Paso 1 (Ingresar detalles) del asistente para crear una regla de ILM" , seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?"
  - Segunda regla: utiliza **Tiempo de ingesta** para que coincida con la versión actual. La regla "Hora no actual" debe aparecer en la política encima de la regla **Hora de ingestión**.

    Para eliminar marcadores de eliminación de objetos vencidos, utilice una regla de **Tiempo de ingesta** para que coincida con los marcadores de eliminación actuales. Los marcadores de eliminación solo se eliminan cuando ha transcurrido un **Período de tiempo** de **Días** y el creador de eliminación actual ha expirado (no hay versiones no actuales).
- **Eliminar objetos en el depósito**: utilice el administrador de inquilinos 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 poder eliminar un depósito versionado.

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

**Información relacionada**

- "Utilice la API REST de S3"
- "Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3"

# Crear y asignar grados de almacenamiento

Los grados de almacenamiento identifican el tipo de almacenamiento utilizado por un nodo de almacenamiento. Puede crear grados de almacenamiento si desea que las reglas ILM coloquen determinados objetos en determinados nodos de almacenamiento.

**Antes de empezar**

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

**Acerca de esta tarea**

Cuando instala StorageGRID por primera vez, el grado de almacenamiento **Predeterminado** se asigna automáticamente a cada nodo de almacenamiento en su sistema. Según sea necesario, puede definir opcionalmente grados de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

El uso de grados de almacenamiento personalizados le permite crear grupos de almacenamiento ILM que contienen solo un tipo específico de nodo de almacenamiento. Por ejemplo, es posible que desee que determinados objetos se almacenen en sus nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento totalmente flash StorageGRID .

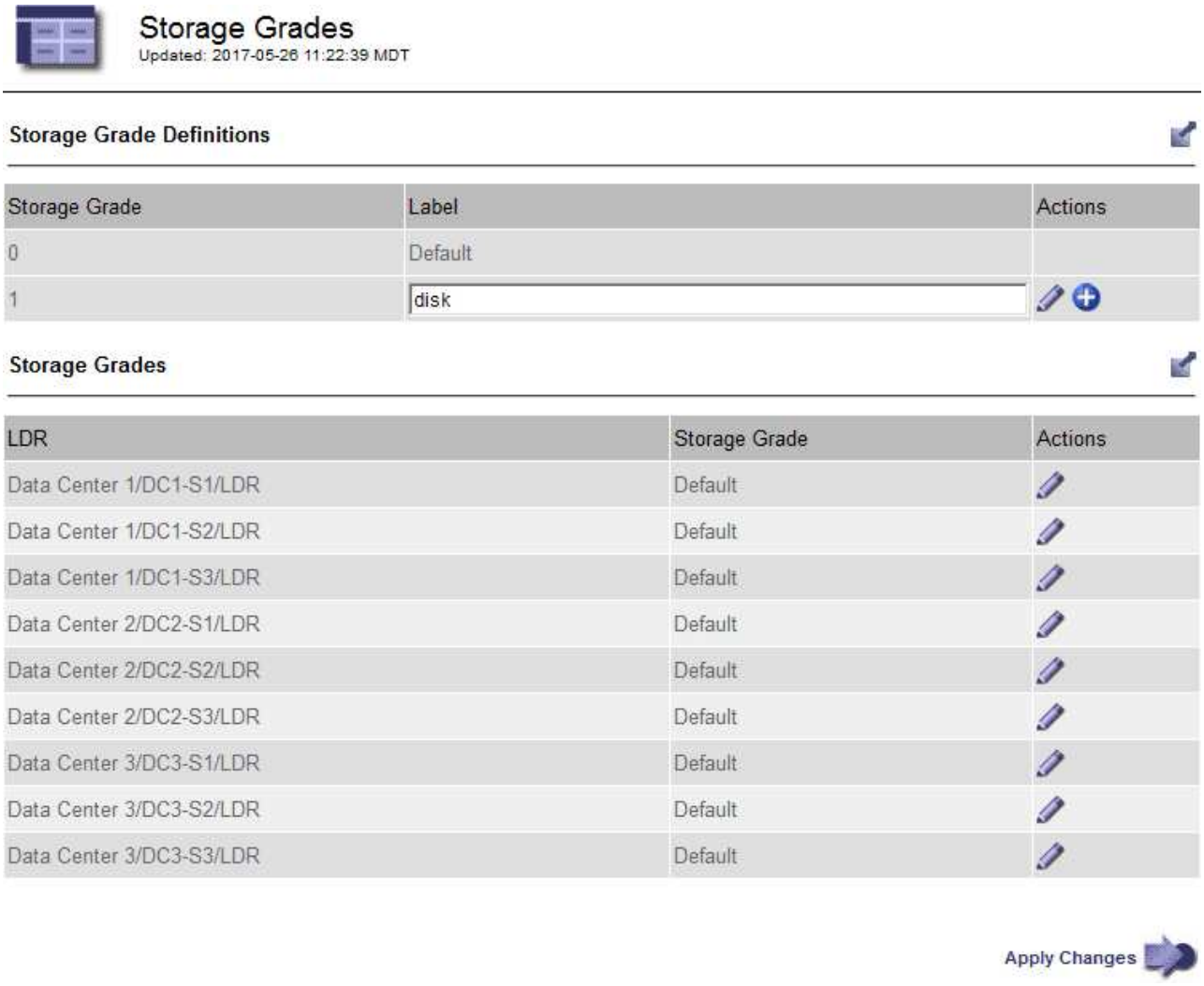
> Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan solo metadatos de objetos y no datos de objetos. A los nodos de almacenamiento de solo metadatos no se les puede asignar un grado de almacenamiento. Para obtener más información, consulte "Tipos de nodos de almacenamiento" .

Si el grado de almacenamiento no es una preocupación (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y usar la selección **incluye todos los grados de almacenamiento** para el grado de almacenamiento cuando"crear grupos de almacenamiento" . El uso de esta selección garantiza que el grupo de almacenamiento incluirá todos los nodos de almacenamiento del sitio, independientemente de su grado de almacenamiento.

> No cree más niveles de almacenamiento de los necesarios. Por ejemplo, no cree un grado de almacenamiento para cada nodo de almacenamiento. En su lugar, asigne cada grado de almacenamiento a dos o más nodos. Los grados de almacenamiento asignados a un solo nodo pueden provocar retrasos en ILM si ese nodo deja de estar disponible.

**Pasos**

1. Seleccione **ILM** > **Grados de almacenamiento**.
2. Definir grados de almacenamiento personalizados:
   a. Para cada grado de almacenamiento personalizado que desee agregar, seleccione *Insertar* para agregar una fila.
   b. Introduzca una etiqueta descriptiva.




c. Seleccione **Aplicar cambios**.

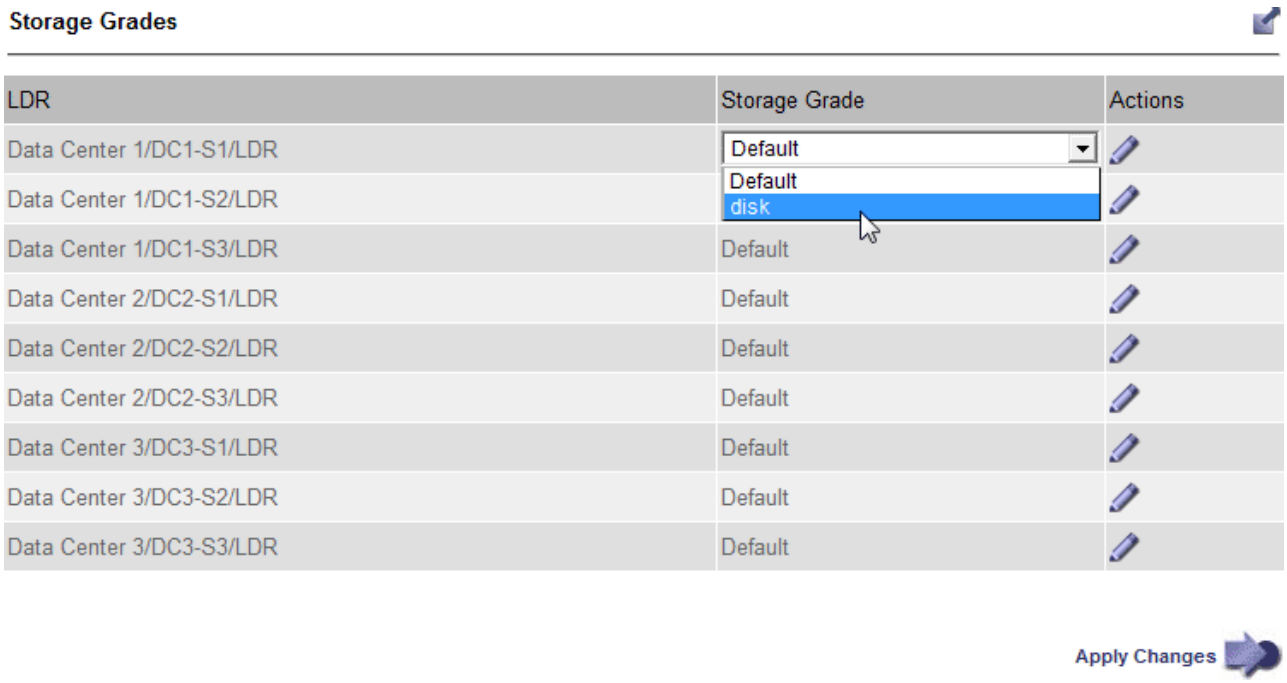
d. Opcionalmente, si necesita modificar una etiqueta guardada, seleccione **Editar*** y seleccione ***Aplicar cambios**.

No se pueden eliminar los niveles de almacenamiento.

3. Asignar nuevos grados de almacenamiento a los nodos de almacenamiento:

a. Localice el nodo de almacenamiento en la lista LDR y seleccione su ícono *Editar* .

b. Seleccione el grado de almacenamiento apropiado de la lista.




> Asignar un grado de almacenamiento a un nodo de almacenamiento determinado solo una vez. Un nodo de almacenamiento recuperado de una falla mantiene el grado de almacenamiento asignado previamente. No cambie esta asignación después de que se active la política ILM. Si se cambia la asignación, los datos se almacenan según el nuevo grado de almacenamiento.

a. Seleccione **Aplicar cambios**.

# Utilice grupos de almacenamiento

## ¿Qué es un pool de almacenamiento?

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

Cuando instala StorageGRID, se crea automáticamente un grupo de almacenamiento por sitio. Puede configurar grupos de almacenamiento adicionales según sea necesario para sus requisitos de almacenamiento.

> Los nodos de almacenamiento se pueden configurar durante la instalación para contener datos de objetos y metadatos de objetos, o solo metadatos de objetos. Los nodos de almacenamiento de solo metadatos no se pueden usar en grupos de almacenamiento. Para obtener más información, consulte "Tipos de nodos de almacenamiento" .

Los grupos de almacenamiento tienen dos atributos:

- **Grado de almacenamiento**: para los nodos de almacenamiento, el rendimiento relativo del almacenamiento de respaldo.
- **Sitio**: El centro de datos donde se almacenarán los objetos.

Los grupos de almacenamiento se utilizan en las reglas ILM para determinar dónde se almacenan los datos de los objetos y el tipo de almacenamiento utilizado. Cuando configura las reglas de ILM para la replicación,

selecciona uno o más grupos de almacenamiento.

## Pautas para la creación de grupos de almacenamiento

Configure y utilice grupos de almacenamiento para protegerse contra la pérdida de datos mediante la distribución de datos en varios sitios. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de grupo de almacenamiento.

Ver "Ejemplos de habilitación de la protección contra pérdida de sitios mediante codificación de replicación y borrado" .

### Directrices para todos los grupos de almacenamiento

- Mantenga las configuraciones del grupo de almacenamiento lo más simples posible. No cree más grupos de almacenamiento de los necesarios.
- Cree grupos de almacenamiento con tantos nodos como sea posible. Cada grupo de almacenamiento debe contener dos o más nodos. Un grupo de almacenamiento con nodos insuficientes puede provocar retrasos en ILM si un nodo deja de estar disponible.
- Evite crear o utilizar grupos de almacenamiento que se superpongan (que contengan uno o más de los mismos nodos). Si los grupos de almacenamiento se superponen, es posible que se guarden más de una copia de datos de objetos en el mismo nodo.
- En general, no utilice el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) ni el sitio Todos los sitios. Estos elementos se actualizan automáticamente para incluir cualquier sitio nuevo que agregue en una expansión, lo que podría no ser el comportamiento deseado.

### Directrices para los grupos de almacenamiento utilizados para copias replicadas

- Para la protección contra pérdida de sitios utilizando"replicación" , especifique uno o más grupos de almacenamiento específicos del sitio en el"Instrucciones de colocación para cada regla 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 de objetos replicados se coloquen exactamente donde usted espera (por ejemplo, una copia de cada objeto en cada sitio para protección contra pérdida del sitio).

- Si agrega un sitio en una expansión, cree un nuevo grupo de almacenamiento que contenga solo el nuevo sitio. Entonces,"actualizar las reglas de ILM" para controlar qué objetos se almacenan en el nuevo sitio.
- Si la cantidad de copias es menor que la cantidad de grupos de almacenamiento, el sistema distribuye las copias para equilibrar el uso del disco entre los grupos.
- Si los grupos de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), todas las copias del objeto podrían guardarse en un solo sitio. Debe asegurarse de que los grupos de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

### Directrices para los grupos de almacenamiento utilizados para copias con código de borrado

- Para la protección contra pérdida de sitios utilizando"codificación de borrado" , cree grupos de almacenamiento que consten de al menos tres sitios. Si un grupo de almacenamiento incluye solo dos sitios, no podrá utilizar ese grupo de almacenamiento para la codificación de borrado. No hay esquemas de codificación de borrado disponibles para un grupo de almacenamiento que tiene dos sitios.

- La cantidad de nodos de almacenamiento y sitios contenidos en el grupo de almacenamiento determinan qué"esquemas de codificación de borrado" están disponibles.
- Si es posible, un grupo de almacenamiento debe incluir más que la cantidad mínima de nodos de almacenamiento necesarios para el esquema de codificación de borrado que seleccione. Por ejemplo, si utiliza un esquema de codificación de borrado 6+3, debe tener al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuya los nodos de almacenamiento en los sitios de la manera más uniforme posible. Por ejemplo, para admitir un esquema de codificación de borrado 6+3, configure un grupo de almacenamiento que incluya al menos tres nodos de almacenamiento en tres sitios.
- Si tiene requisitos de alto rendimiento, 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 disminución del rendimiento de la red TCP.

  La disminución del rendimiento afecta las tasas máximas alcanzables de ingesta y recuperación de objetos (cuando se selecciona Equilibrado o Estricto como comportamiento de ingesta) o podría generar retrasos en la cola de ILM (cuando se selecciona Confirmación dual como comportamiento de ingesta). Ver "Comportamiento de ingesta de reglas ILM" .

> Si su red incluye solo un sitio, no podrá utilizar el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) ni el sitio Todos los sitios en un perfil de codificación de borrado. Este comportamiento evita que el perfil se vuelva inválido si se agrega un segundo sitio.

## Habilitar la protección contra pérdida de sitios

Si su implementación de StorageGRID incluye más de un sitio, puede usar codificación de replicación y borrado con grupos de almacenamiento configurados adecuadamente para habilitar la protección contra pérdida de sitios.

La codificación de replicación y borrado requiere diferentes configuraciones de grupo de almacenamiento:

- Para utilizar la replicación para la protección contra pérdida del sitio, utilice los grupos de almacenamiento específicos del sitio que se crean automáticamente durante la instalación de StorageGRID . Luego crea reglas ILM con"instrucciones de colocación" que especifican múltiples grupos de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar la codificación de borrado para la protección contra pérdida del sitio,"crear grupos de almacenamiento que consten de varios sitios" . Luego, cree reglas ILM que utilicen un grupo de almacenamiento compuesto por varios sitios y cualquier esquema de codificación de borrado disponible.

> Al configurar su implementación de StorageGRID para la protección contra pérdida de sitios, también debe tener en cuenta los efectos de"opciones de ingesta" y"consistencia" .

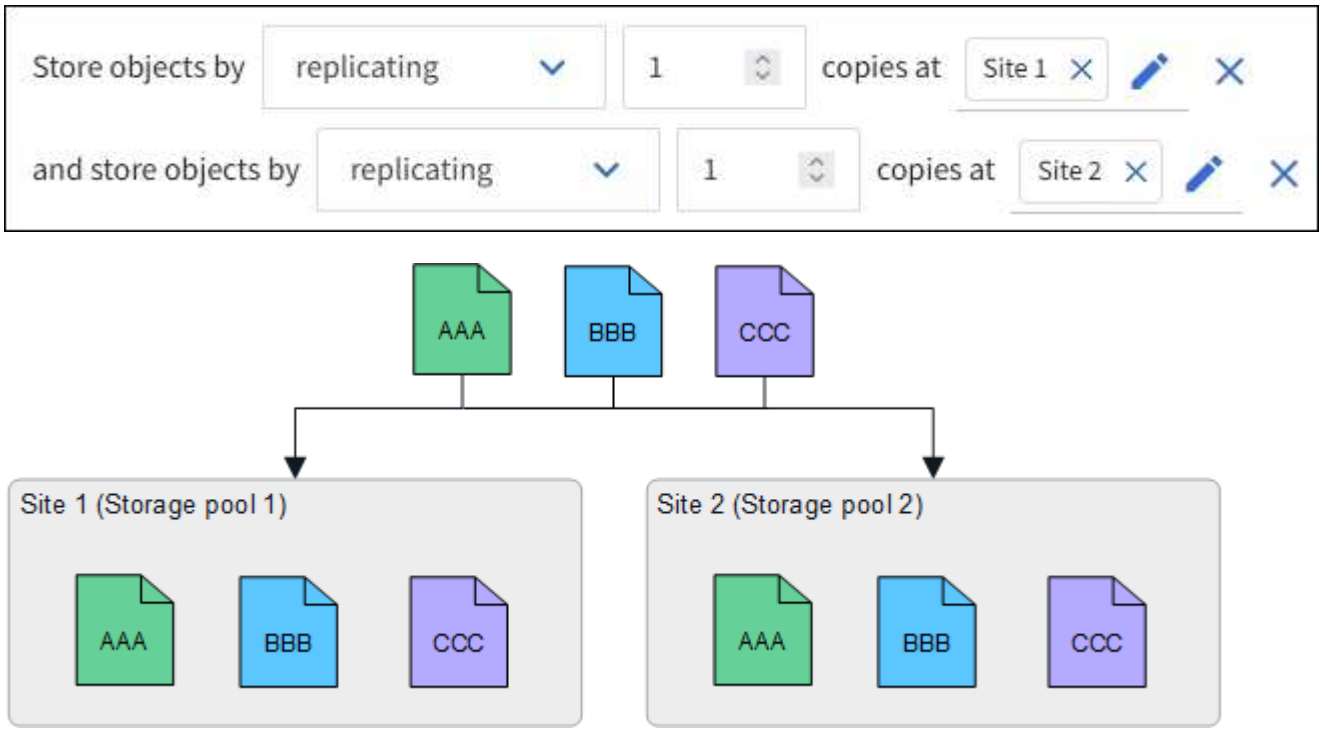
### Ejemplo de replicación

De forma predeterminada, se crea un grupo de almacenamiento para cada sitio durante la instalación de StorageGRID . Tener grupos de almacenamiento que constan de un solo sitio le permite configurar reglas ILM que utilizan la replicación para la protección contra pérdida del sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene el Sitio 1

- El grupo de almacenamiento 2 contiene el Sitio 2
- La regla ILM contiene dos colocaciones:
  - Almacenar objetos replicando 1 copia en el Sitio 1
  - Almacenar objetos replicando 1 copia en el Sitio 2

Ubicación de las reglas de ILM:




Si se pierde un sitio, hay copias de los objetos disponibles en el otro sitio.

**Ejemplo de codificación de borrado**

Tener grupos de almacenamiento que constan de más de un sitio por grupo de almacenamiento le permite configurar reglas ILM que utilizan codificación de borrado para la protección contra pérdida de sitios. En este ejemplo:

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

Ubicación de las reglas de ILM:

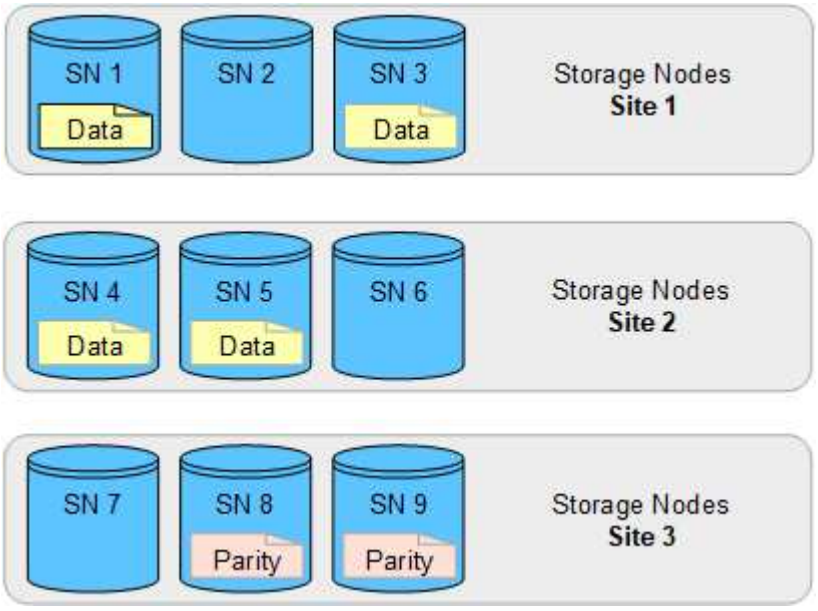

En este ejemplo:

- 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.

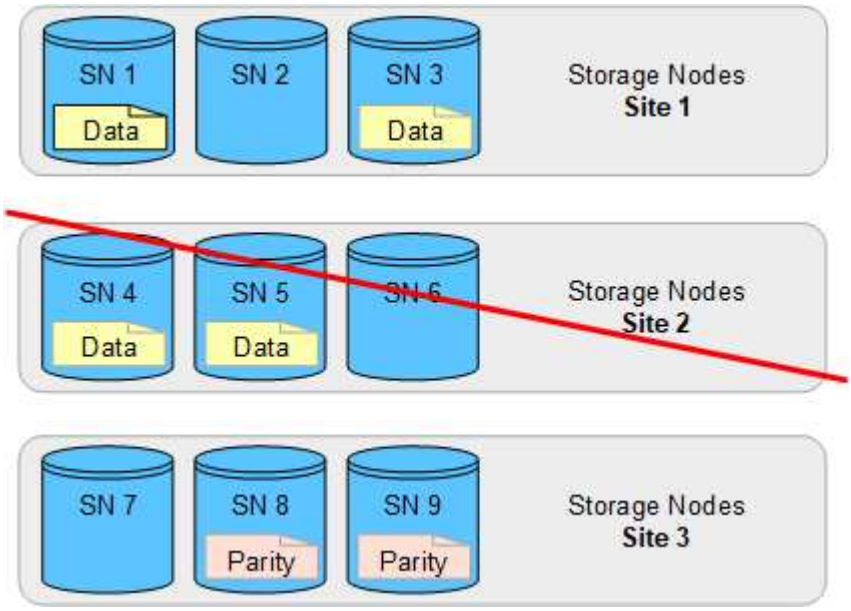
- Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centros de datos para brindar protección de datos ante fallas de nodos o pérdidas de sitios.

> Se permite la codificación de borrado en grupos de almacenamiento que contengan cualquier cantidad de sitios *excepto* dos sitios.

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




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




## Crear un grupo de almacenamiento

Crea grupos de almacenamiento para determinar dónde el sistema StorageGRID almacena los datos de los objetos y el tipo de almacenamiento utilizado. Cada grupo de almacenamiento incluye uno o más sitios y uno o más grados de almacenamiento.

> Cuando instala StorageGRID 11.9 en una nueva red, se crean automáticamente grupos de almacenamiento para cada sitio. Sin embargo, si instaló inicialmente StorageGRID 11.6 o una versión anterior, los grupos de almacenamiento no se crean automáticamente para cada sitio.

Si desea crear grupos de almacenamiento en la nube para almacenar datos de objetos fuera de su sistema StorageGRID , consulte la"Información sobre el uso de grupos de almacenamiento en la nube" .

**Antes de empezar**

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Ha revisado las pautas para crear grupos de almacenamiento.

**Acerca de esta tarea**

Los grupos de almacenamiento determinan dónde se almacenan los datos de los objetos. La cantidad de grupos de almacenamiento que necesita depende de la cantidad de sitios en su red y de los tipos de copias que desea: replicadas o con código de borrado.

- Para la replicación y la codificación de borrado de un solo sitio, cree un grupo de almacenamiento para cada sitio. Por ejemplo, si desea almacenar copias de objetos replicados en tres sitios, cree tres grupos de almacenamiento.
- Para la codificación de borrado en tres o más sitios, cree un grupo de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si desea borrar objetos de código en tres sitios, cree un grupo de almacenamiento.

> No incluya el sitio Todos los sitios en un grupo de almacenamiento que se utilizará en un perfil de codificación de borrado. En su lugar, agregue una entrada separada al grupo de almacenamiento para cada sitio que almacenará datos codificados con borrado. Vereste paso por ejemplo.

- Si tiene más de un grado de almacenamiento, no cree un grupo de almacenamiento que incluya diferentes grados de almacenamiento en un solo sitio. Ver el"Pautas para la creación de grupos de almacenamiento" .

**Pasos**

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

   La pestaña Grupos de almacenamiento enumera todos los grupos de almacenamiento definidos.

   > Para las nuevas instalaciones de StorageGRID 11.6 o anteriores, el grupo de almacenamiento Todos los nodos de almacenamiento se actualiza automáticamente cada vez que agrega nuevos sitios de centros de datos. No utilice este grupo en las reglas de ILM.

2. Para crear un nuevo grupo de almacenamiento, seleccione **Crear**.
3. Introduzca un nombre único para el grupo de almacenamiento. Utilice un nombre que sea fácil de identificar cuando configure perfiles de codificación de borrado y reglas ILM.
4. En la lista desplegable **Sitio**, seleccione un sitio para este grupo de almacenamiento.

   Cuando selecciona un sitio, la cantidad de nodos de almacenamiento en la tabla se actualiza automáticamente.

En general, no utilice el sitio Todos los sitios en ningún grupo de almacenamiento. Las reglas ILM que utilizan un grupo de almacenamiento de todos los sitios colocan los objetos en cualquier sitio disponible, lo que le brinda menos control sobre la ubicación de los objetos. Además, un grupo de almacenamiento de todos los sitios utiliza los nodos de almacenamiento en un nuevo sitio de inmediato, lo que podría no ser el comportamiento esperado.

5. En la lista desplegable **Grado de almacenamiento**, seleccione el tipo de almacenamiento que se utilizará si una regla ILM usa este grupo de almacenamiento.

   El grado de almacenamiento, *incluye todos los grados de almacenamiento*, incluye todos los nodos de almacenamiento en el sitio seleccionado. Si creó grados de almacenamiento adicionales para los nodos de almacenamiento en su cuadrícula, aparecerán en el menú desplegable.

6. Si desea utilizar el grupo de almacenamiento en un perfil de codificación de borrado de varios sitios, seleccione **Agregar más nodos** para agregar una entrada para cada sitio al grupo de almacenamiento.

   > Se le advertirá si agrega más de una entrada con diferentes grados de almacenamiento para un sitio.

   Para eliminar una entrada, seleccione el icono de eliminar ✕ .

7. Cuando esté satisfecho con sus selecciones, seleccione **Guardar**.

   El nuevo grupo de almacenamiento se agrega a la lista.

## Ver detalles del grupo de almacenamiento

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

**Antes de empezar**

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

**Pasos**

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

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

   - **Nombre**: el nombre para mostrar único del grupo de almacenamiento.
   - **Recuento de nodos**: la cantidad de nodos en el grupo de almacenamiento.
   - **Uso de almacenamiento**: el porcentaje del espacio utilizable total que se ha utilizado para datos de objetos en este nodo. Este valor no incluye metadatos del objeto.
   - **Capacidad total**: el tamaño del grupo de almacenamiento, que equivale a la cantidad total de espacio utilizable para datos de objetos para todos los nodos del grupo de almacenamiento.
   - **Uso de ILM**: cómo se utiliza actualmente el grupo de almacenamiento. Es posible que un grupo de almacenamiento no se utilice o que se utilice en una o más reglas ILM, perfiles de codificación de borrado o ambos.

2. Para ver los detalles de un grupo de almacenamiento específico, seleccione su nombre.

Aparece la página de detalles del grupo de almacenamiento.

3. Consulte la pestaña **Nodos** para obtener información sobre los nodos de almacenamiento incluidos en el grupo de almacenamiento.

   La tabla incluye la siguiente información para cada nodo:

   - Nombre del nodo
   - Nombre del sitio
   - Grado de almacenamiento
   - Uso de almacenamiento: el porcentaje del espacio total utilizable para los 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 objeto para cada nodo de almacenamiento (seleccione **NODOS** > ***Nodo de almacenamiento*** > **Almacenamiento**).

4. Vea la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento se está utilizando actualmente en alguna regla de ILM o perfil de codificación de borrado.
5. Opcionalmente, vaya a la **página de reglas de ILM** para conocer y administrar las reglas que utilizan el grupo de almacenamiento.

   Ver el"Instrucciones para trabajar con reglas ILM" .

## Editar grupo de almacenamiento

Puede editar un grupo de almacenamiento para cambiar su nombre o actualizar sitios y grados de almacenamiento.

**Antes de empezar**

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Usted ha revisado el"Pautas para la creación de grupos de almacenamiento" .
- Si planea editar un grupo de almacenamiento que se utiliza en una regla de la política ILM activa, debe considerar cómo sus cambios afectarán la ubicación de los datos de los objetos.

**Acerca de esta tarea**

Si está agregando un nuevo sitio o grado de almacenamiento a un grupo de almacenamiento que se utiliza en la política ILM activa, tenga en cuenta que los nodos de almacenamiento en el nuevo sitio o grado de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a usar un nuevo sitio o grado de almacenamiento, debe activar una nueva política ILM después de guardar el grupo de almacenamiento editado.

**Pasos**

1. Seleccione **ILM** > **Grupos de almacenamiento**.
2. Seleccione la casilla de verificación del grupo de almacenamiento que desea editar.

   No se puede editar el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores).

3. Seleccione **Editar**.
4. Según sea necesario, cambie el nombre del grupo de almacenamiento.
5. Según sea necesario, seleccione otros sitios y grados de almacenamiento.

   No se le permite cambiar el sitio o el grado de almacenamiento si el grupo de almacenamiento se utiliza en un perfil de codificación de borrado y el cambio provocaría que el esquema de codificación de borrado se vuelva inválido. Por ejemplo, si un grupo de almacenamiento utilizado en un perfil de codificación de borrado actualmente incluye un grado de almacenamiento con un solo sitio, no podrá utilizar un grado de almacenamiento con dos sitios porque el cambio haría que el esquema de codificación de borrado no sea válido.

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

6. Seleccione **Guardar**.

**Después de terminar**

Si agregó un nuevo sitio o grado de almacenamiento a un grupo de almacenamiento utilizado en la política ILM activa, active una nueva política ILM para forzar a StorageGRID a usar el nuevo sitio o grado de almacenamiento. Por ejemplo, clone su política ILM existente y luego active el clon. Ver "Trabajar con las reglas y políticas de ILM" .

## Eliminar un grupo de almacenamiento

Puedes eliminar un grupo de almacenamiento que no esté en uso.

**Antes de empezar**

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

**Pasos**

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

   No se puede eliminar un grupo de almacenamiento si se está utilizando en una regla ILM o en un perfil de codificación de borrado. Según sea necesario, seleccione ***nombre del grupo de almacenamiento*** > **uso de ILM** para determinar dónde se utiliza el grupo de almacenamiento.

3. Si el grupo de almacenamiento que desea eliminar no está en uso, seleccione la casilla de verificación.
4. Seleccione **Eliminar**.
5. Seleccione **Aceptar**.

# Utilice grupos de almacenamiento en la nube

## ¿Qué es un pool de almacenamiento en la nube?

Un grupo de almacenamiento en la nube le permite usar ILM para mover datos de objetos fuera de su sistema StorageGRID . Por ejemplo, es posible que desee mover

objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor costo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivo en el almacenamiento de blobs de Microsoft Azure. O bien, es posible que desee mantener una copia de seguridad en la nube de los objetos StorageGRID para mejorar la recuperación ante desastres.

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

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

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

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

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

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

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

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

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

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

1. **Objeto almacenado en StorageGRID**

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

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

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

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

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

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

5. **Objeto recuperado**

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

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

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

1. **Objeto almacenado en StorageGRID**

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

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

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

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

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

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

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

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

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

5. **Objeto recuperado**

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

**Información relacionada**

"Utilice la API REST de S3"

## Cuándo utilizar grupos de almacenamiento en la nube

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

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

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

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

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

Para implementar una solución de respaldo:

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

### Datos de niveles desde StorageGRID a una ubicación externa

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

Para implementar una solución de niveles:

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

### Mantener múltiples puntos finales en la nube

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

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

Para implementar múltiples puntos finales en la nube:

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

## Consideraciones para los grupos de almacenamiento en la nube

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

### Consideraciones generales

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

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

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

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

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

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

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

### Consideraciones sobre los costos

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

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

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

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

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

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

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

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`

- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

### S3: Consideraciones para el ciclo de vida del depósito externo

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

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

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

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

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

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

Si desea transferir objetos del grupo de almacenamiento en la nube a S3 Glacier Deep Archive (en lugar de a

Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida del bucket. Sin embargo, tenga en cuenta que no puede utilizar el `Expedited` Nivel para restaurar objetos del Archivo S3 Glacier Deep.

#### Azure: Consideraciones para el nivel de acceso

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

#### Azure: No se admite la gestión del ciclo de vida

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

#### Información relacionada

"Crear un grupo de almacenamiento en la nube"

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

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

| | Grupo de almacenamiento en la nube | Servicio de replicación CloudMirror |
|---|---|---|
| ¿Cuál es el propósito principal? | Actúa como un objetivo de archivo. La copia del objeto en el grupo de almacenamiento en la nube puede ser la única copia del objeto o puede ser una copia adicional. Es decir, en lugar de mantener dos copias en el sitio, puede mantener una copia dentro de StorageGRID y enviar una copia al grupo de almacenamiento en la nube. | Permite que un inquilino replique automáticamente objetos desde un depósito en StorageGRID (origen) a un depósito S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente. |
| ¿Cómo está configurado? | Se define de la misma manera que los grupos de almacenamiento, utilizando Grid Manager o la API de administración de Grid. Se puede seleccionar como ubicación de colocación en una regla ILM. Mientras que un grupo de almacenamiento consta de un grupo de nodos de almacenamiento, un grupo de almacenamiento en la nube se define mediante un punto final remoto de S3 o Azure (dirección IP, credenciales, etc.). | Un usuario inquilino"configura la replicación de CloudMirror" definiendo un punto final de CloudMirror (dirección IP, credenciales, etc.) mediante el Administrador de inquilinos o la API S3. Una vez configurado el punto final de CloudMirror, cualquier depósito propiedad de esa cuenta de inquilino se puede configurar para apuntar al punto final de CloudMirror. |

| | Grupo de almacenamiento en la nube | Servicio de replicación CloudMirror |
|---|---|---|
| ¿Quién es responsable de configurarlo? | Por lo general, un administrador de red | Normalmente, un usuario inquilino |
| ¿Cual es el destino? | • Cualquier infraestructura S3 compatible (incluido Amazon S3)<br>• Nivel de archivo de blobs de Azure<br>• Plataforma de Google Cloud (GCP) | • Cualquier infraestructura S3 compatible (incluido Amazon S3)<br>• Plataforma de Google Cloud (GCP) |
| ¿Qué hace que los objetos se muevan al destino? | Una o más reglas ILM en las políticas ILM activas. Las reglas de ILM definen qué objetos StorageGRID mueve al grupo de almacenamiento en la nube y cuándo se mueven los objetos. | El acto de ingerir un nuevo objeto en un depósito de origen que se ha configurado con un punto final de CloudMirror. Los objetos que existían en el depósito de origen antes de que este se configurara con el punto final de CloudMirror no se replican, a menos que se modifiquen. |
| ¿Cómo se recuperan los objetos? | Las aplicaciones deben realizar solicitudes a StorageGRID para recuperar objetos que se han movido a un grupo de almacenamiento en la nube. Si la única copia de un objeto se ha transferido al almacenamiento de archivo, StorageGRID administra el proceso de restauración del objeto para que pueda recuperarse. | Dado que la copia reflejada en el depósito de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes a StorageGRID o al destino S3. Por ejemplo, supongamos que utiliza la replicación de CloudMirror para reflejar objetos en una organización asociada. El socio puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario utilizar StorageGRID . |
| ¿Puedes leer desde el destino directamente? | No. Los objetos trasladados a un grupo de almacenamiento en la nube son administrados por StorageGRID. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del grupo de almacenamiento en la nube). | Sí, porque la copia reflejada es una copia independiente. |
| ¿Qué sucede si se elimina un objeto de la fuente? | El objeto también se elimina del grupo de almacenamiento en la nube. | La acción de eliminar no se replica. Un objeto eliminado ya no existe en el depósito StorageGRID , pero continúa existiendo en el depósito de destino. De manera similar, los objetos en el depósito de destino se pueden eliminar sin afectar el origen. |

| | Grupo de almacenamiento en la nube | Servicio de replicación CloudMirror |
|---|---|---|
| ¿Cómo acceder a los objetos después de un desastre (el sistema StorageGRID no está operativo)? | Los nodos StorageGRID fallidos deben recuperarse. Durante este proceso, se pueden restaurar copias de objetos replicados utilizando las copias en el grupo de almacenamiento en la nube. | Las copias de objetos en el destino CloudMirror son independientes de StorageGRID, por lo que se puede acceder a ellas directamente antes de que se recuperen los nodos de StorageGRID . |

## Crear un grupo de almacenamiento en la nube

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

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

StorageGRID valida el grupo de almacenamiento en la nube tan pronto como lo guarda, por lo que debe asegurarse de que el depósito o contenedor especificado en el grupo de almacenamiento en la nube exista y sea accesible.

**Antes de empezar**

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

**Pasos**

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

| Campo | Descripción |
|---|---|
| Nombre del grupo de almacenamiento en la nube | Un nombre que describe brevemente el grupo de almacenamiento en la nube y su propósito. Utilice un nombre que sea fácil de identificar cuando configure las reglas de ILM. |

| Campo | Descripción |
| --- | --- |
| Tipo de proveedor | ¿Qué proveedor de nube utilizará para este grupo de almacenamiento en la nube?<br>• **Amazon S3/GCP**: seleccione esta opción para un proveedor de Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3.<br>• **Almacenamiento de blobs de Azure** |
| Cubo o contenedor | El nombre del depósito S3 externo o del contenedor de Azure. No es posible cambiar este valor una vez guardado el grupo de almacenamiento en la nube. |

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

**Amazon S3/GCP**

a. Para el protocolo, seleccione HTTPS o HTTP.

> No utilice conexiones HTTP para datos confidenciales.

b. Introduzca el nombre del host. Ejemplo:

`s3-aws-region.amazonaws.com`

c. Seleccione el estilo de URL:

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

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

**Almacenamiento de blobs de Azure**

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

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

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

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

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

**Tecla de acceso**

*Para Amazon S3/GCP u otro proveedor compatible con S3*

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

**Roles de IAM en cualquier lugar**

*Para el servicio AWS IAM Roles Anywhere*

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

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

**CAP (portal de acceso C2S)**

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

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

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

**Almacenamiento de blobs de Azure**

*Para Azure Blob Storage, solo clave compartida*

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

Puede utilizar el portal de Azure para encontrar estos valores.

**Anónimo**

No se requiere información adicional

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

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

6. Seleccione **Guardar**.

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

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

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

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

## Ver detalles del grupo de almacenamiento en la nube

Puede ver los detalles de un grupo de almacenamiento en la nube para determinar

dónde se utiliza y ver qué nodos y grados de almacenamiento están incluidos.

**Antes de empezar**

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

**Pasos**

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

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

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

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

## Editar un grupo de almacenamiento en la nube

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

**Antes de empezar**

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Usted ha revisado el"Consideraciones para los grupos de almacenamiento en la nube" .

**Pasos**

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

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

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

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

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

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

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

4. Seleccione **Guardar**.

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

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

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

## Eliminar un grupo de almacenamiento en la nube

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

**Antes de empezar**

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

**Si es necesario, utilice ILM para mover datos de objetos**

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

**Pasos**

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

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

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

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

6. Edite cada una de las reglas que clonó.

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

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

#### Eliminar grupo de almacenamiento en la nube

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

**Antes de empezar**

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

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

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

**Pasos**

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

## Solucionar problemas de grupos de almacenamiento en la nube

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

### Determinar si se ha producido un error

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

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

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

### Comprobar si se ha resuelto un error

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

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

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

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

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

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

Es posible que encuentre este error cuando intente crear, editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el depósito o contenedor incluye el `x-ntap-sgws-cloud-pool-uuid` archivo marcador, pero ese archivo no tiene el campo de metadatos con el UUID esperado.

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

Pruebe uno de estos pasos para corregir el problema:

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

nuevo depósito y use este nuevo depósito en su lugar.

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

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

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

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

Es posible que encuentre este error en las siguientes circunstancias:

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

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

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

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

**Error: No se pudo analizar el certificado de CA**

Es posible que encuentre este error cuando intente crear o editar un grupo de almacenamiento en la nube. El error ocurre si StorageGRID no pudo analizar el certificado ingresado al configurar el grupo de almacenamiento en la nube.

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

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

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

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

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

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

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

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

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

**Error: Ya se han colocado objetos en este depósito**

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

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

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

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

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

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

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

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

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

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

Pruebe estos pasos para corregir el problema:

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

#### Información relacionada

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

# Administrar perfiles de codificación de borrado

Puede ver los detalles de un perfil de codificación de borrado y cambiar el nombre de un perfil si es necesario. Puede desactivar un perfil de codificación de borrado si no se utiliza actualmente en ninguna regla ILM.

#### Antes de empezar

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

## Ver detalles del perfil de codificación de borrado

Puede ver los detalles de un perfil de codificación de borrado para determinar su estado, el esquema de codificación de borrado utilizado y otra información.

#### Pasos

1. Seleccione **CONFIGURACIÓN** > **Sistema** > **Codificación de borrado**.
2. Seleccione el perfil. Aparece la página de detalles del perfil.
3. Opcionalmente, consulte la pestaña de reglas de ILM para obtener una lista de las reglas de ILM que usan el perfil y las políticas de ILM que usan esas reglas.
4. Opcionalmente, consulte la pestaña Nodos de almacenamiento para obtener detalles sobre cada nodo de almacenamiento en el grupo de almacenamiento del perfil, como el sitio donde está ubicado y el uso del almacenamiento.

## Cambiar el nombre de un perfil de codificación de borrado

Es posible que desees cambiar el nombre de un perfil de codificación de borrado para que sea más obvio lo que hace el perfil.

#### Pasos

1. Seleccione **CONFIGURACIÓN** > **Sistema** > **Codificación de borrado**.
2. Seleccione el perfil que desea renombrar.
3. Seleccione **Cambiar nombre**.

4. Introduzca un nombre único para el perfil de codificación de borrado.

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

   > Los nombres de los perfiles de codificación de borrado deben ser únicos. Se produce un error de validación si utiliza el nombre de un perfil existente, incluso si dicho perfil se ha desactivado.

5. Seleccione **Guardar**.

## Desactivar un perfil de codificación de borrado

Puede desactivar un perfil de codificación de borrado si ya no planea usarlo y si el perfil no se utiliza actualmente en ninguna regla de ILM.

> Confirme que no haya operaciones de reparación de datos con código de borrado ni procedimientos de desmantelamiento en proceso. Se devuelve un mensaje de error si intenta desactivar un perfil de codificación de borrado mientras alguna de estas operaciones está en progreso.

**Acerca de esta tarea**

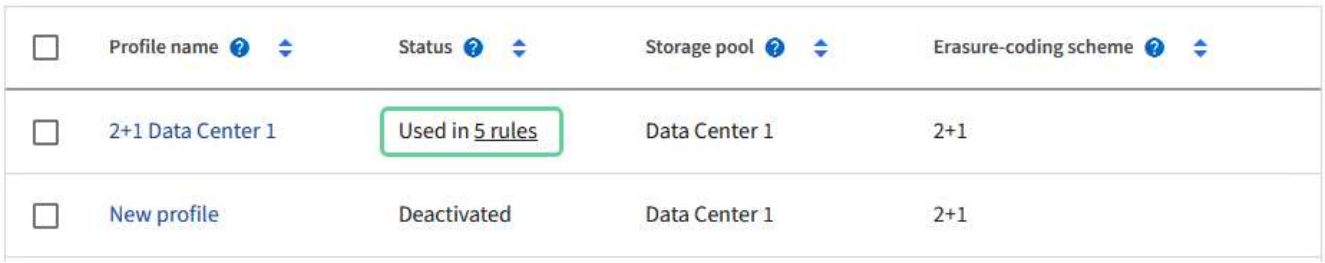
StorageGRID le impide desactivar un perfil de codificación de borrado si se cumple alguna de las siguientes condiciones:

- Actualmente, el perfil de codificación de borrado se utiliza en una regla ILM.
- El perfil de codificación de borrado ya no se utiliza en ninguna regla ILM, pero los datos de objetos y los fragmentos de paridad para el perfil aún existen.

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Sistema** > **Codificación de borrado**.
2. En la pestaña Activo, revise la columna **Estado** para confirmar que el perfil de codificación de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

   No se puede desactivar un perfil de codificación de borrado si se utiliza en alguna regla ILM. En el ejemplo, el perfil 2+1 del centro de datos 1 se utiliza en al menos una regla 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 ILM, siga estos pasos:
   a. Seleccione **ILM** > **Reglas**.
   b. Seleccione cada regla y revise el diagrama de retención para determinar si la regla utiliza el perfil de codificación de borrado que desea desactivar.
   c. Si la regla ILM utiliza el perfil de codificación de borrado que desea desactivar, determine si la regla se

utiliza en alguna política ILM.

d. Complete los pasos adicionales de la tabla, según dónde se utilice el perfil de codificación de borrado.

| ¿Dónde se ha utilizado el perfil? | Pasos adicionales a realizar antes de desactivar el perfil | Consulte estas instrucciones adicionales |
|---|---|---|
| Nunca se utiliza en ninguna regla ILM | No se requieren pasos adicionales. Continúe con este procedimiento. | *Ninguno* |
| En una regla ILM que nunca se ha utilizado en ninguna política ILM | i. Editar o eliminar todas las reglas ILM afectadas. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado.<br>ii. Continúe con este procedimiento. | "Trabajar con las reglas y políticas de ILM" |
| En una regla ILM que actualmente se encuentra en una política ILM activa | i. Clonar la política.<br>ii. Eliminar la regla ILM que utiliza el perfil de codificación de borrado.<br>iii. Agregue una o más reglas ILM nuevas para garantizar que los objetos estén protegidos.<br>iv. Guarde, simule y active la nueva política.<br>v. Espere a que se aplique la nueva política y a que los objetos existentes se muevan a nuevas ubicaciones según las nuevas reglas que agregó.<br>**Nota:** Dependiendo de la cantidad de objetos y el tamaño de su sistema StorageGRID , las operaciones de ILM podrían tardar semanas o incluso meses en mover los objetos a nuevas ubicaciones, según las nuevas reglas de ILM.<br>Si bien puede intentar desactivar de forma segura un perfil de codificación de borrado mientras aún esté asociado con datos, la operación de desactivación fallará. Un mensaje de error le informará si el perfil aún no está listo para ser desactivado.<br>vi. Edite o elimine la regla que quitó de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado.<br>vii. Continúe con este procedimiento. | "Crear una política ILM"<br>"Trabajar con las reglas y políticas de ILM" |

| ¿Dónde se ha utilizado el perfil? | Pasos adicionales a realizar antes de desactivar el perfil | Consulte estas instrucciones adicionales |
|---|---|---|
| En una regla ILM que actualmente se encuentra en una política ILM | i. Editar la política.<br>ii. Eliminar la regla ILM que utiliza el perfil de codificación de borrado.<br>iii. Agregue una o más reglas ILM nuevas para garantizar que todos los objetos estén protegidos.<br>iv. Guardar la política.<br>v. Edite o elimine la regla que quitó de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado.<br>vi. Continúe con este procedimiento. | "Crear una política ILM"<br><br>"Trabajar con las reglas y políticas de ILM" |

e. Actualice la página Perfiles de codificación de borrado para asegurarse de que el perfil no se utilice en una regla ILM.

4. Si el perfil no se utiliza en una regla ILM, seleccione el botón de opción y seleccione **Desactivar**. Aparece el cuadro de diálogo Desactivar perfil de codificación de borrado.

> Puede seleccionar varios perfiles para desactivarlos al mismo tiempo, siempre que cada perfil no se utilice en ninguna regla.

5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.

**Resultados**

- Si StorageGRID puede desactivar el perfil de codificación de borrado, su estado es Desactivado. Ya no puedes seleccionar este perfil para ninguna regla ILM. No es posible reactivar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto aún están asociados con este perfil. Es posible que tengas que esperar varias semanas antes de intentar nuevamente el proceso de desactivación.

# Configurar regiones (opcional y solo S3)

Las reglas ILM pueden filtrar objetos según las regiones donde se crean los buckets S3, lo que le permite almacenar objetos de diferentes regiones en diferentes ubicaciones de almacenamiento.

Si desea utilizar una región de bucket S3 como filtro en una regla, primero debe crear las regiones que los buckets pueden usar en su sistema.

> No es posible cambiar la región de un depósito una vez creado el mismo.

**Antes de empezar**

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

- Tienes"permisos de acceso específicos" .

**Acerca de esta tarea**

Al crear un depósito S3, puede especificar que el depósito se cree en una región específica. Al especificar una región, el bucket puede estar geográficamente cerca de sus usuarios, lo que puede ayudar a optimizar la latencia, minimizar los costos y abordar los requisitos regulatorios.

Al crear una regla ILM, es posible que desee utilizar la región asociada con un depósito S3 como filtro avanzado. Por ejemplo, puede diseñar una regla que se aplique únicamente a los objetos en los depósitos S3 creados en el `us-west-2` región. Luego, puede especificar que se coloquen copias de esos objetos en nodos de almacenamiento en un sitio del centro de datos dentro de esa región para optimizar la latencia.

Al configurar regiones, siga estas pautas:

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

  > EU no se considera un alias de eu-west-1. Si desea utilizar la región UE o eu-west-1, debe utilizar el nombre exacto.

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

  Puede obtenerse una región no válida si utiliza una región como filtro avanzado en una regla ILM pero luego elimina esa región, o si utiliza la API de administración de cuadrícula para crear una regla y especificar una región que no ha definido.

- Si elimina una región después de usarla para crear un depósito S3, deberá volver a agregar la región si alguna vez desea utilizar el filtro avanzado de Restricción de ubicación para buscar objetos en ese depósito.

**Pasos**

1. Seleccione **ILM** > **Regiones**.

   Aparece la página Regiones, con una lista de las regiones definidas actualmente. **Región 1** muestra la región predeterminada, `us-east-1` , que no se puede modificar ni eliminar.

2. Para agregar una región:
   a. Seleccione **Agregar otra región**.
   b. Ingrese el nombre de la región que desea utilizar al crear depósitos S3.

      Debe utilizar este nombre de región exacto como elemento de solicitud LocationConstraint cuando cree el bucket S3 correspondiente.

3. Para eliminar una región no utilizada, seleccione el icono de eliminar ✕ .

   Aparece un mensaje de error si intenta eliminar una región que se utiliza actualmente en cualquier política (activa o inactiva).

4. Cuando haya terminado de realizar cambios, seleccione **Guardar**.

   Ahora puede seleccionar estas regiones desde la sección Filtros avanzados en el paso 1 del asistente Crear regla ILM. Ver "Utilice filtros avanzados en las reglas de ILM" .

# Crear regla ILM

## Utilice reglas ILM para administrar objetos

Para administrar objetos, debe crear un conjunto de reglas de administración del ciclo de vida de la información (ILM) y organizarlas en una política ILM.

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

> ⓘ Los metadatos de los objetos no son administrados por las reglas ILM. En cambio, los metadatos de los objetos se almacenan en una base de datos de 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 contra pérdidas.

### Elementos de una regla ILM

Una regla ILM tiene tres elementos:

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

### Filtrado de reglas ILM

Cuando se crea una regla ILM, se especifican filtros para identificar a qué objetos se aplica la regla.

En el caso más simple, es posible que una regla no utilice ningún filtro. Cualquier regla que no utilice filtros se aplica a todos los objetos, por lo que debe ser la última regla (predeterminada) en una política ILM. La regla predeterminada proporciona instrucciones de almacenamiento para los objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos le permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Estos filtros le permiten aplicar una regla a cuentas de inquilinos específicos, depósitos S3 específicos o ambos.

  Los filtros básicos le brindan una forma sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que sea necesario almacenar los registros financieros de su empresa para cumplir con los requisitos reglamentarios, mientras que es posible que sea necesario almacenar los datos del departamento de marketing para facilitar las operaciones diarias. Después de crear cuentas de inquilinos independientes para cada departamento o después de segregar datos de los diferentes departamentos en grupos S3 separados, puede 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 le brindan un control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades del objeto:
  - Tiempo de ingesta
  - Hora del último 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)

Puede filtrar objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de imágenes de un hospital pueden usarse con frecuencia cuando tienen menos de 30 días y con poca frecuencia después, mientras que los objetos que contienen información de visitas de pacientes pueden necesitar copiarse al departamento de facturación en la sede central de la red de salud. Puede crear filtros que identifiquen cada tipo de objeto según el nombre del objeto, el tamaño, las etiquetas de objeto S3 o cualquier otro criterio relevante y luego crear reglas independientes para almacenar cada conjunto de objetos de forma adecuada.

Puede combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imágenes grandes de forma diferente a sus registros de proveedores, mientras que el departamento de Recursos Humanos podría necesitar almacenar registros de personal en una geografía específica e información de políticas de forma centralizada. En este caso, puede crear reglas que filtren por cuenta de inquilino para segregar los registros de cada departamento, mientras utiliza filtros en cada regla para identificar el tipo específico de objetos a los que se aplica la regla.

**Instrucciones de 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 más instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo.

Al crear instrucciones de ubicación:

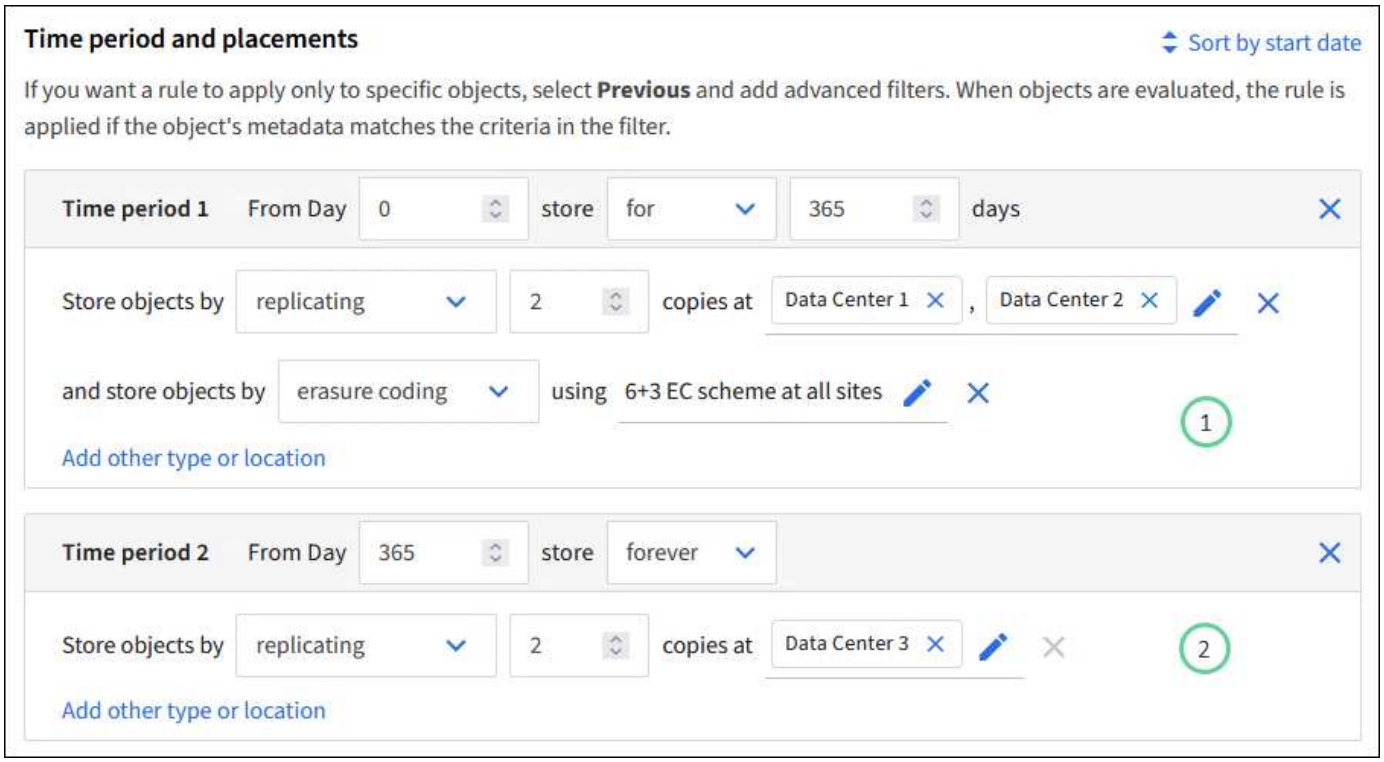
- Comienza especificando el tiempo de referencia, que determina cuándo comienzan las instrucciones de colocación. El tiempo de referencia puede ser cuando se ingiere un objeto, cuando se accede a un objeto, cuando un objeto versionado deja de ser actual o un tiempo definido por el usuario.
- A continuación, especifica cuándo se aplicará la ubicación, en relación con el tiempo de referencia. Por ejemplo, una ubicación podría comenzar el día 0 y continuar durante 365 días, en relación con el momento en que se ingirió el objeto.

- Por último, se especifica el tipo de copias (codificación de replicación o borrado) y la ubicación donde se almacenan las copias. Por ejemplo, es posible que desee almacenar dos copias replicadas en dos sitios diferentes.

Cada regla puede definir múltiples ubicaciones para un solo período de tiempo y diferentes ubicaciones para diferentes períodos de tiempo.

- Para colocar objetos en varias ubicaciones durante un solo período de tiempo, seleccione **Agregar otro tipo o ubicación** para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione **Agregar otro período de tiempo** para agregar el siguiente período de tiempo. Luego, especifique una o más líneas dentro del período de tiempo.

El ejemplo muestra dos instrucciones de ubicación en la página Definir ubicaciones del asistente Crear regla de ILM.




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

- La primera línea crea dos copias de objetos replicados en dos sitios de 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 colocación (2) crea dos copias después de un año y conserva esas copias para siempre.

Al definir el conjunto de instrucciones de ubicación para una regla, debe asegurarse de que al menos una instrucción de ubicación comience en el día 0, que no haya espacios entre los períodos de tiempo que haya definido y que la instrucción de ubicación final continúe para siempre o hasta que ya no necesite copias de objetos.

A medida que expira cada período de tiempo de la regla, se aplican las instrucciones de ubicación de

contenido para el siguiente período de tiempo. Se crean nuevas copias de objetos y se eliminan las copias innecesarias.

#### Comportamiento de ingesta de reglas ILM

El comportamiento de ingesta controla si las copias de objetos se colocan inmediatamente de acuerdo con las instrucciones de la regla, o si se realizan copias provisionales y las instrucciones de ubicación se aplican más tarde. Los siguientes comportamientos de ingesta están disponibles para las reglas ILM:

- **Equilibrado**: StorageGRID intenta realizar todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se realizan copias provisionales y se devuelve el resultado exitoso al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Estricto**: Se deben realizar todas las copias especificadas en la regla ILM antes de devolver el resultado exitoso al cliente.
- **Confirmación dual**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Cuando sea posible se realizarán las copias especificadas en la regla ILM.

#### Información relacionada

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

#### Ejemplo de regla ILM

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

- Aplicar únicamente a los objetos pertenecientes al Inquilino A.
- Haga dos copias replicadas de esos objetos y almacene cada copia en un sitio diferente.
- Conserve 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 por una solicitud de eliminación del cliente o hasta que expire el ciclo de vida de un depósito.
- Utilice la opción Equilibrado para el comportamiento de ingesta: la instrucción de ubicación de dos sitios se aplica tan pronto como el Inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar inmediatamente ambas copias requeridas.

  Por ejemplo, si no se puede acceder al Sitio 2 cuando el Inquilino A guarda un objeto, StorageGRID hará dos copias provisionales en los Nodos de almacenamiento del Sitio 1. Tan pronto como el Sitio 2 esté disponible, StorageGRID hará la copia requerida en ese sitio.

#### Información relacionada

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

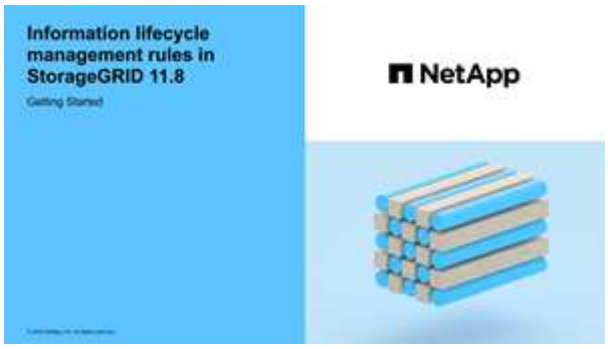
## Acceda al asistente para crear una regla ILM

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

Si desea crear la regla ILM predeterminada para una política, siga las"Instrucciones para crear una regla ILM predeterminada" en cambio.

**Antes de empezar**

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Si desea especificar a qué cuentas de inquilino se aplica esta regla, tiene la"Permiso de cuentas de inquilinos" o conoce el ID de cuenta para cada cuenta.
- Si desea que la regla filtre objetos según los metadatos de la hora del último acceso, las actualizaciones de la hora del último acceso deben estar habilitadas por el bucket S3.
- Ha configurado todos los grupos de almacenamiento en la nube que planea utilizar. Ver "Crear un grupo de almacenamiento en la nube" .
- Estás familiarizado con el"opciones de ingesta" .
- Si necesita crear una regla compatible para usarla con S3 Object Lock, está familiarizado con el"Requisitos para el bloqueo de objetos S3" .
- Opcionalmente has visto el vídeo: "Vídeo: Resumen de las reglas de ILM" .




**Acerca de esta tarea**

Al crear reglas ILM:

- Tenga en cuenta la topología y las configuraciones de almacenamiento del sistema StorageGRID .
- Considere qué tipos de copias de objetos desea realizar (replicadas o codificadas por borrado) y la cantidad de copias de cada objeto que se requieren.
- Determinar qué tipos de metadatos de objetos se utilizan en las aplicaciones que se conectan al sistema StorageGRID . Las reglas ILM filtran objetos según sus metadatos.
- Considere dónde desea que se coloquen las copias de objetos a lo largo del tiempo.
- Decide qué opción de ingesta utilizar (equilibrada, estricta o confirmación dual).

**Pasos**

1. Seleccione **ILM** > **Reglas**.
2. Seleccione **Crear**. "Paso 1 (Ingresar detalles)"Aparece el asistente Crear una regla ILM.

## Paso 1 de 3: Ingrese los detalles

El paso **Ingresar detalles** del asistente Crear una regla ILM le permite ingresar un nombre y una descripción para la regla y definir filtros para la regla.

Ingresar una descripción y definir filtros para la regla son opcionales.

**Acerca de esta tarea**

Al evaluar un objeto frente a un"Regla ILM" StorageGRID compara los metadatos del objeto con los filtros de la regla. Si los metadatos del objeto coinciden con todos los filtros, StorageGRID utiliza la regla para colocar el objeto. Puede diseñar una regla para aplicarla a todos los objetos, o puede especificar filtros básicos, como una o más cuentas de inquilino o nombres de depósito, o filtros avanzados, como el tamaño del objeto o los metadatos del usuario.

**Pasos**

1. Introduzca un nombre único para la regla en el campo **Nombre**.
2. Opcionalmente, ingrese una breve descripción de la regla en el campo **Descripción**.

   Debes describir el propósito o función de la regla para poder reconocerla más adelante.

3. Opcionalmente, seleccione una o más cuentas de inquilino S3 a las que se aplica esta regla. Si esta regla se aplica a todos los inquilinos, deje este campo en blanco.

   Si no tiene el permiso de acceso de raíz o el permiso de cuentas de inquilino, no podrá seleccionar inquilinos de la lista. En su lugar, ingrese el ID del inquilino o ingrese varios ID como una cadena delimitada por comas.

4. De manera opcional, especifique los buckets S3 a los que se aplica esta regla.

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

5. Para los inquilinos de S3, seleccione opcionalmente **Sí** para aplicar la regla solo a versiones de objetos más antiguas en depósitos de S3 que tengan habilitada la función de control de versiones.

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

   > El tiempo no actual se aplica únicamente a objetos S3 en depósitos con control de versiones habilitado. Ver"Operaciones en buckets, PutBucketVersioning" y"Administrar objetos con S3 Object Lock" .

   Puede utilizar esta opción para reducir el impacto de almacenamiento de los objetos versionados filtrando las versiones de objetos no actuales. Ver "Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3" .

6. Opcionalmente, seleccione **Agregar un filtro avanzado** para especificar filtros adicionales.

   Si no configura 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, consulteUtilice filtros avanzados en las reglas de ILM yEspecificar múltiples tipos y valores de metadatos .

7. Seleccione **Continuar**. "Paso 2 (Definir ubicaciones)"Aparece el asistente Crear una regla ILM.

### Utilice filtros avanzados en las reglas de ILM

El filtrado avanzado le permite crear reglas ILM que se aplican solo a objetos específicos en función de sus metadatos. Cuando configura el filtrado avanzado para una regla, selecciona el tipo de metadatos que desea que coincidan, selecciona un operador y especifica un valor de metadatos. Cuando se evalúan objetos, la

regla ILM se aplica solo a aquellos objetos que tienen metadatos que coinciden con el filtro avanzado.

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

| Tipo de metadatos | Operadores compatibles | Valor de metadatos |
|---|---|---|
| Tiempo de ingesta | • es<br>• no es<br>• es antes<br>• está en o antes<br>• es despues<br>• está en o después | Hora y fecha en que se ingirió el objeto.<br><br>**Nota:** Para evitar problemas de recursos al activar una nueva política ILM, puede usar el filtro avanzado Tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta para que sea mayor o igual al tiempo aproximado en que entrará en vigencia la nueva política para garantizar que los objetos existentes no se muevan innecesariamente. |
| Llave | • es igual<br>• no es igual<br>• contiene<br>• no contiene<br>• comienza con<br>• no empieza con<br>• termina con<br>• no termina con | Toda o parte de una clave de objeto S3 única.<br><br>Por ejemplo, es posible que desees hacer coincidir objetos que terminen con `.txt` o empezar con `test-object/` . |
| Hora del último acceso | • es<br>• no es<br>• es antes<br>• está en o antes<br>• es despues<br>• está en o después | Hora y fecha en que se recuperó (leyó o vio) el objeto por última vez.<br><br>**Nota:** Si planeas"utilizar la hora del último acceso" Como filtro avanzado, se deben habilitar las actualizaciones de la última hora de acceso para el bucket S3. |
| Restricción de ubicación (solo S3) | • es igual<br>• no es igual | La región donde se creó un depósito S3. Utilice **ILM** > **Regiones** para definir las regiones que se muestran.<br><br>**Nota:** Un valor de us-east-1 coincidirá con objetos en depósitos creados en la región us-east-1, así como con objetos en depósitos que no tienen ninguna región especificada. Ver "Configurar regiones (opcional y solo S3)" . |

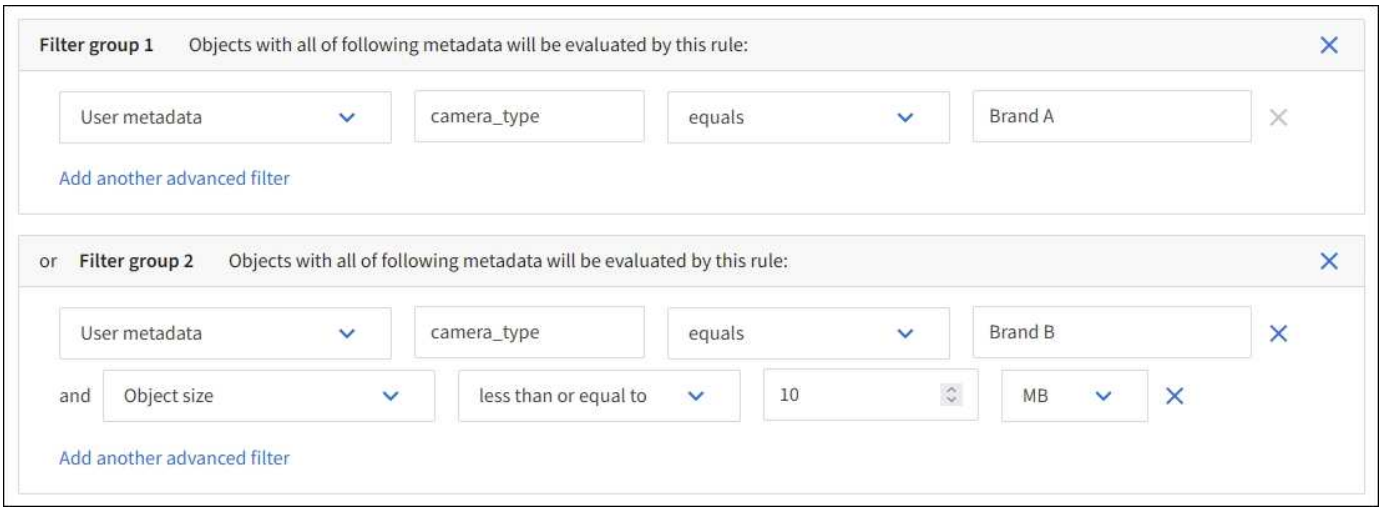
| Tipo de metadatos | Operadores compatibles | Valor de metadatos |
| --- | --- | --- |
| Tamaño del objeto | • es igual<br>• no es igual<br>• menos que<br>• menor o igual a<br>• más que<br>• mayor o igual a | El tamaño del objeto.<br><br>La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado. |
| Metadatos del usuario | • contiene<br>• termina con<br>• es igual<br>• existe<br>• comienza con<br>• no contiene<br>• no termina con<br>• no es igual<br>• no existe<br>• no empieza con | Par clave-valor, donde **Nombre de metadatos del usuario** es la clave y **Valor de metadatos** es el valor.<br><br>Por ejemplo, para filtrar objetos que tienen metadatos de usuario de `color=blue` , especificar `color` para **Nombre de metadatos de usuario**, `equals` para el operador, y `blue` para **Valor de metadatos**.<br><br>**Nota:** Los nombres de metadatos del usuario no distinguen entre mayúsculas y minúsculas; los valores de metadatos del usuario sí distinguen entre mayúsculas y minúsculas. |
| Etiqueta de objeto (solo S3) | • contiene<br>• termina con<br>• es igual<br>• existe<br>• comienza con<br>• no contiene<br>• no termina con<br>• no es igual<br>• no existe<br>• no empieza con | Par clave-valor, donde **Nombre de etiqueta de objeto** es la clave y **Valor de etiqueta de objeto** es el valor.<br><br>Por ejemplo, para filtrar objetos que tienen una etiqueta de objeto de `Image=True` , especificar `Image` para **Nombre de etiqueta de objeto**, `equals` para el operador, y `True` para **Valor de etiqueta de objeto**.<br><br>**Nota:** Los nombres de las etiquetas de objeto y los valores de las etiquetas de objeto distinguen entre mayúsculas y minúsculas. Debes ingresar estos elementos exactamente como fueron definidos para el objeto. |

**Especificar múltiples tipos y valores de metadatos**

Al definir el filtrado avanzado, puede especificar múltiples tipos de metadatos y múltiples valores de metadatos. Por ejemplo, si desea que una regla coincida con objetos entre 10 MB y 100 MB de tamaño, deberá seleccionar el tipo de metadatos **Tamaño del objeto** y especificar dos valores de metadatos.

- El primer valor de metadatos especifica objetos mayores o iguales a 10 MB.
- El segundo valor de metadatos especifica objetos menores o iguales a 100 MB.


El uso de múltiples entradas le permite tener un control preciso sobre qué objetos coinciden. En el siguiente ejemplo, la regla se aplica a los objetos que tienen Marca A o Marca B como valor de los metadatos de usuario camera_type. Sin embargo, la regla sólo se aplica a aquellos objetos de la marca B que tengan un tamaño inferior a 10 MB.




## Paso 2 de 3: Definir ubicaciones

El paso **Definir ubicaciones** del asistente Crear regla ILM le permite definir las instrucciones de ubicación que determinan durante cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y la cantidad de copias.

Las capturas de pantalla que se muestran son ejemplos. Los resultados pueden variar según la versión de StorageGRID .

**Acerca de esta tarea**

Una regla ILM puede incluir una o más instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo. Cuando se utiliza más de una instrucción, los períodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar el día 0. Las instrucciones pueden continuar indefinidamente o hasta que ya no necesite ninguna copia de objeto.

Cada instrucción de ubicación puede tener varias líneas si desea crear diferentes tipos de copias o utilizar diferentes ubicaciones durante ese período de tiempo.

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

**Pasos**

1. Para **Hora de referencia**, seleccione el tipo de hora que se utilizará al calcular la hora de inicio de una instrucción de ubicación.

| Opción | Descripción |
|---|---|
| Tiempo de ingesta | El momento en que se ingirió el objeto. |
| Hora del último acceso | La hora en que se recuperó el objeto por última vez (se leyó o se vio).<br><br>Para utilizar esta opción, las actualizaciones de la hora del último acceso deben estar habilitadas para el bucket S3. Consulte "Utilice la hora del último acceso en las reglas de ILM" . |
| Hora de creación definida por el usuario | Un tiempo especificado en metadatos definidos por el usuario. |
| Tiempo no actual | "Hora no actual" se selecciona automáticamente si seleccionó **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en buckets S3 con control de versiones habilitado)?" en"Paso 1 del asistente para crear una regla de ILM" . |

   Si desea crear una regla *compatible*, debe seleccionar **Tiempo de ingesta**. Consulte "Administrar objetos con S3 Object Lock" .

2. En la sección **Período de tiempo y ubicaciones**, ingrese una hora de inicio y una duración para el primer período de tiempo.

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

3. Si desea crear copias replicadas:
   a. En la lista desplegable **Almacenar objetos por**, seleccione **replicando**.
   b. Seleccione el número de copias que desea realizar.

      Aparece una advertencia si cambia el número de copias a 1. Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Consulte "Por qué no debería utilizar la replicación de copia única" .

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

      - Aumentar el número de copias para el período de tiempo.
      - Agregue copias a otros grupos de almacenamiento o a un grupo de almacenamiento en la nube.
      - Seleccione **codificación de borrado** en lugar de **replicación**.

        Puede ignorar esta advertencia de forma segura si esta regla ya crea múltiples copias para todos los períodos de tiempo.

   c. En el campo **copias en**, seleccione los grupos de almacenamiento que desea agregar.

      **Si especifica solo un grupo de almacenamiento**, tenga en cuenta que StorageGRID solo puede

almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento determinado. Si su red incluye tres nodos de almacenamiento y selecciona 4 como número de copias, solo se realizarán tres copias: una copia para cada nodo de almacenamiento.

La alerta **Colocación ILM inalcanzable** se activa para indicar que la regla ILM no se pudo aplicar por completo.

**Si especifica más de un grupo de almacenamiento**, tenga en cuenta estas reglas:

- La cantidad de copias no puede ser mayor que la cantidad de grupos de almacenamiento.
- Si la cantidad de copias es igual a la cantidad de grupos de almacenamiento, se almacena una copia del objeto en cada grupo de almacenamiento.
- Si la cantidad de copias es menor que la cantidad 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 y, al mismo tiempo, garantizar que ningún sitio obtenga más de una copia de un objeto.
- Si los grupos de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), todas las copias del objeto podrían guardarse en un solo sitio. Por este motivo, no especifique el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) y otro grupo de almacenamiento.

4. Si desea crear una copia con código de borrado:

   a. En la lista desplegable **Almacenar objetos por**, seleccione **codificación de borrado**.

   > La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

   b. Si no agregó un filtro de tamaño de objeto para un valor mayor a 200 KB, seleccione **Anterior** para regresar al Paso 1. Luego, seleccione **Agregar un filtro avanzado** y configure un filtro de **Tamaño de objeto** en cualquier valor mayor a 200 KB.

   c. Seleccione el grupo de almacenamiento que desea agregar y el esquema de codificación de borrado que desea utilizar.

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

   Los esquemas de codificación de borrado disponibles están limitados por la cantidad de nodos de almacenamiento en el grupo de almacenamiento que seleccione. A `Recommended` La insignia aparece junto a los esquemas que proporcionan el"La mejor protección o la menor sobrecarga de almacenamiento" .

5. Opcionalmente:

   a. Seleccione **Agregar otro tipo o ubicación** para crear copias adicionales en diferentes ubicaciones.

   b. Seleccione **Agregar otro período de tiempo** para agregar diferentes períodos de tiempo.

Las eliminaciones de objetos se producen según las siguientes configuraciones:

- Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que otro período de tiempo finalice **para siempre**.
- Dependiendo de"Configuración del período de retención de depósitos e inquilinos" Es posible que los objetos no se eliminen incluso si finaliza el período de retención de ILM.

6. Si desea almacenar objetos en un grupo de almacenamiento en la nube:
   a. En la lista desplegable **Almacenar objetos por**, seleccione **replicando**.
   b. Seleccione el campo **copias en** y luego seleccione un grupo de almacenamiento en la nube.

      Al utilizar grupos de almacenamiento en la nube, tenga en cuenta estas reglas:

      - No puede seleccionar más de un grupo de almacenamiento en la nube en una sola instrucción de ubicación. De manera similar, no es posible seleccionar un grupo de almacenamiento en la nube y un grupo de almacenamiento en la misma instrucción de ubicación.
      - Solo puedes almacenar una copia de un objeto en un grupo de almacenamiento en la nube determinado. Aparece un mensaje de error si configura **Copias** en 2 o más.
      - No es posible almacenar más de una copia de objeto en ningún grupo de almacenamiento en la nube al mismo tiempo. Aparece un mensaje de error si varias ubicaciones que utilizan un grupo de almacenamiento en la nube tienen fechas superpuestas o si varias líneas en la misma ubicación utilizan un grupo de almacenamiento en la nube.
      - Puede almacenar un objeto en un grupo de almacenamiento en la nube al mismo tiempo que ese objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debe incluir más de una línea en la instrucción de ubicación para el período de tiempo, de modo que pueda especificar la cantidad y los tipos de copias para cada ubicación.

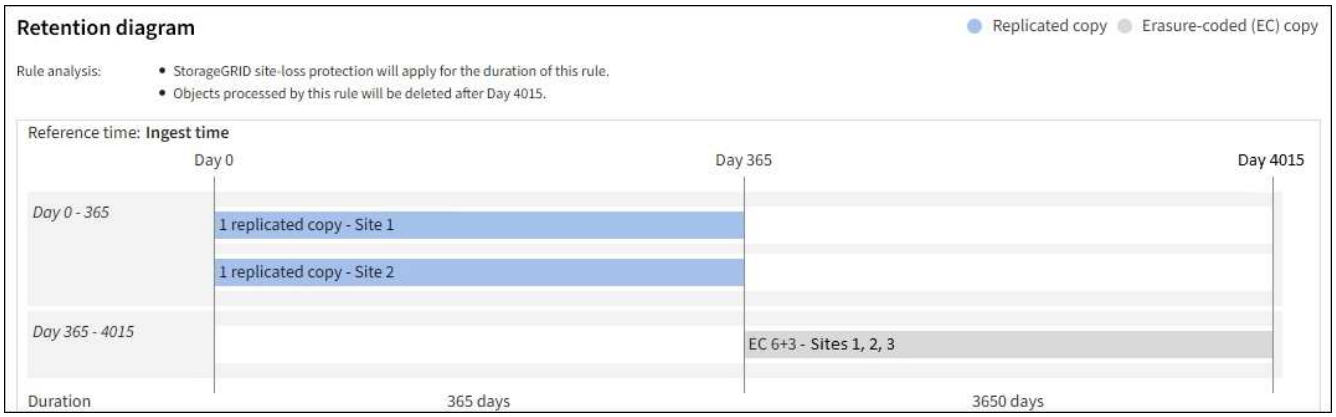
7. En el diagrama de retención, confirme sus instrucciones de ubicación.

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

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

   - La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
   - Los objetos procesados por esta regla se eliminarán después del día 4015.

     Consulte "Habilitar la protección contra pérdida del sitio."




8. Seleccione **Continuar**. "Paso 3 (Seleccionar el comportamiento de ingesta)"Aparece el asistente Crear una regla ILM.

## Utilice la hora del último acceso en las reglas de ILM

Puede utilizar la hora del último acceso como hora de referencia en una regla ILM. Por ejemplo, es posible que desee dejar objetos que se hayan visto en los últimos tres meses en nodos de almacenamiento locales, mientras que mueve objetos que no se hayan visto recientemente a una ubicación externa. También puede utilizar Hora del último acceso como filtro avanzado si desea que una regla 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 la hora del último acceso en una regla ILM, revise las siguientes consideraciones:

- Al utilizar la hora del último acceso como tiempo de referencia, tenga en cuenta que cambiar la hora del último acceso de un objeto no activa una evaluación ILM inmediata. En su lugar, se evalúan las ubicaciones del objeto y el objeto se mueve según sea necesario cuando ILM en segundo plano evalúa el objeto. Esto podría tomar dos semanas o más después de acceder al objeto.

  Tenga en cuenta esta latencia al crear reglas ILM basadas en el último tiempo de acceso y evite ubicaciones que utilicen períodos de tiempo cortos (menos de un mes).

- Al utilizar la Hora del último acceso como filtro avanzado o como hora de referencia, debe habilitar las actualizaciones de la Hora del último acceso para los buckets S3. Puedes utilizar el"Administrador de inquilinos" o el"API de gestión de inquilinos" .

> Las actualizaciones del último tiempo de acceso están deshabilitadas de manera predeterminada para los buckets S3.

> Tenga en cuenta que habilitar actualizaciones de la última hora de acceso puede reducir el rendimiento, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento se produce porque StorageGRID debe actualizar los objetos con nuevas marcas de tiempo cada vez que se recuperan los objetos.

La siguiente tabla resume si la hora del último acceso se actualiza para todos los objetos en el depósito para diferentes tipos de solicitudes.

| Tipo de solicitud | Si la hora del último acceso se actualiza cuando las actualizaciones de la hora del último acceso están deshabilitadas | Si la hora del último acceso se actualiza cuando se habilitan las actualizaciones de la hora del último acceso |
|---|---|---|
| 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 depósito a otro | • No, para la copia fuente<br>• Sí, para la copia de destino | • Sí, para la copia fuente<br>• Sí, para la copia de destino |
| Solicitud para completar una carga de varias partes | Sí, para el objeto ensamblado | Sí, para el objeto ensamblado |

## Paso 3 de 3: Seleccionar el comportamiento de ingesta

El paso **Seleccionar comportamiento de ingesta** del asistente Crear regla de ILM le permite elegir cómo se protegen los objetos filtrados por esta regla a medida que se ingieren.

### Acerca de esta tarea

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

### Pasos

1. Seleccione el"comportamiento de ingestión" Para utilizar.

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

   > No puedes usar la opción Equilibrado o Estricto si la regla utiliza una de estas ubicaciones:
   >
   > - Un grupo de almacenamiento en la nube en el día 0
   > - Un grupo de almacenamiento en la nube cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia
   >
   > Ver "Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto" .

2. Seleccione **Crear**.

   Se crea la regla ILM. La regla no se activa hasta que se agrega a una"Política de ILM" y esa política se activa.

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

## Crear una regla ILM predeterminada

Antes de crear una política ILM, debe crear una regla predeterminada para colocar cualquier objeto que no coincida con otra regla en la política. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los depósitos y todas las versiones de objetos.

### Antes de empezar

- Ha 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 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 en la política.

En esta política de ejemplo, la primera regla se aplica solo 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 inquilino.


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

- La regla predeterminada se colocará automáticamente como última regla cuando la agregue a una política.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones del objeto.
- La regla predeterminada debería crear copias replicadas.

No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deben utilizar un filtro avanzado para evitar que se codifiquen por borrado objetos más pequeños.

- En general, la regla predeterminada debería conservar los objetos para siempre.
- Si está utilizando (o planea habilitar) la configuración global de bloqueo de objetos S3, la regla predeterminada debe ser compatible.

**Pasos**

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

   Aparece el paso 1 (Ingresar detalles) del asistente Crear regla ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre de la regla**.
4. Opcionalmente, ingrese una breve descripción de la regla en el campo **Descripción**.
5. Deje el campo **Cuentas de inquilinos** en blanco.

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

6. Deje la selección desplegable del nombre del depósito como **se aplica a todos los depósitos**.

   La regla predeterminada debe aplicarse a todos los buckets S3.

7. Mantenga la respuesta predeterminada, **No**, para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?"
8. No agregue filtros avanzados.

   La regla predeterminada no puede especificar ningún filtro.

9. Seleccione **Siguiente**.

   Aparece el paso 2 (Definir ubicaciones).

10. Para el tiempo de referencia, seleccione cualquier opción.

    Si mantuvo la respuesta predeterminada, **No**, para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores?" La hora no actual no se incluirá en la lista desplegable. La regla predeterminada debe aplicarse a todas las versiones del objeto.

11. Especifique las instrucciones de ubicación para la regla predeterminada.
    - La regla predeterminada debería conservar los objetos para siempre. Aparece una advertencia cuando se activa una nueva política si la regla predeterminada no retiene los objetos para siempre. Debes confirmar que este es el comportamiento que esperas.
    - La regla predeterminada debería crear copias replicadas.

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

- Si está utilizando (o planea habilitar) la configuración global de Bloqueo de objetos S3, la regla predeterminada debe ser compatible:
  - Debe crear al menos dos copias del objeto replicado 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 grupo de almacenamiento en la nube.
  - Al menos una línea de las instrucciones de ubicación debe comenzar en el día 0, utilizando el tiempo de ingesta como tiempo de referencia.
  - Al menos una línea de las instrucciones de colocación debe ser "para siempre".

12. Mire el diagrama de retención para confirmar sus instrucciones de ubicación.
13. Seleccione **Continuar**.

    Aparece el paso 3 (Seleccionar comportamiento de ingesta).

14. Seleccione la opción de ingesta que desea utilizar y seleccione **Crear**.

# Administrar políticas de ILM

## Utilice las políticas de ILM

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

> Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irrecuperable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

### Política ILM predeterminada

Cuando instala StorageGRID y agrega sitios, se crea automáticamente una política ILM predeterminada, de la siguiente manera:

- Si su cuadrícula contiene un sitio, la política predeterminada contiene una regla predeterminada que replica dos copias de cada objeto en ese sitio.
- Si su cuadrícula contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

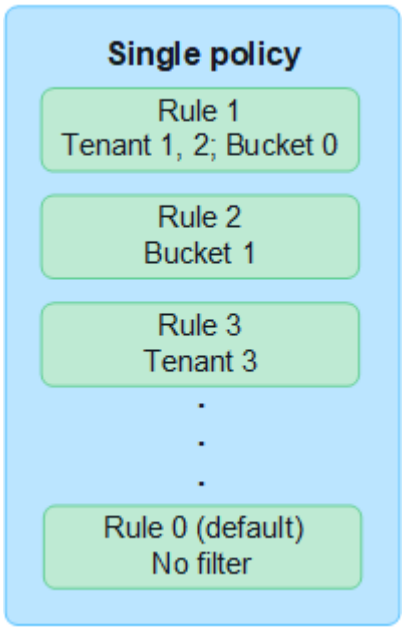
Si la política predeterminada no cumple con sus requisitos de almacenamiento, puede crear sus propias reglas y políticas. Ver"Crear una regla ILM" y"Crear una política ILM" .

### ¿Una o varias políticas ILM activas?

Puede tener una o más políticas ILM activas a la vez.

#### Una política

Si su red utilizará un esquema de protección de datos simple con pocas reglas específicas para cada inquilino y cada depósito, utilice una única política ILM activa. Las reglas de ILM pueden contener filtros para administrar diferentes grupos o inquilinos.




Cuando solo tiene una política y cambian los requisitos de un inquilino, debe crear una nueva política ILM o clonar la política existente para aplicar los cambios, simular y luego activar la nueva política ILM. Los cambios en la política de ILM podrían generar movimientos de objetos que podrían demorar muchos días y causar latencia del sistema.

#### Múltiples políticas

Para brindar diferentes opciones de calidad de servicio a los inquilinos, puede tener más de una póliza activa a la vez. Cada política puede administrar inquilinos, depósitos S3 y objetos específicos. Cuando se aplica o cambia una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

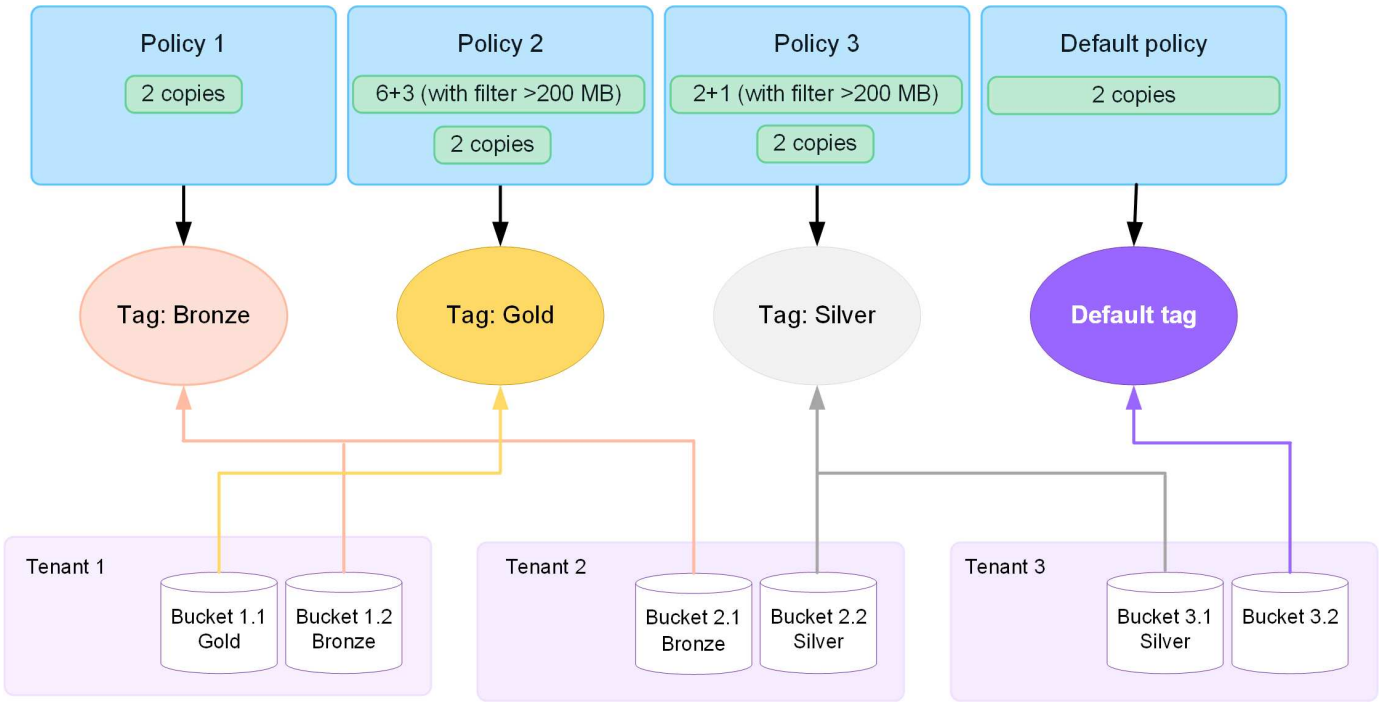
### Etiquetas de política de ILM

Si desea permitir que los inquilinos cambien fácilmente entre múltiples políticas de protección de datos por depósito, utilice múltiples políticas ILM con *etiquetas de política ILM*. Asigna cada política de ILM a una etiqueta y luego los inquilinos etiquetan un depósito para aplicar la política a ese depósito. Puede configurar etiquetas de política ILM solo en depósitos S3.

Por ejemplo, podría tener tres etiquetas denominadas Oro, Plata y Bronce. Puede asignar una política ILM a cada etiqueta, en función de cuánto tiempo y dónde esa política almacena los objetos. Los inquilinos pueden elegir qué política utilizar etiquetando sus áreas. Un depósito etiquetado como Oro es administrado por la política Oro y recibe el nivel Oro de protección de datos y rendimiento.

### Etiqueta de política ILM predeterminada

Se crea automáticamente una etiqueta de política ILM predeterminada cuando instala StorageGRID. Cada cuadrícula debe tener una política activa asignada a la etiqueta Predeterminada. La política predeterminada se aplica a cualquier depósito S3 sin etiquetar.




### ¿Cómo evalúa una política ILM los objetos?

Una política 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 en función del conjunto ordenado de reglas ILM en la política, de la siguiente manera:

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se ingiere de acuerdo con el comportamiento de ingesta de esa regla y se almacena de acuerdo con las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, este se evalúa en relación con cada regla posterior 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 en la política. La regla predeterminada es la última regla de una política. La regla predeterminada debe aplicarse a todos los inquilinos, todos los depósitos S3 y todas las versiones de objetos, y no puede usar ningún filtro avanzado.

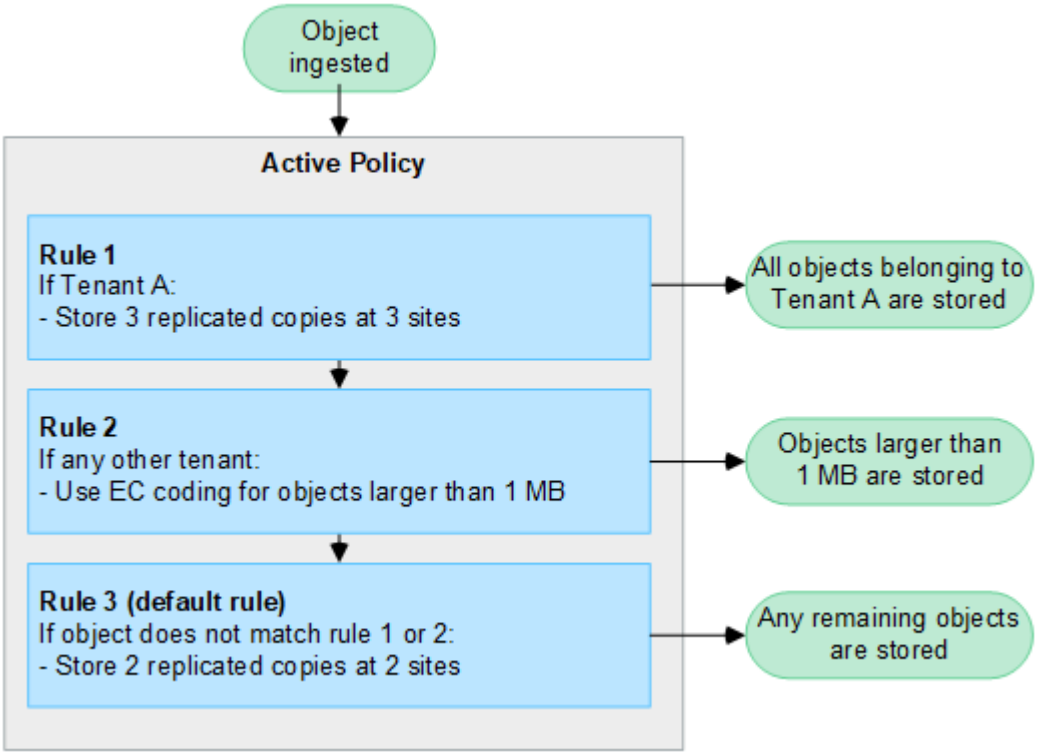
### Ejemplo de política ILM

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

- **Regla 1: Copias replicadas para el inquilino A**
  - Empareja todos los objetos que pertenecen al inquilino A.
  - Almacene estos objetos como tres copias replicadas en tres sitios.
  - Los objetos que pertenecen a otros inquilinos no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.
- **Regla 2: Codificación de borrado para objetos mayores a 1 MB**
  - Coincide con todos los objetos de otros inquilinos, pero solo si son mayores a 1 MB. Estos objetos más grandes se almacenan utilizando codificación de borrado 6+3 en tres sitios.

- No coincide con objetos de 1 MB o más pequeños, por lo que estos objetos se evalúan según la Regla 3.

- **Regla 3: 2 copias, 2 centros de datos** (predeterminado)
  - Es la última regla predeterminada de la política. No utiliza filtros.
  - Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenecen al Inquilino A y que tienen 1 MB o menos).




### ¿Qué son las políticas activas e inactivas?

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

Cuando crea por primera vez una política ILM, selecciona una o más reglas ILM y las organiza en un orden específico. Después de haber simulado la política para confirmar su comportamiento, actívela.

Cuando activa una política ILM, StorageGRID utiliza esa política para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Los objetos existentes podrían trasladarse a nuevas ubicaciones cuando se implementen las reglas ILM en la nueva política.

Si activa más de una política ILM a la vez y los inquilinos aplican etiquetas de política a los depósitos S3, los objetos en cada depósito se administran de acuerdo con la política asignada a la etiqueta.

Un sistema StorageGRID rastrea el historial de políticas que se han activado o desactivado.

### Consideraciones para la creación de una política ILM

- Utilice únicamente la política proporcionada por el sistema (política Baseline 2 copias) en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla Hacer 2 copias en esta política utiliza el grupo de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su

sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

> El grupo de almacenamiento Todos los nodos de almacenamiento se crea automáticamente durante la instalación de StorageGRID 11.6 y versiones anteriores. Si actualiza a una versión posterior de StorageGRID, el grupo de todos los nodos de almacenamiento seguirá existiendo. Si instala StorageGRID 11.7 o posterior como una instalación nueva, no se crea el grupo Todos los nodos de almacenamiento.

- Al diseñar una nueva política, tenga en cuenta todos los diferentes tipos de objetos que podrían incorporarse a su red. Asegúrese de que la política incluya reglas para hacer coincidir y colocar estos objetos según sea necesario.
- Mantenga la política de ILM lo más simple posible. Esto evita situaciones potencialmente peligrosas en las que los datos de los objetos no están protegidos como se espera cuando se realizan cambios en el sistema StorageGRID a lo largo del tiempo.
- Asegúrese de que las reglas de la política estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba. 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 en cada política ILM es la regla ILM predeterminada, que no puede usar ningún filtro. Si un objeto no ha sido emparejado con otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se conserva.
- Antes de activar una nueva política, revise cualquier cambio que la política esté realizando en la ubicación de los objetos existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

## Crear políticas ILM

Cree una o más políticas ILM para satisfacer sus requisitos de calidad de servicio.

Tener una política ILM activa le permite aplicar las mismas reglas ILM a todos los inquilinos y grupos.

Tener múltiples políticas ILM activas le permite aplicar las reglas ILM adecuadas a inquilinos y grupos específicos para cumplir con múltiples requisitos de calidad de servicio.

### Crear una política ILM

#### Acerca de esta tarea

Antes de crear su propia política, verifique que la"política ILM predeterminada" no cumple con sus requisitos de almacenamiento.

> Utilice únicamente las políticas proporcionadas por el sistema, 2 copias de la política (para redes de un sitio) o 1 copia por sitio (para redes de varios sitios), en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla predeterminada en esta política utiliza el grupo de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

Si el"Se ha habilitado la configuración global de bloqueo de objetos S3" , debe asegurarse de que la política ILM cumpla con los requisitos de los depósitos que tienen habilitado el bloqueo de objetos S3. En esta sección, siga las instrucciones que mencionan tener habilitado el bloqueo de objetos S3.

**Antes de empezar**

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"permisos de acceso necesarios" .
- Tienes"creó reglas ILM" dependiendo de si el bloqueo de objetos S3 está habilitado.

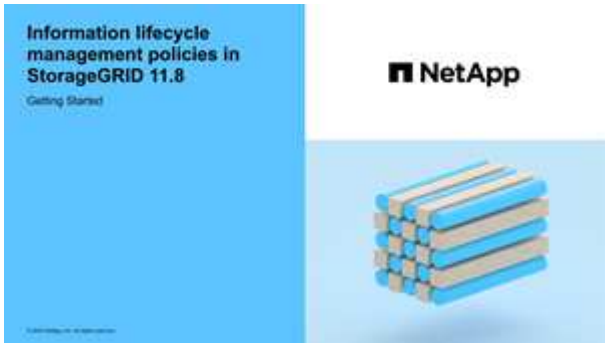
  **Bloqueo de objetos S3 no habilitado**

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

  **Bloqueo de objetos S3 habilitado**

  - El"La configuración global de bloqueo de objetos S3 ya está habilitada" para el sistema StorageGRID .
  - Tienes"creó las reglas ILM compatibles y no compatibles" desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y luego editar la política para agregar las nuevas reglas.
  - Tienes"creó una regla ILM predeterminada" para la política que se cumple.

- Opcionalmente has visto el vídeo: "Vídeo: Resumen de las políticas de ILM"




Consulte también "Utilice las políticas de ILM" .

**Pasos**

1. Seleccione **ILM** > **Políticas**.

   Si la configuración global de Bloqueo de objetos S3 está habilitada, la página de políticas de ILM indica qué reglas de ILM son compatibles.

2. Determine cómo desea crear la política ILM.

**Crear nueva política**

a. Seleccione **Crear política**.

**Clonar política existente**

a. Seleccione la casilla de verificación de la política con la que desea comenzar y luego seleccione **Clonar**.

**Editar la política existente**

a. Si una política está inactiva, puedes editarla. Seleccione la casilla de verificación de la política inactiva con la que desea comenzar y luego seleccione **Editar**.

3. En el campo **Nombre de la política**, ingrese un nombre único para la política.
4. Opcionalmente, en el campo **Motivo del cambio**, ingrese el motivo por el cual está creando una nueva política.
5. Para agregar reglas a la política, seleccione **Seleccionar reglas**. Seleccione un nombre de regla para ver la configuración de esa regla.

   Si está clonando una política:

   - Se seleccionan las reglas utilizadas por la política que estás clonando.
   - Si la política que está clonando utilizó reglas sin filtros que no eran la regla predeterminada, se le solicitará que elimine todas esas reglas excepto una.
   - Si la regla predeterminada utilizó un filtro, se le solicitará que seleccione una nueva regla predeterminada.
   - Si la regla predeterminada no fue la última regla, puede mover la regla al final de la nueva política.

**Bloqueo de objetos S3 no habilitado**

a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **Página de reglas ILM**.

   La regla predeterminada se aplica a cualquier objeto que no coincida con otra regla de la política. La regla predeterminada no puede usar ningún filtro y siempre se evalúa en último lugar.

   > No utilice la regla Hacer 2 copias como regla predeterminada para una política. La regla Hacer 2 copias utiliza un único grupo de almacenamiento, Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

**Bloqueo de objetos S3 habilitado**

a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **Página de reglas ILM**.

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

   > No utilice la regla Hacer 2 copias como regla predeterminada para una política. La regla Hacer 2 copias utiliza un único grupo de almacenamiento, Todos los nodos de almacenamiento, que contiene todos los sitios. Si utiliza esta regla, es posible que se coloquen varias copias de un objeto en el mismo sitio.

b. Si necesita una regla "predeterminada" diferente para los objetos en depósitos S3 no compatibles, seleccione **Incluir una regla sin filtros para depósitos S3 no compatibles** y seleccione una regla no compatible que no use un filtro.

   Por ejemplo, es posible que desee utilizar un grupo de almacenamiento en la nube para almacenar objetos en depósitos que no tengan habilitado el bloqueo de objetos S3.

   > Solo puede seleccionar una regla no compatible que no utilice un filtro.

Consulte también "Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3" .

6. Cuando haya terminado de seleccionar la regla predeterminada, seleccione **Continuar**.
7. Para el paso Otras reglas, seleccione cualquier otra regla que desee agregar a la política. Estas reglas utilizan al menos un filtro (cuenta de inquilino, nombre del depósito, filtro avanzado o tiempo de referencia no actual). Luego seleccione **Seleccionar**.

   La ventana Crear una política ahora enumera las reglas que seleccionó. La regla predeterminada está al final, con las demás reglas encima.

   Si el bloqueo de objetos S3 está habilitado y también seleccionó una regla "predeterminada" no compatible, esa regla se agrega como la segunda a la última regla en la política.

Aparece una advertencia si alguna regla no retiene los objetos para siempre. Cuando activa esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurran las instrucciones de ubicación de la regla predeterminada (a menos que un ciclo de vida de depósito conserve los objetos durante un período de tiempo más prolongado).

8. Arrastre las filas de las reglas no predeterminadas para determinar el orden en que se evaluarán estas reglas.

   No puedes mover la regla predeterminada. Si el bloqueo de objetos S3 está habilitado, tampoco podrá mover la regla "predeterminada" no compatible si se seleccionó una.

   Debes confirmar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba.

9. Según sea necesario, seleccione **Seleccionar reglas** para agregar o eliminar reglas.
10. Cuando haya terminado, seleccione **Guardar**.
11. Repita estos pasos para crear políticas ILM adicionales.
12. Simular una política ILM . Siempre debe simular una política antes de activarla para asegurarse de que funcione como se espera.

### Simular una política

Simule una política en objetos de prueba antes de activarla y aplicarla a sus datos de producción.

#### Antes de empezar

- Conoces la clave de objeto/depósito S3 para cada objeto que deseas probar.

#### Pasos

1. Usando un cliente S3 o el"Consola S3" , ingerir los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, seleccione la casilla de verificación de la política y luego seleccione **Simular**.
3. En el campo **Objeto**, ingrese el S3 `bucket/object-key` para un objeto de prueba. Por ejemplo, `bucket-01/filename.png` .
4. Si el control de versiones S3 está habilitado, ingrese opcionalmente un ID de versión para el objeto en el campo **ID de versión**.
5. Seleccione **Simular**.
6. En la sección Resultados de simulación, confirme que cada objeto coincidió con la regla correcta.
7. Para determinar qué grupo de almacenamiento o perfil de codificación de borrado está en vigor, seleccione el nombre de la regla coincidente para ir a la página de detalles de la regla.

   Revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

#### Resultados

Cualquier modificación a las reglas de la política se reflejará en los resultados de la simulación y mostrará el nuevo partido y el partido anterior. La ventana de política Simular conserva los objetos que probó hasta que

seleccione **Borrar todo** o el ícono de eliminar para cada objeto en la lista de resultados de simulación.

**Información relacionada**

"Ejemplo de simulaciones de políticas de ILM"

### Activar una política

Cuando se activa una única política ILM nueva, los objetos existentes y los objetos recientemente ingeridos son administrados por esa política. Cuando se activan varias políticas, las etiquetas de política ILM asignadas a los depósitos determinan los objetos que se deben administrar.

Antes de activar una nueva política:

1. Simule la política para confirmar que se comporta como espera.
2. Revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

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

**Acerca de esta tarea**

Cuando se activa una política 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 recibirla. En algunos casos, el sistema espera para implementar una nueva política activa para garantizar que los objetos de la cuadrícula no se eliminen accidentalmente. Específicamente:

- Si realiza cambios de política que **aumentan la redundancia o durabilidad de los datos**, esos cambios se implementan de inmediato. Por ejemplo, si activa una nueva política que incluye una regla de tres copias en lugar de una regla de dos copias, esa política se implementará de inmediato porque aumenta la redundancia de datos.
- Si realiza cambios de política que **podrían disminuir la redundancia o durabilidad de los datos**, dichos cambios no se implementarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activa una nueva política que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva política aparecerá en la pestaña Política activa, pero no tendrá efecto hasta que todos los nodos estén en línea y disponibles.

**Pasos**

Siga los pasos para activar una o varias políticas:

**Activar una política**

Siga estos pasos si solo tendrá una política activa. Si ya tiene una o más políticas activas y está activando políticas adicionales, siga los pasos para activar varias políticas.

1. Cuando esté listo para activar una política, seleccione **ILM** > **Políticas**.

   Alternativamente, puede activar una sola política desde la página **ILM** > **Etiquetas de política**.

2. En la pestaña Políticas, seleccione la casilla de verificación de la política que desea activar y luego seleccione **Activar**.
3. Siga el paso apropiado:
   - Si un mensaje de advertencia le solicita que confirme que desea activar la política, seleccione **Aceptar**.
   - Si aparece un mensaje de advertencia que contiene detalles sobre la política:
     i. Revise los detalles para asegurarse de que la política administre los datos como se espera.
     ii. Si la regla predeterminada almacena objetos durante una cantidad limitada de días, revise el diagrama de retención y luego escriba esa cantidad de días en el cuadro de texto.
     iii. Si la regla predeterminada almacena objetos para siempre, pero una o más reglas tienen una retención limitada, escriba **sí** en el cuadro de texto.
     iv. Seleccione **Activar política**.

**Activar múltiples políticas**

Para activar varias políticas, debe crear etiquetas y asignar una política a cada etiqueta.

Cuando se utilizan varias etiquetas, si los inquilinos reasignan con frecuencia etiquetas de políticas a los depósitos, el rendimiento de la red podría verse afectado. Si tiene inquilinos que no son de confianza, considere usar solo la etiqueta Predeterminada.

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

Los nombres y descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al momento de seleccionar etiquetas de políticas para asignar a sus grupos. Por ejemplo, si la política asignada eliminará objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

4. Seleccione **Crear etiqueta**.
5. En la tabla de etiquetas de políticas de ILM, utilice el menú desplegable para seleccionar una política para asignar a la etiqueta.
6. Si aparecen advertencias en la columna Limitaciones de la política, seleccione **Ver detalles de la política** para revisar la política.
7. Asegúrese de que cada política gestione los datos como se espera.
8. Seleccione **Activar políticas asignadas**. O seleccione **Borrar cambios** para eliminar la asignación

de política.

9. En el cuadro de diálogo Activar políticas con nuevas etiquetas, revise las descripciones de cómo cada etiqueta, política y regla administrará los objetos. Realice los cambios necesarios para garantizar que las políticas administren los objetos como se espera.
10. Cuando esté seguro de que desea activar las políticas, escriba **sí** en el cuadro de texto y luego seleccione **Activar políticas**.

**Información relacionada**

"Ejemplo 6: Cambiar una política de ILM"

## Ejemplo de simulaciones de políticas de ILM

Los ejemplos de simulaciones de políticas ILM proporcionan pautas para estructurar y modificar simulaciones para su entorno.

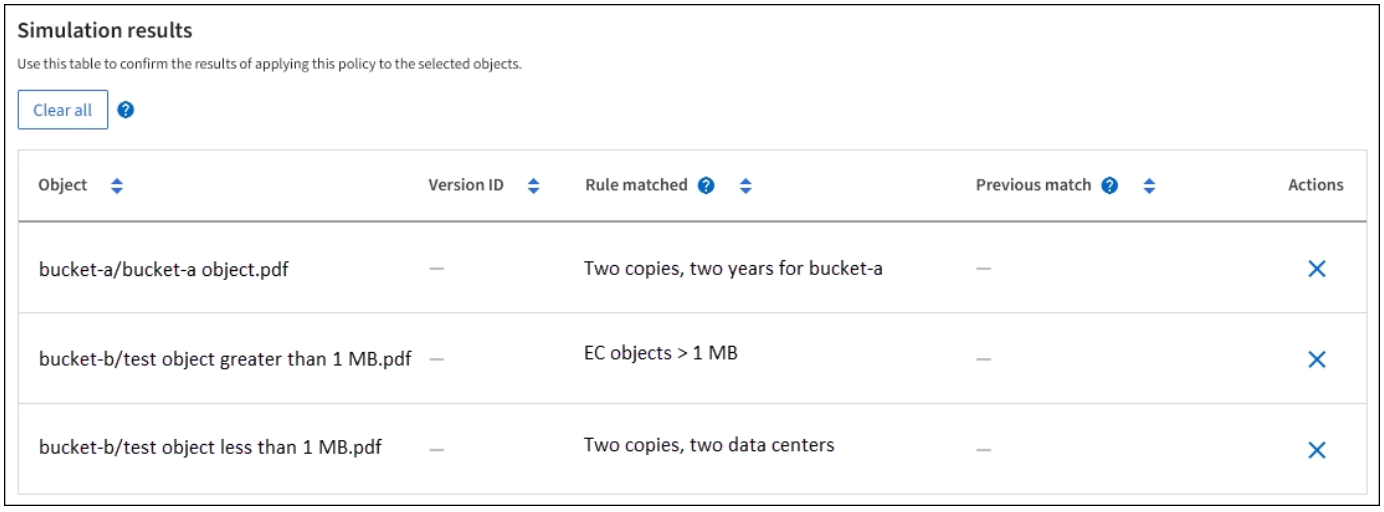
### Ejemplo 1: Verificar reglas al simular una política ILM

Este ejemplo describe cómo verificar reglas al simular una política.

En este ejemplo, se simula la **política ILM de ejemplo** contra los objetos ingeridos en dos buckets. La política incluye tres reglas, como sigue:

- La primera regla, **Dos copias, dos años para el contenedor a**, se aplica únicamente a los objetos del contenedor a.
- La segunda regla, **Objetos EC > 1 MB**, se aplica a todos los buckets, pero filtra los objetos mayores de 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 no actual.

Después de simular la política, confirme que cada objeto coincida con 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`está en `bucket-b , por lo que no coincidía con la primera regla. En cambio, la segunda regla coincidió correctamente, ya que filtra objetos de más de 1 MB.
- `bucket-b/test object less than 1 MB.pdf`no coincidió con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye filtros.

**Ejemplo 2: Reordenar reglas al simular una política ILM**

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

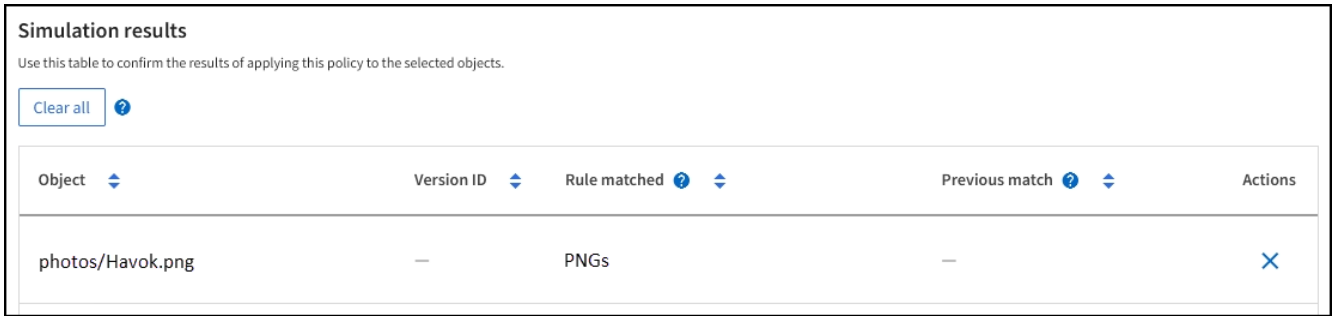
En este ejemplo, se está simulando la política **Demo**. Esta política, que tiene como objetivo encontrar objetos que tengan metadatos de usuario series=x-men, incluye tres reglas, como sigue:

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

**Pasos**

1. Después de agregar las reglas y guardar la política, seleccione **Simular**.
2. En el campo **Objeto**, ingrese la clave de objeto/depósito S3 para un objeto de prueba y seleccione **Simular**.

   Aparecen los resultados de la simulación, que muestran que `Havok.png` El objeto coincidió con la regla **PNGs**.

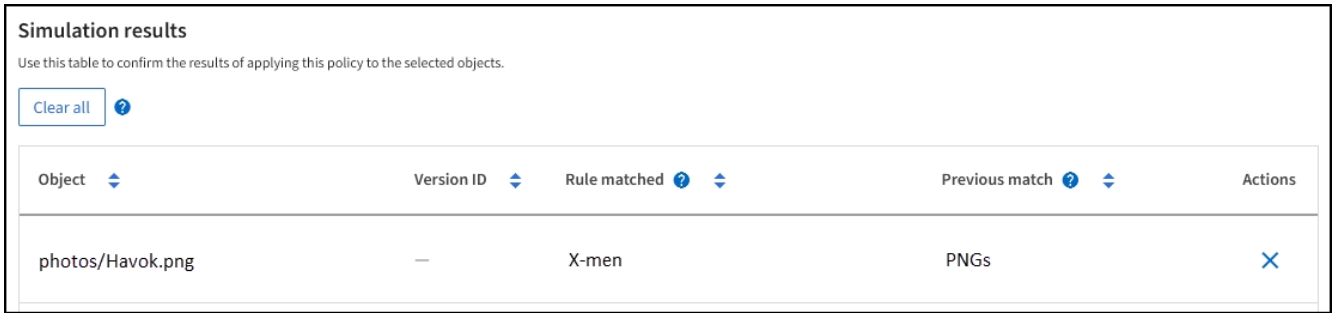



   Sin embargo, `Havok.png` Estaba destinado a probar la regla de los **X-men**.

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

   Los objetos que probó anteriormente se vuelven a evaluar en función de la política actualizada y se muestran los nuevos resultados de la simulación. En el ejemplo, la columna Regla coincidente muestra que `Havok.png` El objeto ahora coincide con la regla de metadatos de X-Men, como se esperaba. La

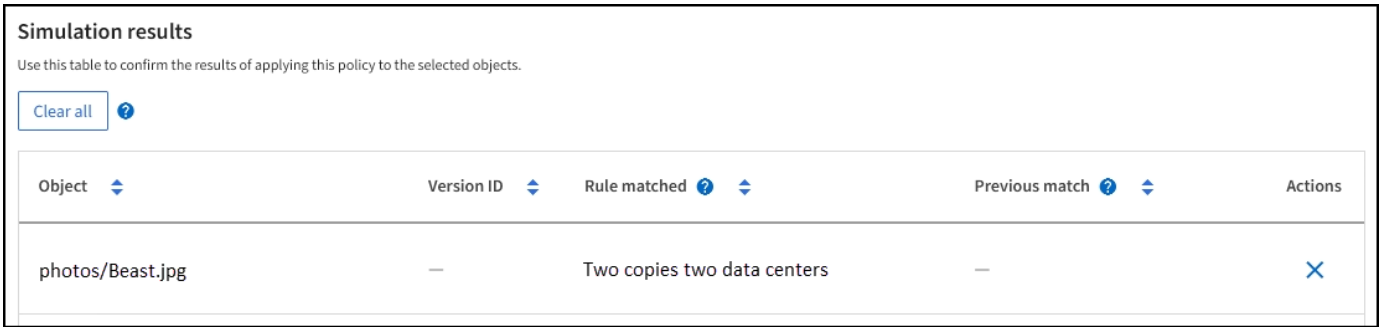
columna Coincidencia anterior muestra que la regla PNG coincidió con el objeto en la simulación anterior.




### Ejemplo 3: Corregir una regla al simular una política 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 tiene como objetivo encontrar objetos que tengan `series=x-men` metadatos del usuario. Sin embargo, se produjeron resultados inesperados al simular esta política contra la `Beast.jpg` objeto. En lugar de coincidir con la regla de metadatos de X-Men, el objeto coincidió con la regla predeterminada: Dos copias, dos centros de datos.




Cuando un objeto de prueba no coincide con la regla esperada en la política, debe examinar cada regla en la política y corregir cualquier error.

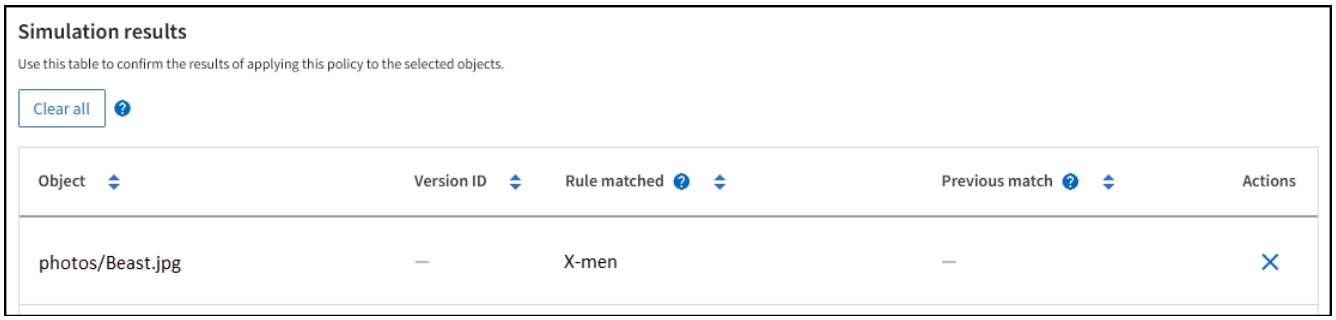
**Pasos**

1. Seleccione **Finalizar** para cerrar el cuadro de diálogo Simular política. En la página de detalles de la política, seleccione **Diagrama de retención**. Luego, seleccione **Expandir todo** o **Ver detalles** para cada regla según sea necesario.
2. Revise la cuenta de inquilino de la regla, el tiempo de referencia y los criterios de filtrado.

   A modo de ejemplo, supongamos que los metadatos para la regla de X-men se ingresaron como "x-men01" en lugar de "x-men".

3. Para resolver el error, corrija la regla de la siguiente manera:
   - Si la regla es parte de la política, puede clonar la regla o eliminarla de la política y luego editarla.
   - Si la regla es parte de la política activa, debe clonar la regla. No se puede editar ni eliminar una regla de la política activa.
4. Realice la simulación nuevamente.

   En este ejemplo, la regla corregida de los X-Men ahora coincide con la `Beast.jpg` objeto basado en el `series=x-men` metadatos del usuario, como se esperaba.




## Administrar etiquetas de políticas de ILM

Puede ver los detalles de la etiqueta de política de ILM, editar una etiqueta o eliminar una etiqueta.

### Antes de empezar

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

### Ver detalles de la etiqueta de política de ILM

Para ver los detalles de una etiqueta:

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

### Editar la etiqueta de política de ILM

> Los nombres y descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al momento de seleccionar etiquetas de políticas para asignar a sus grupos. Por ejemplo, si la política asignada eliminará objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

Para editar la descripción de una etiqueta existente:

1. Seleccione **ILM** > **Etiquetas de política**.
2. Seleccione la casilla de verificación de la etiqueta y luego seleccione **Editar**.

   Alternativamente, seleccione el nombre de la etiqueta. Aparecerá la página de detalles de la etiqueta y podrás seleccionar **Editar** en esa página.

3. Cambie la descripción de la etiqueta según sea necesario
4. Seleccione **Guardar**.

#### Eliminar la etiqueta de política de ILM

Cuando se elimina una etiqueta de política, a todos los depósitos que tengan asignada esa etiqueta se les aplicará la política predeterminada.

Para eliminar una etiqueta:

1. Seleccione **ILM** > **Etiquetas de política**.
2. Seleccione la casilla de verificación de la etiqueta y luego seleccione **Eliminar**. Aparece un cuadro de diálogo de confirmación.

   Alternativamente, seleccione el nombre de la etiqueta. Aparecerá la página de detalles de la etiqueta y podrás seleccionar **Eliminar** en esa página.

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

## Verificar una política de ILM con la búsqueda de metadatos de objetos

Después de haber activado una política ILM, ingiera objetos de prueba representativos en el sistema StorageGRID y luego realice una búsqueda de metadatos de objetos para confirmar que se estén realizando copias según lo previsto y se estén colocando en las ubicaciones correctas.

#### Antes de empezar

Tiene un identificador de objeto, que puede ser uno de los siguientes: * **UUID**: el identificador único universal del objeto. * **CBID**: El identificador único del objeto dentro de StorageGRID. Puede obtener el CBID de un objeto desde el registro de auditoría. Introduzca el CBD en mayúsculas. ***Clave de objeto y depósito S3**: cuando se ingiere un objeto a través de la interfaz S3, la aplicación cliente utiliza una combinación de clave de objeto y depósito para almacenar e identificar el objeto. Si el bucket S3 tiene versiones y desea buscar una versión específica de un objeto S3 usando la clave del bucket y del objeto, tendrá el **ID de versión**.

#### Pasos

1. Ingerir el objeto.
2. Seleccione **ILM** > **Búsqueda de metadatos de objetos**.
3. Escriba el identificador del objeto en el campo **Identificador**. Puede ingresar un UUID, CBID o una clave de objeto/depósito S3.
4. Opcionalmente, ingrese un ID de versión para el objeto (sólo S3).
5. Seleccione **Buscar**.

   Aparecen los resultados de la búsqueda de metadatos del objeto. En esta página se enumeran los siguientes tipos de información:

   - Metadatos del sistema, como ID de objeto (UUID), tipo de resultado (objeto, marcador de eliminación, depósito S3) y tamaño lógico del objeto. Consulte la captura de pantalla de ejemplo a continuación para obtener más detalles.
   - Cualquier par clave-valor de metadatos de usuario personalizados asociados con el objeto.
   - Para los objetos S3, cualquier par clave-valor de etiqueta de objeto asociado con el objeto.
   - Para copias de objetos replicados, la ubicación de almacenamiento actual de cada copia.
   - Para las copias de objetos con código de borrado, la ubicación de almacenamiento actual de cada

fragmento.

- Para las copias de objetos en un grupo de almacenamiento en la nube, la ubicación del objeto, incluido el nombre del depósito externo y el identificador único del objeto.
- Para objetos segmentados y objetos multiparte, una lista de segmentos de objetos que incluye identificadores de segmento y tamaños de datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
- Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema que no se garantiza que persistan de una versión a otra.

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

   Si la opción Auditoría está habilitada, también puede supervisar el registro de auditoría para el mensaje Reglas de objeto ORLM cumplidas. El mensaje de auditoría de ORLM puede brindarle más información sobre el estado del proceso de evaluación de ILM, pero no puede brindarle información sobre la exactitud de la ubicación de los datos del objeto ni sobre la integridad de la política de ILM. Debes evaluar esto tú mismo. Para obtener más información, consulte "Revisar los registros de auditoría" .

El siguiente ejemplo muestra los resultados de la búsqueda de metadatos de un objeto de prueba S3 que se almacena como dos copias replicadas.

> La siguiente captura de pantalla es un ejemplo. Los resultados variarán según la 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**


**Información relacionada**

"Utilice la API REST de S3"

# Trabajar con políticas y reglas de ILM

A medida que cambian sus requisitos de almacenamiento, es posible que necesite implementar políticas adicionales o modificar las reglas de ILM asociadas con una política. Puede ver las métricas de ILM para determinar el rendimiento del sistema.

**Antes de empezar**

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

## Ver las políticas de ILM

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

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

> Si visualiza los detalles de una política cuyo estado es Editado o Eliminado, aparece un mensaje que explica que está visualizando la versión de la política que estuvo activa durante el período de tiempo especificado y que desde entonces ha sido editada o eliminada.

## Editar una política de ILM

Sólo puedes editar una política inactiva. Si desea editar una política activa, desactívela o cree un clon y edítelo.

Para editar una política:

1. Seleccione **ILM** > **Políticas**.
2. Seleccione la casilla de verificación de la política que desea editar y luego seleccione **Editar**.
3. Edite la política siguiendo las instrucciones en"Crear políticas ILM" .
4. Simule la política antes de reactivarla.

> Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irrecuperable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

## Clonar una política de ILM

Para clonar una política ILM:

1. Seleccione **ILM** > **Políticas**.
2. Seleccione la casilla de verificación de la política que desea clonar y luego seleccione **Clonar**.
3. Cree una nueva política a partir de la política que ha clonado siguiendo las instrucciones en"Crear políticas ILM" .

> Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irrecuperable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

## Eliminar una política de ILM

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

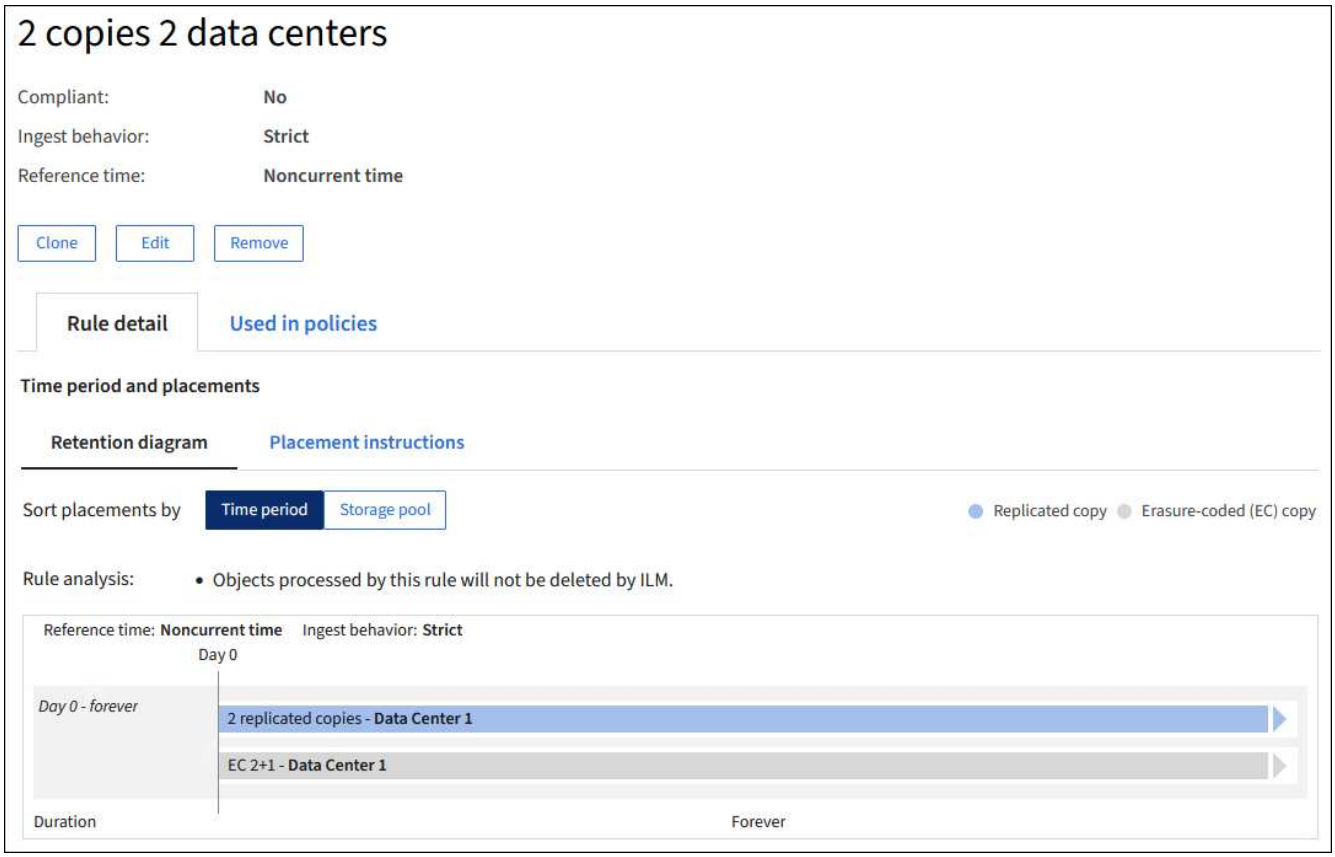
1. Seleccione **ILM** > **Políticas**.

2. Seleccione la casilla de verificación de la política inactiva que desea eliminar.
3. Seleccione **Eliminar**.

## Ver detalles de las reglas de ILM

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

1. Seleccione **ILM** > **Reglas**.
2. Seleccione el nombre de la regla cuyos detalles desea ver. Ejemplo:




Además, puede 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 ILM

Puede clonar una regla existente si desea crear una nueva regla que utilice algunas de las configuraciones de la regla existente. Si necesita editar una regla que se utiliza en alguna política, debe clonar la regla y realizar cambios en el clon. Después de realizar cambios en el clon, puede eliminar la regla original de la política y reemplazarla con la versión modificada según sea necesario.

No se puede clonar una regla ILM si se creó utilizando StorageGRID versión 10.2 o anterior.

**Pasos**

1. Seleccione **ILM** > **Reglas**.
2. Seleccione la casilla de verificación de la regla que desea clonar y luego seleccione **Clonar**.

Alternativamente, seleccione el nombre de la regla y luego seleccione **Clonar** en la página de detalles de la regla.

3. Actualice la regla clonada siguiendo los pasos paraeditar una regla ILM y"Uso de filtros avanzados en las reglas de ILM" .

   Al clonar una regla ILM, debe ingresar un nuevo nombre.

## Editar una regla de ILM

Es posible que necesite editar una regla ILM para cambiar un filtro o una instrucción de ubicación.

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

> Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irrecuperable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

**Pasos**

1. Seleccione **ILM** > **Reglas**.
2. Confirme que la regla que desea editar no se utiliza en ninguna política de ILM.
3. Si la regla que desea editar no está en uso, seleccione la casilla de verificación de la regla y seleccione **Acciones** > **Editar**. Alternativamente, seleccione el nombre de la regla y luego seleccione **Editar** en la página de detalles de la regla.
4. Complete los pasos del asistente Editar regla de ILM. Según sea necesario, siga los pasos para"creando una regla ILM" y"Uso de filtros avanzados en las reglas de ILM" .

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

## Eliminar una regla ILM

Para mantener manejable la lista de reglas ILM actuales, elimine cualquier regla ILM que probablemente no utilice.

**Pasos**

Para eliminar una regla ILM que se utiliza actualmente en una política activa:

1. Clonar la política.
2. Eliminar la regla ILM del clon de política.
3. Guarde, simule y active la nueva política para asegurarse de que los objetos estén protegidos como se espera.
4. Vaya a los pasos para eliminar una regla ILM que se utiliza actualmente en una política inactiva.

Para eliminar una regla ILM que se utiliza actualmente en una política inactiva:

1. Seleccione la política inactiva.
2. Eliminar la regla ILM de la política oeliminar la política .

3. Vaya a los pasos para eliminar una regla ILM que no se utiliza actualmente.

Para eliminar una regla ILM que no se utiliza actualmente:

1. Seleccione **ILM** > **Reglas**.
2. Confirme que la regla que desea eliminar no se utiliza en ninguna política.
3. Si la regla que desea eliminar no está en uso, selecciónela y seleccione **Acciones** > **Eliminar**. Puede seleccionar varias reglas y eliminarlas todas al mismo tiempo.
4. Seleccione **Sí** para confirmar que desea eliminar la regla ILM.

## Ver métricas de ILM

Puede ver métricas de ILM, como la cantidad de objetos en la cola y la tasa de evaluación. Puede supervisar estas métricas para determinar el rendimiento del sistema. Una cola o tasa de evaluación grande podría indicar que el sistema no puede mantener el ritmo de la tasa de ingesta, que la carga de las aplicaciones cliente es excesiva o que existe alguna condición anormal.

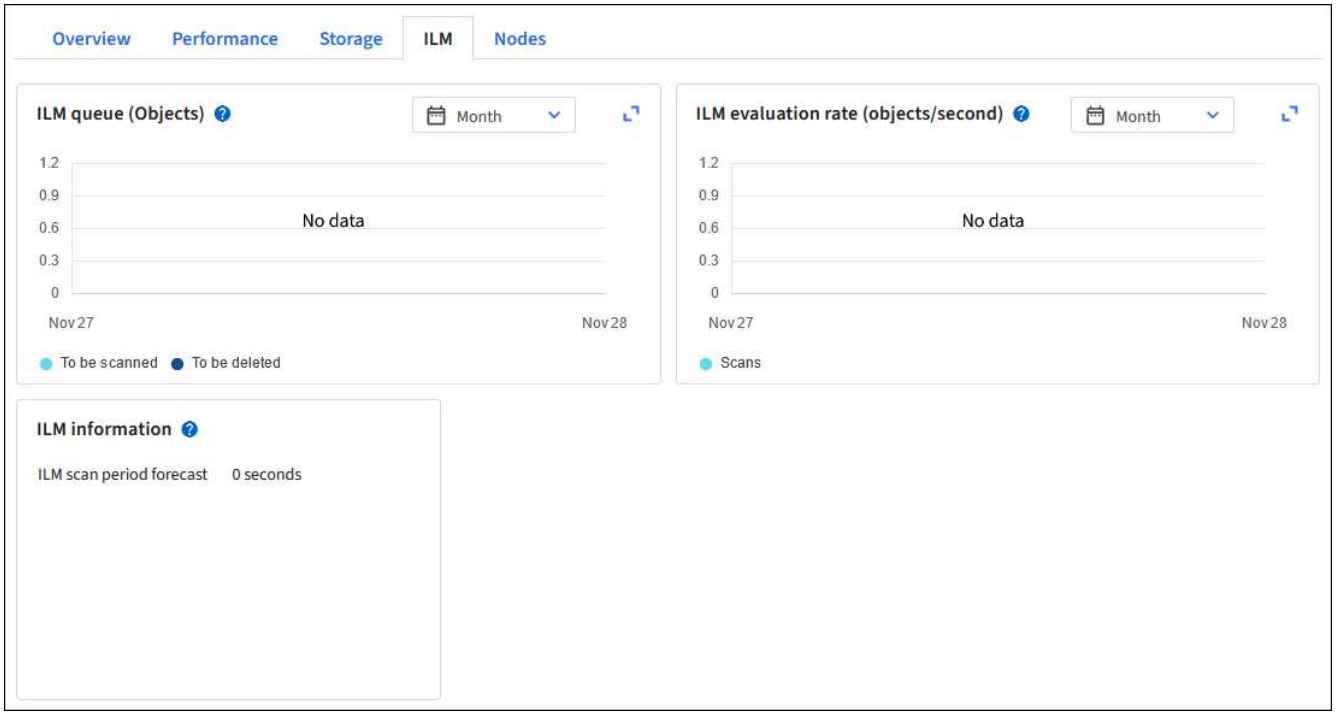
**Pasos**

1. Seleccione **Panel de control** > **ILM**.

   Debido a que el panel se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervise las métricas en la pestaña ILM.

   Puedes seleccionar el signo de interrogación para ver una descripción de los elementos en la pestaña ILM.



# Usar bloqueo de objetos S3

## Administrar objetos con S3 Object Lock

Como administrador de la red, puede habilitar el bloqueo de objetos S3 para su sistema StorageGRID e implementar una política ILM compatible para ayudar a garantizar que los objetos en depósitos S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo específico.

### ¿Qué es el bloqueo de objetos S3?

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

Cuando la configuración global de Bloqueo de objetos S3 está habilitada para un sistema StorageGRID , una cuenta de inquilino S3 puede crear depósitos con o sin el Bloqueo de objetos S3 habilitado. Si un bucket tiene habilitado el bloqueo de objetos S3, se requiere el control de versiones del bucket y se habilita automáticamente.

**Un depósito sin bloqueo de objetos S3** solo puede tener objetos sin configuraciones de retención especificadas. Ningún objeto ingerido tendrá configuraciones de retención.

**Un depósito con bloqueo de objetos S3** puede tener objetos con y sin configuraciones de retención especificadas por las aplicaciones cliente S3. Algunos objetos ingeridos tendrán configuraciones de retención.

**Un depósito con bloqueo de objetos S3 y retención predeterminada configurada** puede tener objetos cargados con configuraciones de retención especificadas y objetos nuevos sin configuraciones de retención. Los nuevos objetos utilizan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

De hecho, todos los objetos recién ingeridos tienen configuraciones de retención cuando se configura la retención predeterminada. Los objetos existentes sin configuraciones de retención de objetos no se verán afectados.

#### Modos de retención

La función de bloqueo de objetos de StorageGRID S3 admite dos modos de retención para aplicar diferentes 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 conservación.
  - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
  - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo de gobernanza:
  - Los usuarios con permiso especial pueden usar un encabezado de omisión en las solicitudes para modificar ciertas configuraciones de retención.
  - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

#### Configuración de retención para versiones de objetos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden usar la aplicación cliente S3 para especificar opcionalmente las siguientes configuraciones de retención para cada objeto que se agregue al depósito:

- **Modo de retención**: Cumplimiento o gobernanza.
- **Conservar hasta fecha**: si la fecha de conservación de una versión de un objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente. Las retenciones legales son independientes de la fecha de conservación.

> Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener detalles sobre la configuración de los objetos, consulte"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .

#### Configuración de retención predeterminada para depósitos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden especificar opcionalmente las siguientes configuraciones predeterminadas para el depósito:

- **Modo de retención predeterminado**: Cumplimiento o gobernanza.
- **Período de retención predeterminado**: durante cuánto tiempo se deben conservar las nuevas versiones de objetos agregadas a este depósito, a partir del día en que se agregan.

La configuración de depósito predeterminada se aplica únicamente a los objetos nuevos que no tienen su propia configuración de retención. Los objetos de bucket existentes no se ven afectados cuando agrega o cambia estas configuraciones predeterminadas.

Ver"Crear un bucket S3" y"Actualizar la retención predeterminada de bloqueo de objetos S3" .

### Comparación del bloqueo de objetos S3 con la conformidad heredada

El bloqueo de objetos S3 reemplaza la función de Cumplimiento que estaba disponible en versiones anteriores de StorageGRID . Debido a que la función de bloqueo de objetos S3 se ajusta a los requisitos de Amazon S3, deja obsoleta la función de cumplimiento patentada de StorageGRID , que ahora se denomina "cumplimiento heredado".

> La configuración de Cumplimiento global está obsoleta. Si habilitó esta configuración utilizando una versión anterior de StorageGRID, la configuración de Bloqueo de objetos S3 se habilita automáticamente. Puede seguir usando StorageGRID para administrar las configuraciones de los depósitos compatibles existentes; sin embargo, no puede crear depósitos compatibles nuevos. Para más detalles, consulte "Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5" .

Si utilizó la función de Cumplimiento heredada en una versión anterior de StorageGRID, consulte la siguiente tabla para saber cómo se compara con la función de Bloqueo de objetos S3 en StorageGRID.

| | Bloqueo de objetos S3 | Cumplimiento (legado) |
|---|---|---|
| ¿Cómo se habilita la función a nivel global? | Desde el Administrador de cuadrícula, seleccione **CONFIGURACIÓN** > **Sistema** > **Bloqueo de objetos S3**. | Ya no se admite. |
| ¿Cómo se habilita la función para un bucket? | Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3. | Ya no se admite. |
| ¿Se admite el control de versiones del bucket? | Sí. El control de versiones del depósito es necesario y se habilita automáticamente cuando S3 Object Lock está habilitado para el depósito. | No. |
| ¿Cómo se establece la retención de objetos? | Los usuarios pueden establecer una fecha de retención para cada versión del objeto o pueden establecer un período de retención predeterminado para cada depósito. | Los usuarios deben establecer un período de retención para todo el depósito. El período de retención se aplica a todos los objetos del depósito. |
| ¿Se puede modificar el periodo de conservación? | • En el modo de cumplimiento, la fecha de retención para una versión de objeto se puede aumentar, pero nunca disminuir.<br>• En el modo de gobernanza, los usuarios con permisos especiales pueden disminuir o incluso eliminar la configuración de retención de un objeto. | El período de retención de un depósito se puede aumentar, pero nunca disminuir. |
| ¿Dónde se controla la retención legal? | Los usuarios pueden colocar una retención legal o levantar una retención legal para cualquier versión de objeto en el depósito. | Se coloca una retención legal en el cubo y afecta a todos los objetos que se encuentran en el cubo. |

| | Bloqueo de objetos S3 | Cumplimiento (legado) |
|---|---|---|
| ¿Cuándo se pueden eliminar objetos? | • En el modo de cumplimiento, se puede eliminar una versión de un objeto una vez alcanzada la fecha de retención, siempre que el objeto no esté bajo retención legal.<br>• En el modo de gobernanza, los usuarios con permisos especiales pueden eliminar un objeto antes de que se alcance su fecha de retención, siempre que el objeto no esté bajo retención legal. | Se puede eliminar un objeto una vez que expire el período de retención, siempre que el depósito no esté bajo retención legal. Los objetos se pueden eliminar de forma automática o manual. |
| ¿Se admite la configuración del ciclo de vida del bucket? | Sí | No |

## Tareas de bloqueo de objetos S3

Como administrador de la red, debe coordinarse estrechamente con los usuarios inquilinos para garantizar que los objetos estén protegidos de una manera que satisfaga sus requisitos de retención.

> La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

Las siguientes listas para administradores de red y usuarios inquilinos contienen las tareas de alto nivel para usar la función de bloqueo de objetos S3.

**Administrador de red**

- Habilite la configuración global de bloqueo de objetos S3 para todo el sistema StorageGRID .
- Asegúrese de que las políticas de gestión del ciclo de vida de la información (ILM) sean *compatibles*; es decir, que cumplan con los requisitos"Requisitos de los buckets con bloqueo de objetos S3 habilitado" .
- Según sea necesario, permita que un inquilino utilice Cumplimiento como modo de retención. De lo contrario, solo se permite el modo Gobernanza.
- Según sea necesario, establezca un período máximo de retención para un inquilino.

**Usuario inquilino**

- Revise las consideraciones para depósitos y objetos con bloqueo de objetos S3.
- Según sea necesario, comuníquese con el administrador de la red para habilitar la configuración global de bloqueo de objetos S3 y establecer permisos.
- Cree depósitos con el bloqueo de objetos S3 habilitado.
- De manera opcional, configure los ajustes de retención predeterminados para un depósito:

    - Modo de retención predeterminado: Gobernanza o Cumplimiento, si lo permite el administrador de la red.
    - Período de retención predeterminado: debe ser menor o igual al período de retención máximo establecido por el administrador de la red.
- Utilice la aplicación cliente S3 para agregar objetos y, opcionalmente, configurar la retención específica de objetos:
    - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la red.
    - Conservar hasta la fecha: debe ser menor o igual a lo permitido por el período máximo de retención establecido por el administrador de la red.

## Requisitos para el bloqueo de objetos S3

Debe revisar los requisitos para habilitar la configuración global de Bloqueo de objetos S3, los requisitos para crear reglas y políticas ILM compatibles y las restricciones que StorageGRID impone a los depósitos y objetos que usan Bloqueo de objetos S3.

### Requisitos para utilizar la configuración global de bloqueo de objetos S3

- Debe habilitar la configuración global de Bloqueo de objetos S3 mediante el Administrador de cuadrícula o la API de administración de cuadrícula antes de que cualquier inquilino de S3 pueda crear un depósito con el Bloqueo de objetos S3 habilitado.
- Al habilitar la configuración global de Bloqueo de objetos S3, se permite que todas las cuentas de inquilinos de S3 creen depósitos con el Bloqueo de objetos S3 habilitado.
- Después de habilitar la configuración global de Bloqueo de objetos S3, no podrá deshabilitarla.
- No se puede habilitar el bloqueo de objetos S3 global a menos que la regla predeterminada en todas las políticas ILM activas sea *compatible* (es decir, la regla predeterminada debe cumplir con los requisitos de los depósitos con el bloqueo de objetos S3 habilitado).
- Cuando la configuración global de Bloqueo de objetos S3 está habilitada, no puede crear una nueva política ILM ni activar una política ILM existente a menos que la regla predeterminada en la política sea compatible. Una vez habilitada la configuración global de bloqueo de objetos S3, las páginas de reglas ILM y políticas ILM indican qué reglas ILM son compatibles.

### Requisitos para el cumplimiento de las normas ILM

Si desea habilitar la configuración global de bloqueo de objetos S3, debe asegurarse de que la regla predeterminada en todas las políticas ILM activas sea compatible. Una regla compatible satisface los requisitos de ambos depósitos con S3 Object Lock habilitado y de cualquier depósito existente que tenga habilitada la conformidad heredada:

- Debe crear al menos dos copias del objeto replicado 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 grupo de almacenamiento en la nube.
- Al menos una línea de las instrucciones de ubicación debe comenzar en el día 0, utilizando **Hora de ingesta** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación debe ser "para siempre".

### Requisitos para las políticas de ILM

Cuando la configuración global de Bloqueo de objetos S3 está habilitada, las políticas ILM activas e inactivas pueden incluir reglas compatibles y no compatibles.

- La regla predeterminada en una política ILM activa o inactiva debe ser compatible.
- Las reglas no conformes solo se aplican a los objetos en depósitos que no tienen habilitado el Bloqueo de objetos S3 o que no tienen habilitada la función de Cumplimiento heredada.
- Las reglas compatibles se pueden aplicar a objetos en cualquier bucket; no es necesario habilitar S3 Object Lock ni la conformidad heredada para el bucket.

"Ejemplo de una política ILM compatible con el bloqueo de objetos S3"

### Requisitos para los buckets con el bloqueo de objetos S3 habilitado

- Si la configuración global de Bloqueo de objetos S3 está habilitada para el sistema StorageGRID , puede usar el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3 para crear depósitos con el Bloqueo de objetos S3 habilitado.
- Si planea utilizar S3 Object Lock, debe habilitar S3 Object Lock cuando cree el depósito. No se puede habilitar el bloqueo de objetos S3 para un depósito existente.
- Cuando S3 Object Lock está habilitado para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención predeterminado y un período de retención para cada depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3. La configuración de retención predeterminada del depósito se aplica únicamente a los objetos nuevos agregados al depósito que no tienen su propia configuración de retención. Puede anular estas configuraciones predeterminadas especificando un modo de retención y una fecha de retención para cada versión del objeto cuando se carga.
- La configuración del ciclo de vida del bucket es compatible con los buckets que tienen el bloqueo de objetos S3 habilitado.
- La replicación de CloudMirror no es compatible con depósitos con el bloqueo de objetos S3 habilitado.

### Requisitos para objetos en depósitos con bloqueo de objetos S3 habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el depósito o puede especificar la configuración de retención para cada versión de objeto. Las configuraciones de retención a nivel de objeto se pueden especificar mediante la aplicación cliente S3 o la API REST S3.
- Las configuraciones de retención se aplican a versiones de objetos individuales. Una versión de objeto puede tener una configuración de conservación hasta la fecha y una configuración de conservación legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta la fecha o de retención legal para un objeto, se protege únicamente la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras la versión anterior del objeto permanece bloqueada.

### Ciclo de vida de objetos en buckets con S3 Object Lock habilitado

Cada objeto que se guarda en un bucket con el bloqueo de objetos S3 habilitado pasa por estas etapas:

1. **Ingesta de objeto**

Cuando se agrega una versión de objeto a un depósito que tiene habilitado el Bloqueo de objetos S3, las configuraciones de retención se aplican de la siguiente manera:

- Si se especifican configuraciones de retención para el objeto, se aplican las configuraciones a nivel de objeto. Se ignoran todas las configuraciones de depósito predeterminadas.
- Si no se especifican configuraciones de retención para el objeto, se aplican las configuraciones de depósito predeterminadas, si existen.
- Si no se especifican configuraciones de retención para el objeto o el depósito, el objeto no estará protegido por el bloqueo de objetos S3.

Si se aplican configuraciones de retención, tanto el objeto como cualquier metadato definido por el usuario de S3 estarán protegidos.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. La cantidad exacta y el tipo de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas compatibles con las políticas ILM activas. Si un objeto protegido se puede eliminar antes de que se alcance su fecha de retención depende de su modo de retención.

   - Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

**Información relacionada**

- "Crear un bucket S3"
- "Actualizar la retención predeterminada de bloqueo de objetos S3"
- "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
- "Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3"

## Habilitar el bloqueo de objetos S3 globalmente

Si una cuenta de inquilino S3 necesita cumplir con requisitos reglamentarios al guardar datos de objetos, debe habilitar S3 Object Lock para todo su sistema StorageGRID . Al habilitar la configuración global de Bloqueo de objetos S3, cualquier usuario inquilino de S3 puede crear y administrar depósitos y objetos con Bloqueo de objetos S3.

**Antes de empezar**

- Tú tienes el"Permiso de acceso root" .
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Ha revisado el flujo de trabajo de bloqueo de objetos S3 y comprende las consideraciones.
- Ha confirmado que la regla predeterminada en la política ILM activa es compatible. Ver"Crear una regla ILM predeterminada" Para más detalles.

**Acerca de esta tarea**

Un administrador de red debe habilitar la configuración global de Bloqueo de objetos S3 para permitir que los usuarios inquilinos creen nuevos depósitos que tengan habilitado el Bloqueo de objetos S3. Una vez habilitada esta configuración, no se podrá deshabilitar.

Revise la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de Bloqueo de objetos S3. Cuando habilita esta configuración, las configuraciones de bloqueo de

objetos S3 por inquilino dependen de la versión de StorageGRID en el momento en que se creó el inquilino.

> La configuración de Cumplimiento global está obsoleta. Si habilitó esta configuración utilizando una versión anterior de StorageGRID, la configuración de Bloqueo de objetos S3 se habilita automáticamente. Puede seguir usando StorageGRID para administrar las configuraciones de los depósitos compatibles existentes; sin embargo, no puede crear depósitos compatibles nuevos. Para más detalles, consulte "Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5" .

**Pasos**

1. Seleccione **CONFIGURACIÓN** > **Sistema** > **Bloqueo de objetos S3**.

   Aparece la página Configuración de bloqueo de objetos S3.

2. Seleccione **Habilitar bloqueo de objetos S3**.
3. Seleccione **Aplicar**.

   Aparece un cuadro de diálogo de confirmación que le recuerda que no puede deshabilitar S3 Object Lock una vez habilitado.

4. Si está seguro de que desea habilitar permanentemente S3 Object Lock para todo el sistema, seleccione **Aceptar**.

   Al seleccionar **Aceptar**:

   - Si la regla predeterminada en la política ILM activa es compatible, el bloqueo de objetos S3 ahora está habilitado para toda la cuadrícula y no se puede deshabilitar.
   - Si la regla predeterminada no se cumple, aparece un error. Debe crear y activar una nueva política ILM que incluya una regla compatible como regla predeterminada. Seleccione **Aceptar**. Luego, crea una nueva política, simulénala y actívala. Ver"Crear una política ILM" para obtener instrucciones.

## Resolver errores de coherencia al actualizar el bloqueo de objetos S3 o la configuración de cumplimiento heredada

Si un sitio de un centro de datos o varios nodos de almacenamiento en un sitio dejan de estar disponibles, es posible que deba ayudar a los usuarios inquilinos de S3 a aplicar cambios en el bloqueo de objetos de S3 o en la configuración de cumplimiento heredada.

Los usuarios inquilinos que tienen depósitos con S3 Object Lock (o cumplimiento heredado) habilitado pueden cambiar ciertas configuraciones. Por ejemplo, un usuario inquilino que utiliza S3 Object Lock podría necesitar colocar una versión de objeto bajo retención legal.

Cuando un usuario inquilino actualiza la configuración de un depósito S3 o una versión de objeto, StorageGRID intenta actualizar inmediatamente los metadatos del depósito o del objeto en toda la red. Si el sistema no puede actualizar los metadatos porque un sitio del centro de datos o varios nodos de almacenamiento 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 resolver este error, siga estos pasos:

1. Intente que todos los nodos o sitios de almacenamiento vuelvan a estar disponibles lo antes posible.
2. Si no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, comuníquese con el soporte técnico, que puede ayudarlo a recuperar nodos y garantizar que los cambios se apliquen de manera uniforme en toda la red.
3. Una vez que se haya resuelto el problema subyacente, recuérdele al usuario inquilino que vuelva a intentar realizar los cambios de configuración.

**Información relacionada**

- "Utilice una cuenta de inquilino"
- "Utilice la API REST de S3"
- "Recuperar y mantener"

# Ejemplo de reglas y políticas de ILM

## Ejemplo 1: Reglas y políticas de ILM para el almacenamiento de objetos

Puede utilizar las siguientes reglas y políticas de ejemplo como punto de partida al definir una política ILM para cumplir con sus requisitos de retención y protección de objetos.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

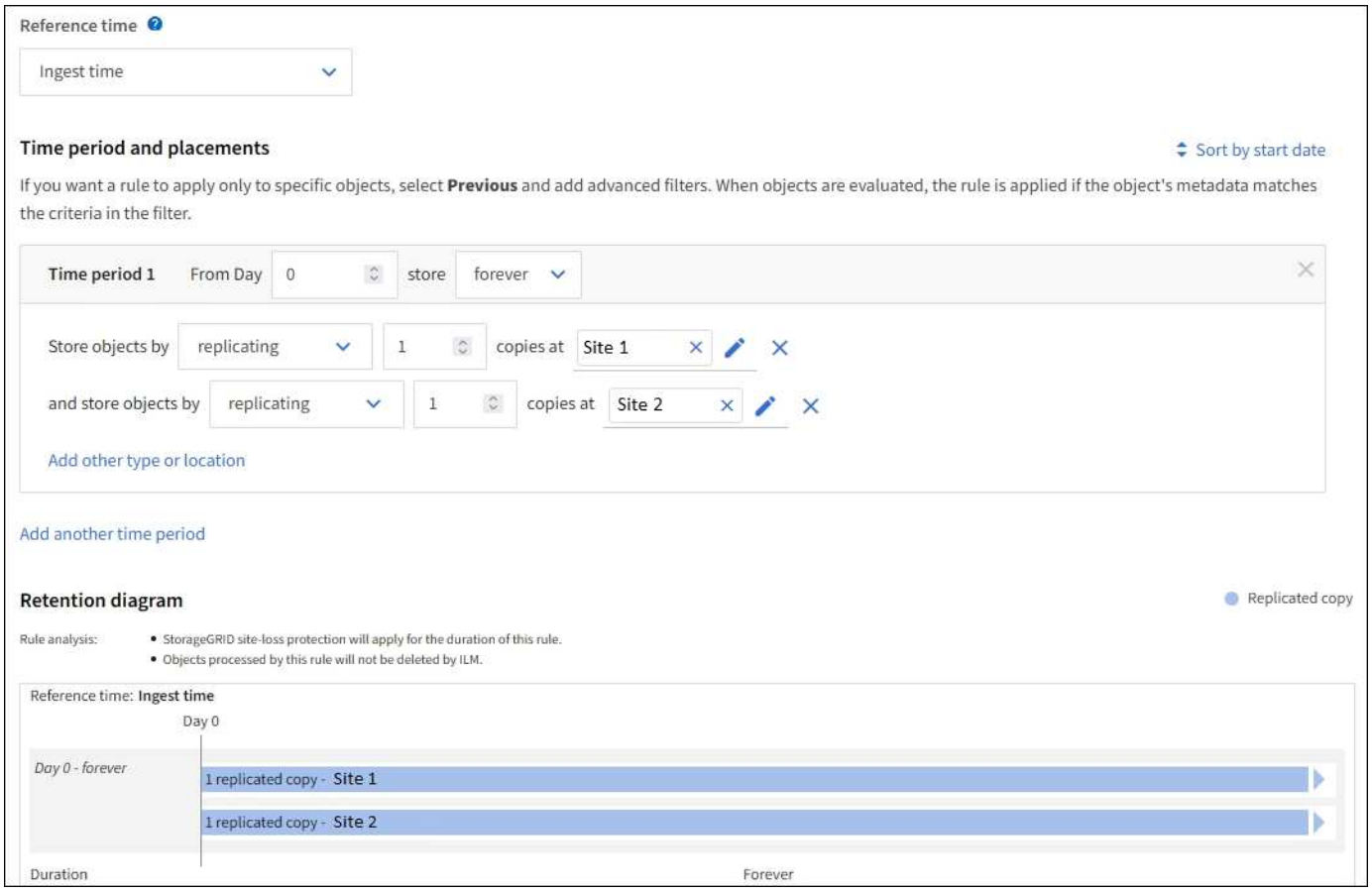
### Regla 1 de ILM para el ejemplo 1: Copiar datos de objetos a dos sitios

Esta regla ILM de ejemplo copia datos de objetos en grupos de almacenamiento en dos sitios.

| Definición de regla | Valor de ejemplo |
|---|---|
| Piscinas de almacenamiento en un solo sitio | Dos grupos de almacenamiento, cada uno con sitios diferentes, denominados Sitio 1 y Sitio 2. |
| Nombre de la regla | Dos copias, dos sitios |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | Desde el día 0 hasta siempre, conserve una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2. |

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

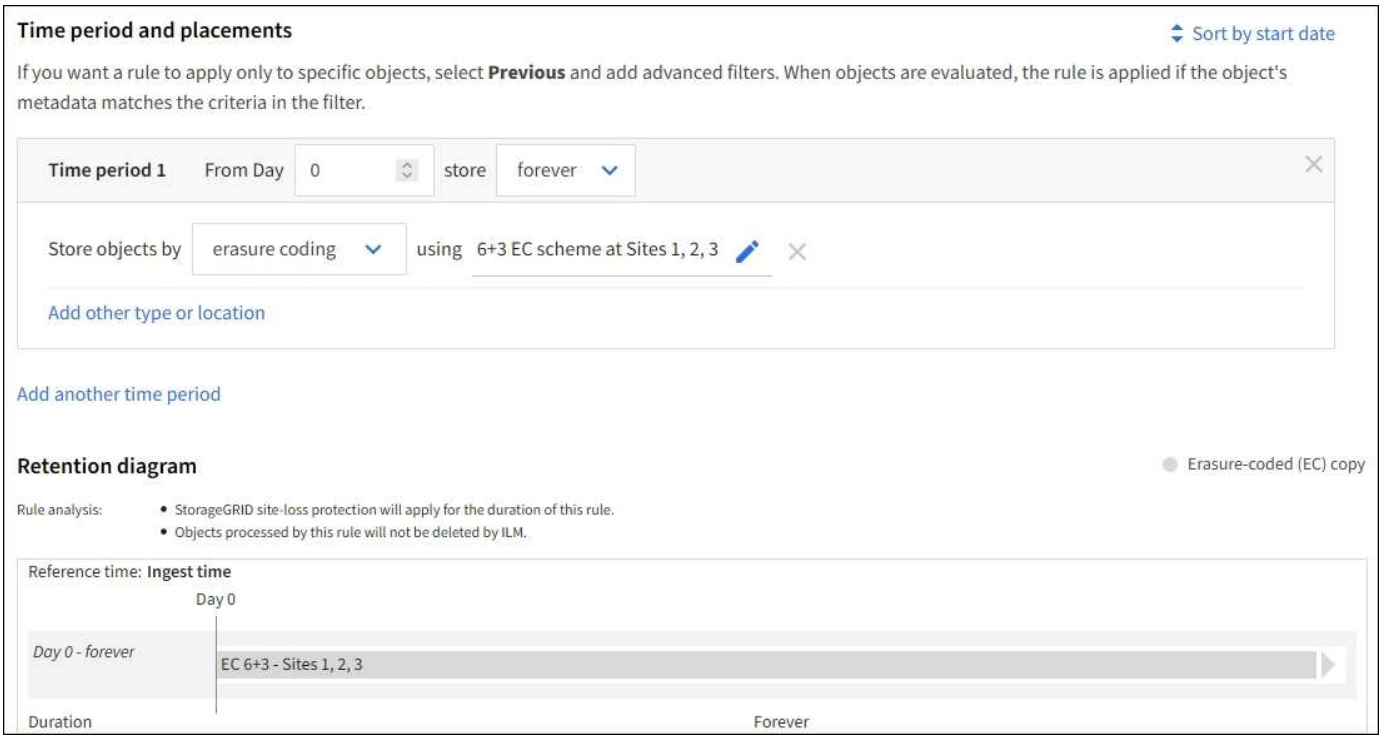
- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- Los objetos procesados por esta regla no serán eliminados por ILM.




### Regla 2 de ILM para el ejemplo 1: Perfil de codificación de borrado con coincidencia de depósito

Esta regla ILM de ejemplo utiliza un perfil de codificación de borrado y un depósito S3 para determinar dónde y durante cuánto tiempo se almacena el objeto.

| Definición de regla | Valor de ejemplo |
|---|---|
| Pool de almacenamiento con múltiples sitios | • Un grupo de almacenamiento en tres sitios (sitios 1, 2 y 3)<br>• Utilice el esquema de codificación de borrado 6+3 |
| Nombre de la regla | Registros financieros del depósito S3 |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | Para los objetos en el bucket S3 llamado finance-records, cree una copia con código de borrado en el grupo especificado por el perfil de codificación de borrado. Conserve esta copia para siempre. |




### Política de ILM, por ejemplo 1

En la práctica, la mayoría de las políticas ILM son simples, aunque el sistema StorageGRID le permite diseñar políticas ILM sofisticadas y complejas.

Una política ILM típica para una red de múltiples sitios podría incluir reglas ILM como las siguientes:

- En la ingesta, almacene todos los objetos que pertenecen al bucket S3 denominado `finance-records` en un grupo de almacenamiento que contiene tres sitios. Utilice la codificación de borrado 6+3.
- Si un objeto no coincide con la primera regla ILM, utilice la regla ILM predeterminada de la política, Dos copias, dos centros de datos, para almacenar una copia de ese objeto en el Sitio 1 y una copia en el Sitio 2.

#### Información relacionada

- "Utilice las políticas de ILM"
- "Crear políticas ILM"

## Ejemplo 2: Reglas y políticas de ILM para el filtrado del tamaño de objetos EC

Puede utilizar las siguientes reglas y políticas de ejemplo como puntos de partida para definir una política ILM que filtre por tamaño de objeto para cumplir con los requisitos de EC recomendados.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

### Regla 1 de ILM para el ejemplo 2: utilizar EC para objetos mayores a 1 MB

Este ejemplo de código de borrado de reglas ILM codifica objetos que tienen más de 1 MB.

> La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

| Definición de regla | Valor de ejemplo |
|---|---|
| Nombre de la regla | Solo objetos EC > 1 MB |
| Tiempo de referencia | Tiempo de ingesta |
| Filtro avanzado para el tamaño del objeto | Tamaño de objeto mayor a 1 MB |
| Colocaciones | Cree una copia con código de borrado 2+1 utilizando tres sitios |


### Regla 2 de ILM para el ejemplo 2: Dos copias replicadas

Esta regla ILM de ejemplo crea dos copias replicadas y no filtra por tamaño de objeto. Esta regla es la regla predeterminada para la política. Dado que la primera regla filtra todos los objetos mayores a 1 MB, esta regla solo se aplica a objetos de 1 MB o menos.

| Definición de regla | Valor de ejemplo |
|---|---|
| Nombre de la regla | Dos copias replicadas |
| Tiempo de referencia | Tiempo de ingesta |
| Filtro avanzado para el tamaño del objeto | Ninguno |
| Colocaciones | Desde el día 0 hasta siempre, conserve una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2. |

### Política de ILM para el ejemplo 2: utilizar EC para objetos mayores a 1 MB

Este ejemplo de política ILM incluye dos reglas ILM:

- La primera regla borra todos los objetos que tengan un tamaño superior a 1 MB.
- La segunda regla ILM (predeterminada) crea dos copias replicadas. Debido a que la regla 1 filtró los objetos de más de 1 MB, la regla 2 solo se aplica a objetos de 1 MB o menos.

## Ejemplo 3: Reglas y políticas de ILM para una mejor protección de los archivos de imagen

Puede utilizar las siguientes reglas y políticas de ejemplo para garantizar que las imágenes de más de 1 MB tengan un código de borrado y que se hagan dos copias de imágenes más pequeñas.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

### Regla 1 de ILM para el ejemplo 3: utilizar EC para archivos de imagen de más de 1 MB

Esta regla ILM de ejemplo utiliza filtrado avanzado para borrar el código de todos los archivos de imagen de más de 1 MB.

> La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

| Definición de regla | Valor de ejemplo |
|---|---|
| Nombre de la regla | Archivos de imagen EC > 1 MB |
| Tiempo de referencia | Tiempo de ingesta |
| Filtro avanzado para el tamaño del objeto | Tamaño de objeto mayor a 1 MB |
| Filtros avanzados para clave | • Termina en .jpg<br>• Termina en .png |
| Colocaciones | Cree una copia con código de borrado 2+1 utilizando tres sitios |

Debido a que esta regla está configurada como la primera regla en la política, la instrucción de ubicación de codificación de borrado solo se aplica a archivos .jpg y .png que tengan más de 1 MB.

#### Regla 2 de ILM para el ejemplo 3: Crear 2 copias replicadas para todos los archivos de imagen restantes

Esta regla ILM de ejemplo utiliza filtrado avanzado para especificar que se repliquen archivos de imagen más pequeños. Dado que la primera regla de la política ya ha coincidido con archivos de imagen de más de 1 MB, esta regla se aplica a archivos de imagen de 1 MB o menos.

| Definición de regla | Valor de ejemplo |
|---|---|
| Nombre de la regla | 2 copias para archivos de imagen |
| Tiempo de referencia | Tiempo de ingesta |
| Filtros avanzados para clave | • Termina en .jpg<br>• Termina en .png |
| Colocaciones | Cree 2 copias replicadas en dos grupos de almacenamiento |

#### Política de ILM, por ejemplo 3: Mejor protección para los archivos de imagen

Este ejemplo de política ILM incluye tres reglas:

- La primera regla borra todos los archivos de imagen mayores a 1 MB.
- La segunda regla crea dos copias de cualquier archivo de imagen restante (es decir, imágenes de 1 MB o menos).
- La regla predeterminada se aplica a todos los objetos restantes (es decir, cualquier archivo que no sea imagen).

## Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3

Si tiene un bucket S3 con control de versiones habilitado, puede administrar las versiones de objetos no actuales incluyendo reglas en su política ILM que utilicen "Hora no actual" como hora de referencia.

> Si especifica un tiempo de retención limitado para los objetos, dichos objetos se eliminarán de forma permanente una vez alcanzado el período de tiempo. Asegúrese de comprender cuánto tiempo se conservarán los objetos.

Como muestra este ejemplo, puede controlar la cantidad de almacenamiento utilizada por objetos versionados mediante el uso de diferentes instrucciones de ubicación para versiones de objetos no actuales.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Para realizar una simulación de política ILM en una versión no actual de un objeto, debe conocer el UUID o CBID de la versión del objeto. Para encontrar el UUID y el CBID, utilice"búsqueda de metadatos de objetos" mientras el objeto todavía esté actual.

**Información relacionada**

"Cómo se eliminan los objetos"

### Regla 1 de ILM, por ejemplo 4: Guardar tres copias durante 10 años

Esta regla ILM de ejemplo almacena una copia de cada objeto en tres sitios durante 10 años.

Esta regla se aplica a todos los objetos, independientemente de si tienen versiones o no.

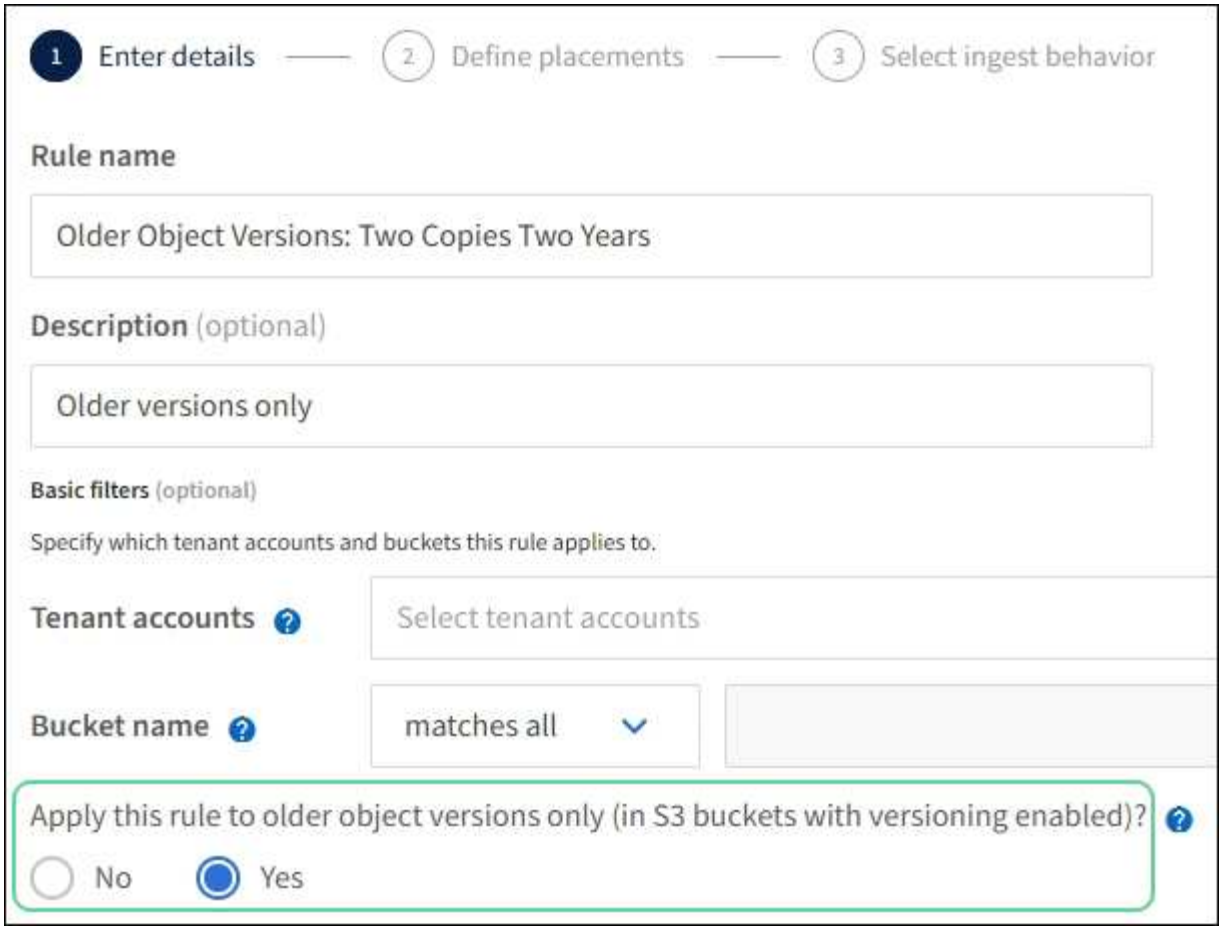
| Definición de regla | Valor de ejemplo |
|---|---|
| Pools de almacenamiento | Tres grupos de almacenamiento, cada uno de ellos compuesto por diferentes centros de datos, denominados Sitio 1, Sitio 2 y Sitio 3. |
| Nombre de la regla | Tres copias, diez años |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | El día 0, conserve tres copias replicadas durante 10 años (3652 días), una en el Sitio 1, una en el Sitio 2 y una en el Sitio 3. Al cabo de 10 años, elimine todas las copias del objeto. |

### Regla 2 de ILM, por ejemplo 4: Guardar dos copias de versiones no actuales durante 2 años

Esta regla ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto versionado S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debe crear otra regla para filtrar las versiones no actuales.

Para crear una regla que use "Hora no actual" como hora de referencia, seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?" en el Paso 1 (Ingresar detalles) del asistente Crear una regla de ILM. Cuando selecciona **Sí**, se selecciona automáticamente *Hora no actual* como hora de referencia y no puede seleccionar una hora de referencia diferente.




En este ejemplo, solo se almacenan dos copias de las versiones no actuales, y esas copias se almacenarán durante dos años.

| Definición de regla | Valor de ejemplo |
|---|---|
| Pools de almacenamiento | Dos grupos de almacenamiento, cada uno en diferentes centros de datos, Sitio 1 y Sitio 2. |
| Nombre de la regla | Versiones no actuales: dos copias dos años |
| Tiempo de referencia | Tiempo no actual<br><br>Se selecciona automáticamente cuando selecciona **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?" en el asistente Crear una regla de ILM. |
| Colocaciones | El día 0 en relación con el tiempo no actual (es decir, a partir del día en que la versión del objeto se convierte en la versión no actual), mantenga dos copias replicadas de las versiones no actuales del objeto durante 2 años (730 días), una en el Sitio 1 y otra en el Sitio 2. Al cabo de 2 años, elimine las versiones no actuales. |

### Política de ILM para el ejemplo 4: objetos versionados S3

Si desea administrar versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilizan "Hora no actual" como hora de referencia deben aparecer en la política ILM antes que las reglas que se aplican a la versión actual del objeto.

Una política ILM para objetos versionados S3 podría incluir reglas ILM como las siguientes:

- Conserve cualquier versión anterior (no actual) de cada objeto durante 2 años, a partir del día en que la versión dejó de estar actual.

> Las reglas de "Hora no actual" deben aparecer en la política antes de las reglas que se aplican a la versión actual del objeto. De lo contrario, las versiones de objetos no actuales nunca coincidirán con la regla "Tiempo no actual".

- Al momento de la ingesta, cree tres copias replicadas y almacene una copia en cada uno de los tres sitios. Conserve copias de la versión actual del objeto durante 10 años.

Al simular la política de ejemplo, esperaría que los objetos de prueba se evaluaran de la siguiente manera:

- Cualquier versión de objeto no actual se corresponderá con la primera regla. Si una versión no actual de un objeto tiene más de 2 años, ILM la elimina de forma permanente (todas las copias de la versión no actual se eliminan de la red).
- La versión actual del objeto coincidiría con la segunda regla. Cuando la versión actual del objeto se ha almacenado durante 10 años, el proceso ILM agrega un marcador de eliminación como la versión actual del objeto y hace que la versión anterior del objeto sea "no actual". La próxima vez que se realiza una evaluación ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en el Sitio 3 se elimina y las dos copias en el Sitio 1 y el Sitio 2 se almacenan durante 2 años más.

## Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto

Puede utilizar un filtro de ubicación y el comportamiento de ingesta estricta en una regla para evitar que los objetos se guarden en una ubicación de centro de datos en particular.

En este ejemplo, un inquilino con sede en París no quiere almacenar algunos objetos fuera de la UE debido a cuestiones regulatorias. Otros objetos, incluidos todos los objetos de otras cuentas de inquilinos, se pueden almacenar en el centro de datos de París o en el centro de datos de EE. UU.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

**Información relacionada**

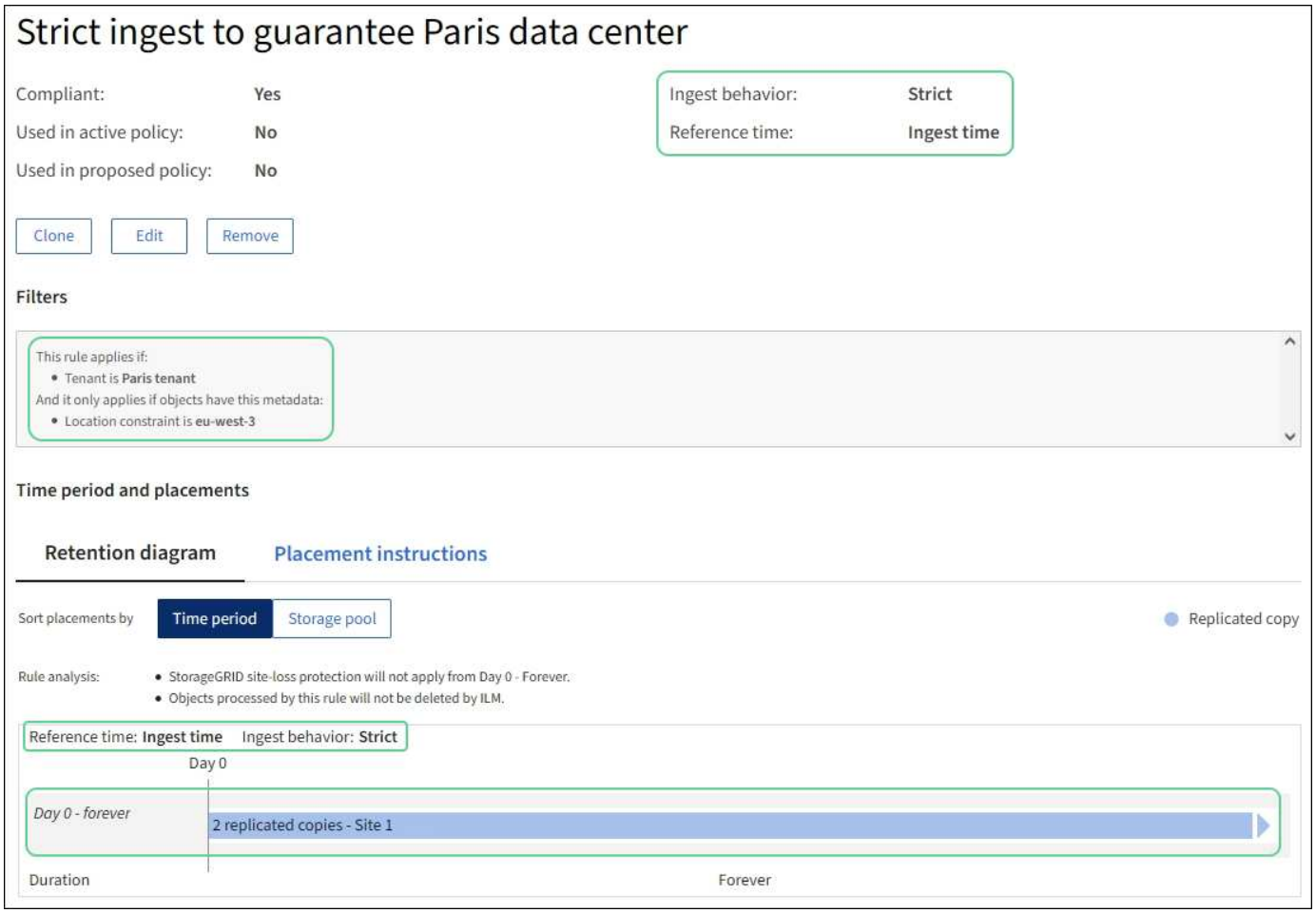
- "Opciones de ingesta"
- "Crear regla de ILM: Seleccionar comportamiento de ingesta"

### Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

Esta regla ILM de ejemplo utiliza el comportamiento de ingesta estricta para garantizar que los objetos guardados por un inquilino con sede en París en depósitos S3 con la región configurada en 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 de París y que tienen la región de depósito S3 establecida en eu-west-3 (París).

| Definición de regla | Valor de ejemplo |
|---|---|
| Cuenta de inquilino | inquilino de París |
| Filtro avanzado | La restricción de ubicación es igual a eu-west-3 |
| Pools de almacenamiento | Sitio 1 (París) |
| Nombre de la regla | Ingesta estricta para garantizar el centro de datos de París |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | El día 0, conserve dos copias replicadas para siempre en el Sitio 1 (París) |
| Comportamiento de ingesta | Estricto. Utilice siempre las ubicaciones de esta regla al ingerir. La ingesta falla si no es posible almacenar dos copias del objeto en el centro de datos de París. |



### Regla 2 de ILM, por ejemplo 5: Ingesta equilibrada para otros objetos

Esta regla ILM de ejemplo utiliza el comportamiento de ingesta equilibrada para proporcionar una eficiencia ILM óptima para cualquier objeto que no coincida con la primera regla. Se almacenarán dos copias de todos los objetos que coincidan con esta regla: una en el centro de datos de EE. UU. y otra en el centro de datos de París. Si la regla no puede cumplirse inmediatamente, 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* |
| Pools de almacenamiento | Sitio 1 (París) y Sitio 2 (EE. UU.) |
| Nombre de la regla | 2 copias 2 centros de datos |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | El día 0, mantenga dos copias replicadas para siempre en dos centros de datos |
| Comportamiento de ingesta | Equilibrado. Los objetos que coinciden con esta regla se colocan de acuerdo con las instrucciones de ubicación de la regla, si es posible. De lo contrario, se realizan copias provisionales en cualquier lugar disponible. |

### Política ILM para el ejemplo 5: Combinación de comportamientos de ingesta

La política ILM de ejemplo incluye dos reglas que tienen diferentes comportamientos de ingesta.

Una política ILM que utiliza dos comportamientos de ingesta diferentes podría incluir reglas ILM como las siguientes:

- Almacene los objetos que pertenecen al inquilino de París y que tienen la región de depósito S3 configurada en eu-west-3 (París) solo en el centro de datos de París. Error en la ingesta si el centro de datos de París no está disponible.
- Almacene todos los demás objetos (incluidos aquellos que pertenecen al inquilino de París pero que tienen una región de depósito diferente) tanto en el centro de datos de EE. UU. como en el centro de datos de París. Haga copias provisionales en cualquier ubicación disponible si no se puede cumplir con las instrucciones de ubicación.

Al simular la política de ejemplo, espera que los objetos de prueba se evalúen de la siguiente manera:

- Todos los objetos que pertenecen al inquilino de París y que tienen la región de bucket S3 establecida en eu-west-3 coinciden con la primera regla y se almacenan en el centro de datos de París. Debido a que la primera regla utiliza ingesta estricta, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los nodos de almacenamiento en el centro de datos de París no están disponibles, la ingesta falla.

- Todos los demás objetos coinciden con la segunda regla, incluidos los objetos que pertenecen al inquilino de París y que no tienen la región de depósito S3 establecida en eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, debido a que la segunda regla utiliza ingesta equilibrada, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

## Ejemplo 6: Cambiar una política de ILM

Si necesita cambiar su protección de datos o agrega nuevos sitios, puede crear y activar una nueva política ILM.

Antes de cambiar una política, debe comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente el rendimiento general de un sistema StorageGRID .

En este ejemplo, se ha agregado un nuevo sitio StorageGRID en una expansión y se debe 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. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

**Cómo afecta el cambio de una política de ILM al rendimiento**

Cuando activa una nueva política ILM, el rendimiento de su sistema StorageGRID podría verse afectado temporalmente, especialmente si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se muevan a nuevas ubicaciones.

Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Para garantizar que una nueva política de ILM no afecte la ubicación de los objetos replicados y codificados por borrado existentes, puede"crear una regla ILM con un filtro de tiempo de ingesta" . Por ejemplo, **La hora de ingesta *es el o después de <fecha y hora>***, de modo que la nueva regla se aplica solo a los objetos ingeridos en o después de la fecha y hora especificadas.

Los tipos de cambios de política de ILM que pueden afectar temporalmente el rendimiento de StorageGRID incluyen los siguientes:

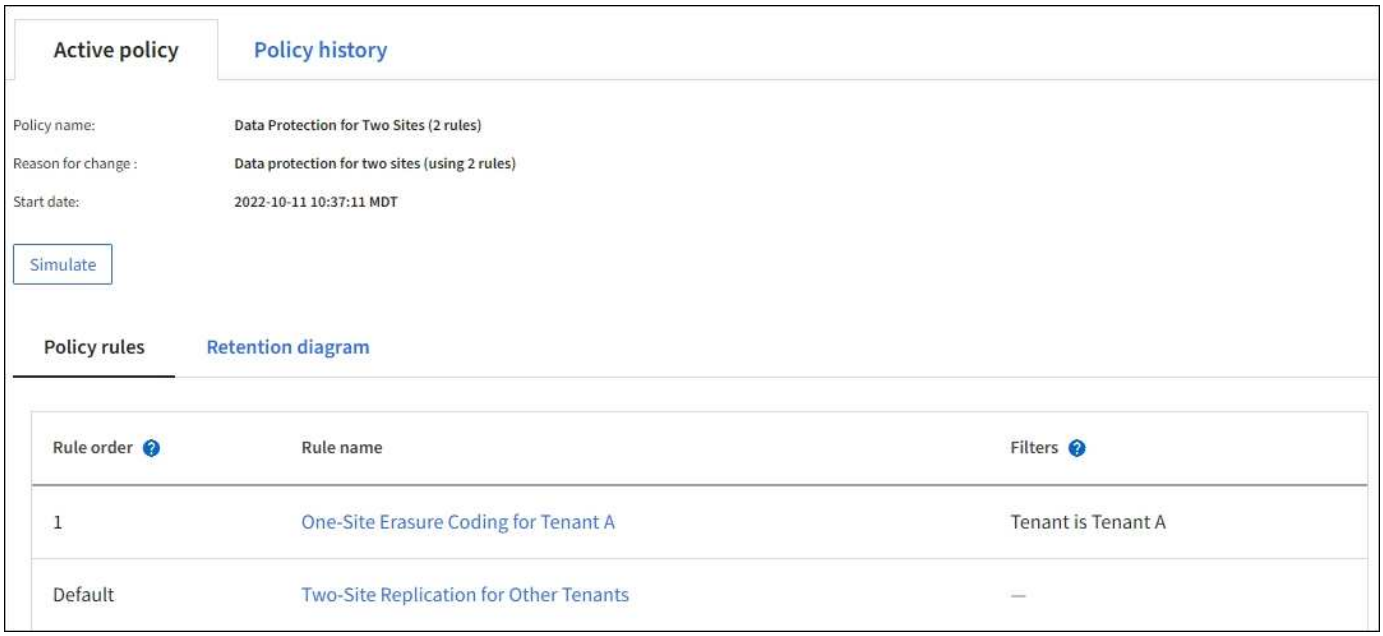
- Aplicar un perfil de codificación de borrado diferente a objetos con codificación de borrado existentes.

  > StorageGRID considera que cada perfil de codificación de borrado es único y no reutiliza fragmentos de codificación de borrado cuando se utiliza un nuevo perfil.

- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos con código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover una gran cantidad de objetos hacia o desde un grupo de almacenamiento en la nube o hacia o desde un sitio remoto.

### Política ILM activa, por ejemplo 6: Protección de datos en dos sitios

En este ejemplo, la política ILM activa se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas ILM.




En esta política ILM, los objetos que pertenecen al inquilino A están protegidos mediante codificación de borrado 2+1 en un solo sitio, mientras que los objetos que pertenecen a todos los demás inquilinos están protegidos en dos sitios mediante replicación de 2 copias.

#### Regla 1: Codificación de borrado de un sitio para el inquilino A

| Definición de regla | Valor de ejemplo |
|---|---|
| Nombre de la regla | Codificación de borrado de un sitio para el inquilino A |
| Cuenta de inquilino | Inquilino A |
| Pool de almacenamiento | Sitio 1 |
| Colocaciones | Codificación de borrado 2+1 en el Sitio 1 desde el día 0 hasta la eternidad |

#### Regla 2: Replicación en dos sitios para otros inquilinos

| Definición de regla | Valor de ejemplo |
|---|---|
| Nombre de la regla | Replicación de dos sitios para otros inquilinos |
| Cuenta de inquilino | Ignorar |
| Pools de almacenamiento | Sitio 1 y Sitio 2 |

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Colocaciones | Dos copias replicadas desde el día 0 hasta siempre: una copia en el Sitio 1 y una copia en el Sitio 2. |

### Política de ILM, ejemplo 6: Protección de datos en tres sitios

En este ejemplo, la política ILM se reemplaza por una nueva política para un sistema StorageGRID de tres sitios.

Después de realizar una expansión para agregar 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 contiene los tres sitios (no el mismo que el grupo de almacenamiento predeterminado Todos los nodos de almacenamiento). Luego, el administrador creó dos nuevas reglas ILM y una nueva política ILM, diseñada para proteger los datos en los tres sitios.

Cuando se activa esta nueva política ILM, los objetos que pertenecen al Inquilino A estarán protegidos mediante codificación de borrado 2+1 en tres sitios, mientras que los objetos que pertenecen a otros inquilinos (y objetos más pequeños que pertenecen al Inquilino A) estarán protegidos en tres sitios mediante replicación de 3 copias.

#### Regla 1: Codificación de borrado de tres sitios para el inquilino A

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Nombre de la regla | Codificación de borrado de tres sitios para el inquilino A |
| Cuenta de inquilino | Inquilino A |
| Pool de almacenamiento | Los 3 sitios (incluye el Sitio 1, el Sitio 2 y el Sitio 3) |
| Colocaciones | Codificación de borrado 2+1 en los 3 sitios desde el día 0 hasta siempre |

#### Regla 2: Replicación en tres sitios para otros inquilinos

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Nombre de la regla | Réplica de tres sitios para otros inquilinos |
| Cuenta de inquilino | Ignorar |
| Pools de almacenamiento | Sitio 1, Sitio 2 y Sitio 3 |
| Colocaciones | Tres copias replicadas desde el día 0 hasta siempre: una copia en el Sitio 1, una copia en el Sitio 2 y una copia en el Sitio 3. |

### Activación de la política ILM por ejemplo 6

Cuando se activa una nueva política ILM, es posible que los objetos existentes se muevan a nuevas

ubicaciones o que se creen nuevas copias de objetos existentes, según las instrucciones de ubicación de cualquier regla nueva o actualizada.

> Los errores en una política ILM pueden provocar una pérdida de datos irrecuperable. Revise cuidadosamente y simule la política antes de activarla para confirmar que funcionará según lo previsto.

> Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

#### ¿Qué sucede cuando cambian las instrucciones de codificación de borrado?

En la política ILM actualmente activa para este ejemplo, los objetos que pertenecen al inquilino A están protegidos mediante codificación de borrado 2+1 en el sitio 1. En la nueva política ILM, los objetos que pertenecen al inquilino A estarán protegidos mediante codificación de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política ILM, se producen las siguientes operaciones ILM:

- Los nuevos objetos ingeridos por el inquilino A se dividen en dos fragmentos de datos y se agrega un fragmento de paridad. Luego, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen al inquilino A se vuelven a evaluar durante el proceso de escaneo ILM en curso. Debido a que las instrucciones de colocación de ILM utilizan un nuevo perfil de codificación de borrado, se crean fragmentos codificados de borrado completamente nuevos y se distribuyen a los tres sitios.

> Los fragmentos 2+1 existentes en el Sitio 1 no se reutilizan. StorageGRID considera que cada perfil de codificación de borrado es único y no reutiliza fragmentos de codificación de borrado cuando se utiliza un nuevo perfil.

#### ¿Qué sucede cuando cambian las instrucciones de replicación?

En la política ILM actualmente activa para este ejemplo, los objetos que pertenecen a otros inquilinos están protegidos mediante dos copias replicadas en grupos de almacenamiento en los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenecen a otros inquilinos estarán protegidos mediante tres copias replicadas en grupos de almacenamiento en los sitios 1, 2 y 3.

Cuando se activa la nueva política ILM, se producen las siguientes operaciones ILM:

- Cuando cualquier inquilino que no sea el inquilino A ingiere un nuevo objeto, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se vuelven a evaluar durante el proceso de escaneo ILM en curso. Dado que las copias de objetos existentes en el Sitio 1 y el Sitio 2 continúan satisfaciendo los requisitos de replicación de la nueva regla ILM, StorageGRID solo necesita crear una nueva copia del objeto para el Sitio 3.

#### Impacto en el rendimiento de la activación de esta política

Cuando se activa la política ILM en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se requerirán niveles de recursos de red superiores a los normales para crear

nuevos fragmentos con código de borrado para los objetos existentes del Inquilino A y nuevas copias replicadas en el Sitio 3 para los objetos existentes de otros inquilinos.

Como resultado del cambio de política de ILM, las solicitudes de lectura y escritura del cliente podrían experimentar temporalmente latencias más altas de lo normal. Las latencias volverán a los niveles normales después de que las instrucciones de ubicación se implementen completamente en toda la red.

Para evitar problemas de recursos al activar una nueva política ILM, puede usar el filtro avanzado Tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta para que sea mayor o igual al tiempo aproximado en que entrará en vigencia la nueva política para garantizar que los objetos existentes no se muevan innecesariamente.

Comuníquese con el soporte técnico si necesita reducir o aumentar la velocidad a la que se procesan los objetos después de un cambio de política de ILM.

## Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3

Puede usar el depósito S3, las reglas ILM y la política ILM en este ejemplo como punto de partida al definir una política ILM para cumplir con los requisitos de protección y retención de objetos para objetos en depósitos con el bloqueo de objetos S3 habilitado.

Si utilizó la función de Cumplimiento heredada en versiones anteriores de StorageGRID , también puede usar este ejemplo para ayudar a administrar cualquier depósito existente que tenga habilitada la función de Cumplimiento heredada.

Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simulérela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

**Información relacionada**

- "Administrar objetos con S3 Object Lock"
- "Crear una política ILM"

### Ejemplo de bloqueo de objetos y cubos para S3

En este ejemplo, una cuenta de inquilino S3 llamada Bank of ABC utilizó el Administrador de inquilinos para crear un depósito con el Bloqueo de objetos S3 habilitado para almacenar registros bancarios críticos.

| Definición de cubo | Valor de ejemplo |
|---|---|
| Nombre de la cuenta del inquilino | Banco de ABC |
| Nombre del depósito | registros bancarios |
| Región del cubo | us-east-1 (predeterminado) |

Cada objeto y versión de objeto que se agrega al depósito de registros bancarios utilizará los siguientes valores para `retain-until-date` y `legal hold` ajustes.

| Configuración para cada objeto | Valor de ejemplo |
| --- | --- |
| `retain-until-date` | "2030-12-30T23:59:59Z" (30 de diciembre de 2030)<br><br>Cada versión del objeto tiene su propia `retain-until-date` configuración. Este ajuste se puede aumentar, pero no disminuir. |
| `legal hold` | "OFF" (Sin efecto)<br><br>Se puede colocar o levantar una retención legal sobre cualquier versión de un objeto en cualquier momento durante el período de retención. Si un objeto se encuentra bajo una retención legal, el objeto no se puede eliminar incluso si `retain-until-date` Se ha alcanzado. |

**Ejemplo de regla 1 de ILM para bloqueo de objetos S3: Perfil de codificación de borrado con coincidencia de depósito**

Esta regla ILM de ejemplo se aplica únicamente a la cuenta de inquilino S3 denominada Banco ABC. Coincide con cualquier objeto del `bank-records` y luego utiliza codificación de borrado para almacenar el objeto en nodos de almacenamiento en tres sitios de centros de datos utilizando un perfil de codificación de borrado 6+3. Esta regla satisface los requisitos de los depósitos con el bloqueo de objetos S3 habilitado: se conserva una copia en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando el tiempo de ingesta como tiempo de referencia.

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Nombre de la regla | Norma de cumplimiento: Objetos CE en el contenedor de registros bancarios - Banco ABC |
| Cuenta de inquilino | Banco de ABC |
| Nombre del depósito | `bank-records` |
| Filtro avanzado | Tamaño del objeto (MB) mayor a 1<br><br>**Nota:** Este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menos. |

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | Desde el día 0 tienda para siempre |
| Perfil de codificación de borrado | • Cree una copia con código de borrado en los nodos de almacenamiento en tres sitios de centros de datos<br>• Utiliza el esquema de codificación de borrado 6+3 |

### Regla 2 de ILM para el ejemplo de bloqueo de objetos S3: regla no conforme

Esta regla ILM de ejemplo almacena inicialmente dos copias de objetos replicados en los nodos de almacenamiento. Después de un año, almacena una copia en un grupo de almacenamiento en la nube para siempre. Debido a que esta regla utiliza un grupo de almacenamiento en la nube, no es compatible y no se aplicará a los objetos en depósitos con el bloqueo de objetos S3 habilitado.

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Nombre de la regla | Regla no conforme: utilizar el grupo de almacenamiento en la nube |
| Cuentas de inquilinos | No especificado |
| Nombre del depósito | No se especifica, pero solo se aplicará a los depósitos que no tengan habilitado el bloqueo de objetos S3 (o la función de cumplimiento heredada). |
| Filtro avanzado | No especificado |

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | • El día 0, mantenga dos copias replicadas en los nodos de almacenamiento del centro de datos 1 y del centro de datos 2 durante 365 días<br>• Después de 1 año, conserve una copia replicada en un grupo de almacenamiento en la nube para siempre |

### Regla 3 de ILM para el ejemplo de bloqueo de objetos S3: regla predeterminada

Esta regla ILM de ejemplo copia datos de objetos en grupos de almacenamiento en dos centros de datos. Esta regla de cumplimiento está diseñada para ser la regla predeterminada en la política ILM. No incluye ningún filtro, no utiliza el tiempo de referencia no actual y satisface los requisitos de los buckets con S3 Object Lock habilitado: se mantienen dos copias de objetos en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando la ingesta como tiempo de referencia.

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Nombre de la regla | Regla de cumplimiento predeterminada: Dos copias, dos centros de datos |
| Cuenta de inquilino | No especificado |
| Nombre del depósito | No especificado |
| Filtro avanzado | No especificado |

| Definición de regla | Valor de ejemplo |
| --- | --- |
| Tiempo de referencia | Tiempo de ingesta |
| Colocaciones | Desde el día 0 y para siempre, conserve dos copias replicadas: una en los nodos de almacenamiento del centro de datos 1 y otra en los nodos de almacenamiento del centro de datos 2. |

### Ejemplo de política ILM compatible con bloqueo de objetos S3

Para crear una política ILM que proteja eficazmente todos los objetos de su sistema, incluidos aquellos en depósitos con el bloqueo de objetos S3 habilitado, debe seleccionar reglas ILM que satisfagan los requisitos de almacenamiento de todos los objetos. Luego debes simular y activar la política.

#### Agregar reglas a la política

En este ejemplo, la política ILM incluye tres reglas ILM, en el siguiente orden:

1. Una regla compatible que utiliza codificación de borrado para proteger objetos de más de 1 MB en un depósito específico con S3 Object Lock habilitado. Los objetos se almacenan en nodos de almacenamiento desde el día 0 hasta siempre.
2. Una regla no conforme que crea dos copias de objetos replicados en nodos de almacenamiento durante un año y luego mueve una copia de objeto a un grupo de almacenamiento en la nube para siempre. Esta regla no se aplica a los depósitos con el bloqueo de objetos S3 habilitado porque utiliza un grupo de almacenamiento en la nube.
3. La regla compatible predeterminada que crea dos copias de objetos replicados en los nodos de almacenamiento desde el día 0 hasta siempre.

#### Simular la política

Después de haber agregado reglas a su política, elegido una regla compatible predeterminada y organizado las otras reglas, debe simular la política probando objetos del depósito con S3 Object Lock habilitado y de otros depósitos. Por ejemplo, al simular la política de ejemplo, esperaría que los objetos de prueba se evaluaran de la siguiente manera:

- La primera regla solo coincidirá con objetos de prueba que tengan más de 1 MB en el depósito de registros bancarios para el inquilino del Banco de ABC.
- La segunda regla hará coincidir todos los objetos en todos los depósitos no compatibles para todas las demás cuentas de inquilino.
- La regla predeterminada coincidirá con estos objetos:
  - Objetos de 1 MB o menos en el depósito de registros bancarios para el inquilino del Banco ABC.
  - Objetos en cualquier otro depósito que tenga habilitado el bloqueo de objetos S3 para todas las demás cuentas de inquilino.

#### Activar la política

Cuando esté completamente satisfecho de que la nueva política protege los datos del objeto como se esperaba, puede activarla.

## Ejemplo 8: Prioridades para el ciclo de vida del depósito S3 y la política de ILM

Según la configuración de su ciclo de vida, los objetos siguen las configuraciones de retención del ciclo de vida del bucket S3 o de una política ILM.

#### Ejemplo de cómo el ciclo de vida del bucket tiene prioridad sobre la política de ILM

**Política de ILM**

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias durante 50 días

**Ciclo de vida del bucket**

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

**Resultado**

- Se ingiere un objeto llamado "docs/text". Coincide con el filtro del ciclo de vida del depósito del prefijo "docs/".
  - Después de 100 días, se crea un marcador de eliminación y "docs/text" deja de estar actualizado.
  - Después de 5 días, un total de 105 días desde la ingesta, se elimina "docs/text".
  - Después de 95 días, un total de 200 días desde la ingesta y 100 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.
- Se ingiere un objeto llamado "video/película". No coincide con el filtro y utiliza la política de retención ILM.
  - Después de 50 días, se crea un marcador de eliminación y el archivo "video/película" deja de estar vigente.
  - Después de 20 días, un total de 70 días desde la ingesta, se elimina "video/película".
  - Después de 30 días, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.

#### Ejemplo de ciclo de vida de un bucket que implícitamente se mantiene para siempre

**Política de ILM**

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias durante 50 días

**Ciclo de vida del bucket**

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

**Resultado**

- Se ingiere un objeto llamado "docs/text". Coincide con el filtro del ciclo de vida del depósito del prefijo "docs/".

  El `Expiration` La acción se aplica solo a los marcadores de eliminación vencidos, lo que implica mantener todo lo demás para siempre (comenzando con "docs/").

Los marcadores de eliminación que comienzan con "docs/" se eliminan cuando caducan.

- Se ingiere un objeto llamado "video/película". No coincide con el filtro y utiliza la política de retención ILM.
  - Después de 50 días, se crea un marcador de eliminación y el archivo "video/película" deja de estar vigente.
  - Después de 20 días, un total de 70 días desde la ingesta, se elimina "video/película".
  - Después de 30 días, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.

**Ejemplo de uso del ciclo de vida del bucket para duplicar ILM y limpiar marcadores de eliminación vencidos**

**Política de ILM**

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias para siempre

**Ciclo de vida del bucket**

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

**Resultado**

- La política ILM se duplica en el ciclo de vida del depósito.
  - La regla permanente de la política ILM está diseñada para eliminar objetos manualmente y limpiar versiones no actuales después de 20 días. En consecuencia, la regla de tiempo de ingesta mantendrá los marcadores de eliminación vencidos para siempre.
  - El ciclo de vida del depósito duplica el comportamiento de la política ILM al agregar `"ExpiredObjectDeleteMarker": true` , que elimina los marcadores de eliminación una vez que han expirado
- Se ingiere un objeto. Sin filtro significa que el ciclo de vida del depósito se aplica a todos los objetos y anula las configuraciones de retención de ILM.
  - Cuando un inquilino emite una solicitud de eliminación de un objeto, se crea un marcador de eliminación y el objeto deja de ser 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.