Gestión de objetos con ILM

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

Gestión de objetos con ILM . . . 1
Gestión de objetos con ILM: Información general . . . 1
ILM y ciclo de vida de los objetos . . . 2
Qué es una política de ILM . . . 23
Qué es una regla de ILM . . . 26
Crear grados de almacenamiento, pools de almacenamiento, perfiles de EC y regiones . . . 30
Cree la regla de ILM . . . 85
Cree una política de ILM . . . 103
Trabaje con las reglas de ILM y las políticas de ILM . . . 128
Utilice la bloqueo de objetos de S3 con ILM . . . 132
Ejemplo de reglas y políticas de ILM . . . 145

Gestión de objetos con ILM

Gestión de objetos con ILM: Información general

Para administrar los objetos de un sistema StorageGRID, configure las reglas y políticas de gestión de ciclo de vida de la información (ILM). Las reglas y políticas de ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo gestionarlos a lo largo del tiempo.

Acerca de estas instrucciones

El diseño e implementación de reglas de ILM y la política de ILM requiere una planificación cuidadosa. Debe comprender los requisitos operativos, la topología del sistema StorageGRID, las necesidades de protección de objetos y los tipos de almacenamiento disponibles. A continuación, debe determinar cómo desea copiar, distribuir y almacenar diferentes tipos de objetos.

Utilice estas instrucciones para:

- Obtenga más información sobre ILM de StorageGRID, incluida la manera en que ILM funciona durante la vida de un objeto, así como sobre qué reglas y políticas de ILM son.
- Aprenda a configurar pools de almacenamiento, perfiles de código de borrado y reglas de ILM.
- Aprenda a crear y activar una política de ILM que protegerá los datos de objetos en uno o más sitios.
- Aprenda a gestionar objetos con el bloqueo de objetos de S3, que ayuda a garantizar que los objetos de bloques de S3 no se eliminen ni se sobrescriban por un periodo de tiempo específico.

Leer más

Para obtener más información, consulte estos vídeos:

- "Vídeo: Reglas de ILM para StorageGRID: Introducción"

- "Vídeo: Políticas de ILM de StorageGRID"

ILM y ciclo de vida de los objetos

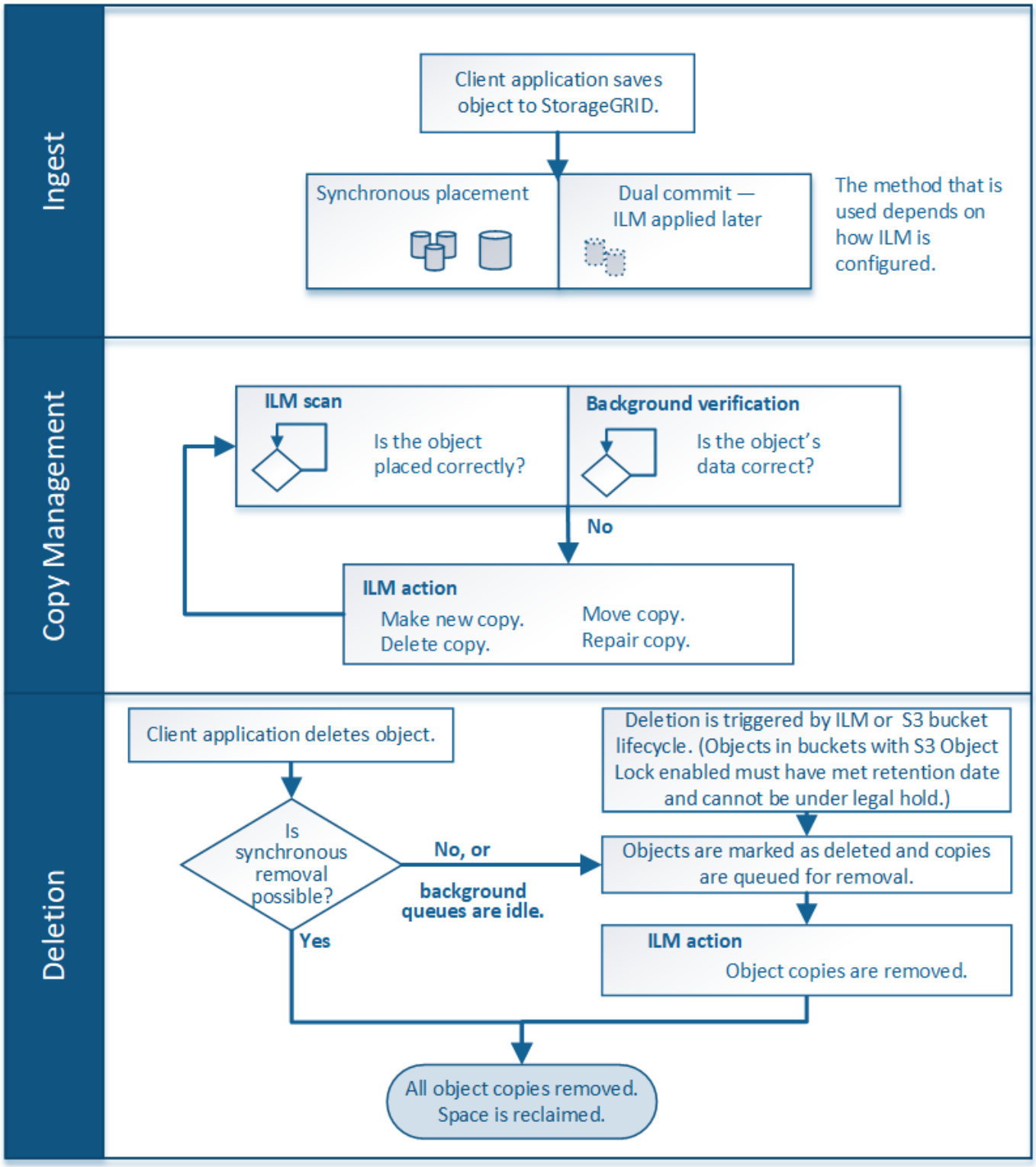
Cómo funciona ILM a lo largo de la vida de un objeto

Comprender cómo utiliza StorageGRID ILM para gestionar objetos durante cada fase de su vida útil puede ayudarle a diseñar una política más eficaz.

- **Ingesta**: La ingesta comienza cuando una aplicación cliente S3 o Swift establece una conexión para guardar un objeto en el sistema StorageGRID, y se completa cuando StorageGRID devuelve un mensaje "'ingesta correcta'" al cliente. Los datos de objetos se protegen durante la ingesta aplicando instrucciones de ILM inmediatamente (ubicación síncrona) o creando copias provisionales y aplicando ILM más tarde (registro doble), según cómo se especifiquen los requisitos de ILM.
- **Administración de copias**: Después de crear el número y el tipo de copias de objetos que se especifican en las instrucciones de colocación de ILM, StorageGRID administra las ubicaciones de objetos y protege los objetos contra pérdidas.
  - Análisis y evaluación de ILM: StorageGRID analiza continuamente la lista de objetos almacenados en la cuadrícula y comprueba si las copias actuales cumplen 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 de forma continua verificación en segundo plano para comprobar la integridad de los datos de objetos. Si se encuentra un problema, StorageGRID crea automáticamente una copia de objeto nueva o un fragmento de objeto con código de borrado de reemplazo en una ubicación que cumple los requisitos actuales de ILM. Consulte las instrucciones para Supervisión y solución de problemas de StorageGRID.
- **Eliminación de objetos**: La gestión 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 bien como resultado de la eliminación por ILM o la eliminación provocada por el vencimiento del ciclo de vida de un bloque de S3.

> Los objetos de un bloque con el bloqueo de objetos S3 activado no se pueden eliminar si se encuentran en una retención legal o si se ha especificado una fecha de retención hasta pero aún no se ha cumplido.

El diagrama resume el funcionamiento de ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

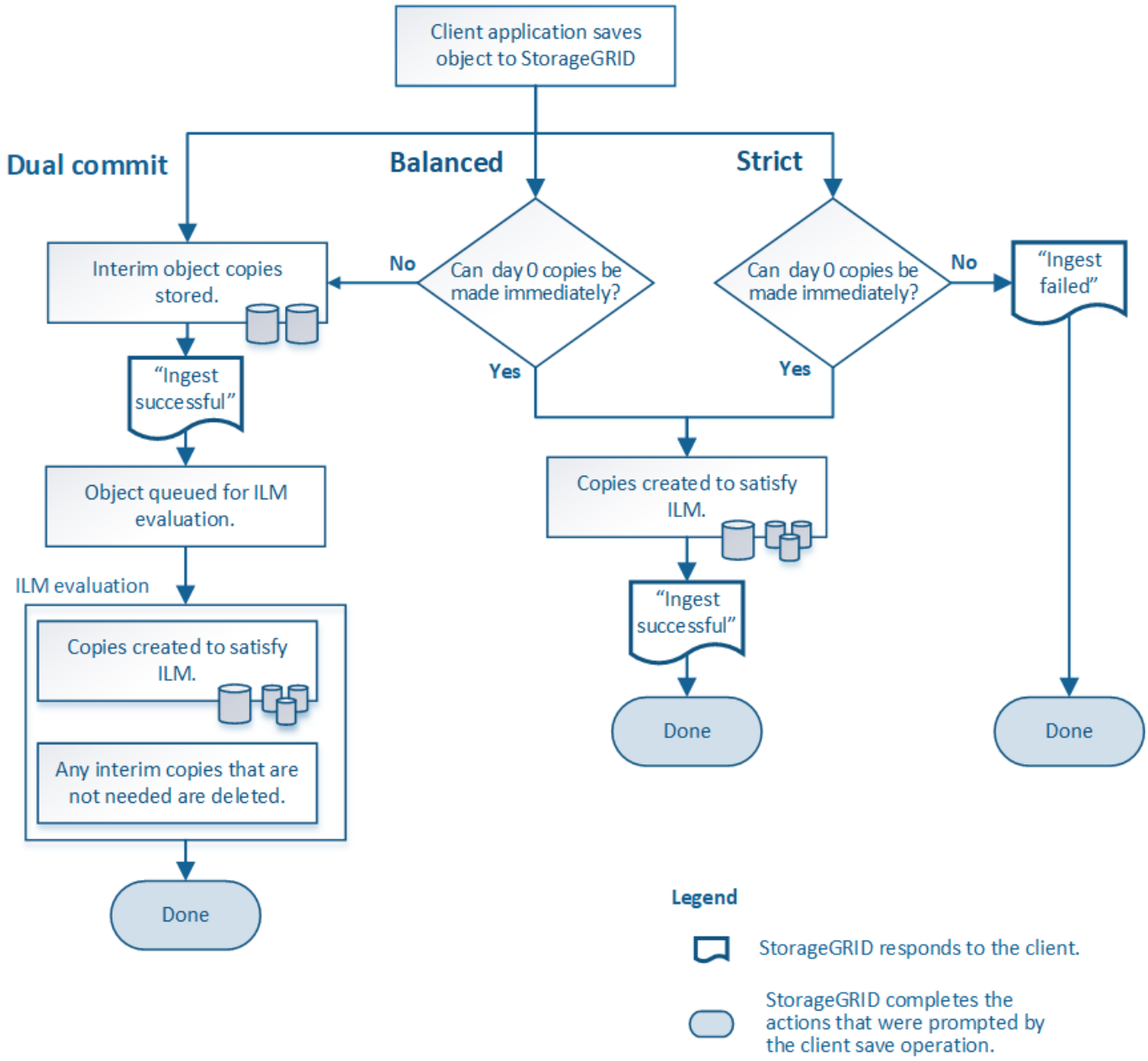
Opciones de protección de datos para consumo

Al crear una regla de ILM, debe especificar una de estas tres opciones para proteger los objetos durante la ingesta: Registro doble, equilibrado o estricto. Según elija,

StorageGRID realiza copias provisionales y pone en cola los objetos para la evaluación de ILM más tarde, o utiliza una ubicación síncrona y realiza copias inmediatamente para cumplir los requisitos de ILM.

Diagrama de flujo de tres opciones de ingesta

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



Registro doble

Al seleccionar la opción de confirmación doble, StorageGRID realiza inmediatamente copias provisionales de objetos en dos nodos de almacenamiento diferentes y devuelve un mensaje «'ingesta correcta'» al cliente. El objeto se pone en cola para la evaluación de ILM, y se realicen copias que cumplan con las instrucciones de ubicación de la regla más adelante.

Cuándo utilizar la opción Dual COMMIT

Utilice la opción Dual Commit en uno de los siguientes casos:

- Está usando reglas de la ILM de varios sitios y la latencia de procesamiento de clientes es su principal consideración. Al usar el registro doble, debe asegurarse de que su grid puede realizar el trabajo adicional de crear y eliminar las copias de registro doble si no satisfacen el ILM. Específicamente:
  - La carga en la cuadrícula debe ser lo suficientemente baja para evitar que se produzca una acumulación de ILM.
  - El grid debe tener un exceso de recursos de hardware (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Utiliza reglas de ILM de varios sitios y la conexión WAN entre los sitios suele tener una alta latencia o un ancho de banda limitado. En este escenario, el uso de la opción Dual commit puede ayudar a evitar los tiempos de espera de los clientes. Antes de elegir la opción Dual commit, debe probar la aplicación cliente con cargas de trabajo realistas.

Estricto

Al seleccionar la opción estricta, StorageGRID utiliza una ubicación síncrona al procesar y crea inmediatamente todas las copias de los objetos especificadas en las instrucciones de ubicación de la regla. Error al procesar si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento necesaria no está disponible temporalmente. El cliente debe volver a intentar la operación.

Cuándo usar la opción estricta

Utilice la opción estricta si tiene un requisito operativo y de normativa para almacenar inmediatamente objetos solo en las ubicaciones descritas en la regla de ILM. Por ejemplo, para satisfacer un requisito normativo, es posible que tenga que utilizar la opción estricta y un filtro avanzado de restricción de ubicación para garantizar que los objetos no se almacenen nunca en un centro de datos determinado.

Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto

Equilibrado

Cuando selecciona la opción equilibrada, StorageGRID también utiliza la ubicación síncrona durante la ingesta y hace 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 doble.

Cuándo utilizar la opción de equilibrio

Utilice la opción equilibrada para lograr la mejor combinación de protección de datos, rendimiento de grid y éxito de procesamiento. Balance es la opción predeterminada en el asistente de reglas de ILM.

Ventajas, inconvenientes y limitaciones de las opciones de protección de datos

Comprender las ventajas y las desventajas de cada una de las tres opciones de protección de datos en el procesamiento (confirmación equilibrada, estricta o doble) puede ayudarle a decidir cuál seleccionar para una regla de ILM.

Ventajas de las opciones equilibradas y estrictas

En comparación con el registro doble, que crea copias provisionales durante la ingesta, las dos opciones de colocación sincrónica pueden proporcionar las siguientes ventajas:

- **Mejor seguridad de datos**: Los datos de objeto están protegidos inmediatamente como se especifica en las instrucciones de colocación de la regla ILM, que se pueden configurar para proteger contra una amplia variedad de condiciones de fallo, incluyendo la falla de más de una ubicación de almacenamiento. La confirmación doble solo puede protegerse contra la pérdida de una única copia local.
- **Funcionamiento de red más eficiente**: Cada objeto se procesa una sola vez, ya que se ingiere. Dado que el sistema StorageGRID no necesita realizar un seguimiento o eliminar copias provisionales, hay menos carga de procesamiento y se consume menos espacio de la base de datos.
- **(equilibrado) recomendado**: La opción equilibrada proporciona una eficiencia óptima de ILM. Se recomienda utilizar la opción de equilibrio a menos que se requiera un comportamiento estricto de la ingesta o que la cuadrícula cumpla todos los criterios para la confirmación doble.
- **(estricta) certeza acerca de las ubicaciones de objetos**: La opción estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de colocación en la regla ILM.

Desventajas de las opciones equilibradas y estrictas

En comparación con la confirmación doble, las opciones equilibradas y estrictas tienen algunas desventajas:

- **Procesamiento de clientes más largos**: Las latencias de procesamiento de clientes pueden ser más largas. Al utilizar las opciones equilibradas y estrictas, no se devuelve al cliente un mensaje «'ingesta correcta» hasta que se crean y almacenan todos los fragmentos codificados con borrado o copias replicadas. Sin embargo, lo más probable es que los datos de objetos lleguen a su ubicación final mucho más rápido.
- **(estricta) tasas más altas de error de procesamiento**: Con la opción estricta, la ingesta falla cuando StorageGRID no puede realizar de inmediato todas las copias especificadas en la regla ILM. Es posible que observe tasas elevadas de error de procesamiento si una ubicación de almacenamiento necesaria está temporalmente sin conexión o si los problemas de red provocan retrasos en la copia de objetos entre sitios.
- * (Estricta) las ubicaciones de carga de varias partes de S3 pueden no ser las esperadas en algunas circunstancias*: Con estricta, se espera que los objetos se coloquen como se describe en la regla ILM o que falle el procesamiento. Sin embargo, con la carga de varias partes de S3, la gestión del ciclo de vida de la información se evalúa para cada parte del objeto según se ingiere y el objeto como un todo cuando se completa la carga de varias partes. En las siguientes circunstancias, esto podría dar lugar a colocaciones que son diferentes de lo esperado:
  - **Si ILM cambia mientras una carga multiparte de S3 está en curso**: Debido a que cada pieza se coloca según la regla que está activa cuando se ingiere la pieza, es posible que algunas partes del objeto no cumplan los requisitos actuales de ILM cuando se completa la carga de varias partes. En estos casos, la ingesta del objeto no falla. En su lugar, cualquier pieza que no se haya colocado correctamente se coloca en la cola de repetición de la evaluación de ILM y se mueve a la ubicación correcta más adelante.
  - **Cuando las reglas de ILM filtran el tamaño**: Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplen los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto, todas las partes del objeto se mueven a DC1.

- **(estricta) la ingesta no falla cuando las etiquetas de objeto o los metadatos se actualizan y las colocaciones recientemente requeridas no se pueden hacer**: Con estricto, se espera que los objetos se coloquen como se describe en la regla ILM o que falle el procesamiento. Sin embargo, cuando se actualizan metadatos o etiquetas de un objeto que ya está almacenado en la cuadrícula, el objeto no se vuelve a procesar. Esto significa que los cambios en la ubicación de objetos que se activan mediante la actualización no se realizan inmediatamente. Los cambios de colocación se realizan cuando la ILM se vuelve a evaluar por los procesos normales de ILM en segundo plano. Si no se pueden realizar cambios de colocación necesarios (por ejemplo, debido a que una ubicación recientemente requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que los cambios de colocación sean posibles.

Limitaciones en la colocación de objetos con las opciones equilibradas o estrictas

Las opciones equilibradas o estrictas no se pueden utilizar para las reglas de ILM que tengan cualquiera de las siguientes instrucciones de colocación:

- Ubicación en un pool de almacenamiento en cloud desde el día 0.
- Ubicación en un nodo de archivado en el día 0.
- Ubicaciones en un pool de almacenamiento en cloud o un nodo de archivado cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones existen porque StorageGRID no puede hacer copias de forma síncrona en un pool de almacenamiento en cloud o un nodo de archivado y un tiempo de creación definido por el usuario puede resolver este problema en el presente.

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

Tanto la regla de ILM como la elección del control de coherencia afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta la colocación inicial de las copias de objetos, mientras que el control de consistencia utilizado cuando se almacena un objeto afecta la colocación inicial de los metadatos de objetos. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

A continuación encontrará un breve resumen de los controles de consistencia disponibles en StorageGRID:

- **All**: Todos los nodos reciben metadatos de objeto inmediatamente o la solicitud falla.
- **Strong-global**: Los metadatos de objetos se distribuyen inmediatamente a todos los sitios. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
- **Strong-site**: Los metadatos del objeto se distribuyen inmediatamente a otros nodos en el sitio. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
- **Read-after-new-write**: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos.
- **Disponible** (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA.

Antes de seleccionar un nivel de coherencia, lea la descripción completa de los controles de coherencia en las instrucciones para S3 o. Swift aplicaciones cliente. Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo puede interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **Norma ILM**: Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Se ha seleccionado el comportamiento de procesamiento estricto.
- **Nivel de coherencia**: "Strong-global" (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

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

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si en su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto 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 de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre los niveles de coherencia y las reglas del ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Información relacionada

- Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto

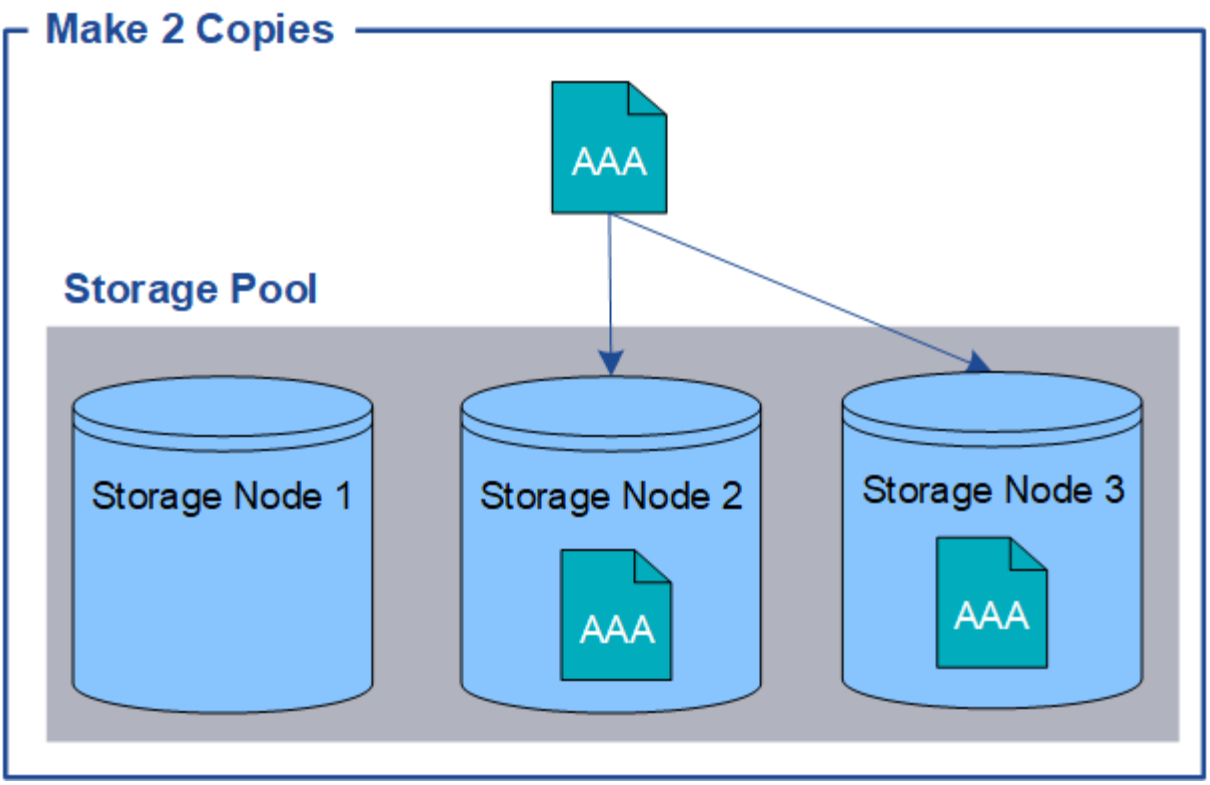
Cómo se almacenan los objetos (codificación de borrado o replicación)

Qué es la replicación

La replicación es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos. Cuando los objetos coinciden con una regla de ILM que usa la replicación, el sistema crea copias exactas de datos de objetos y almacena las copias en nodos de almacenamiento o nodos de archivado.

Cuando configura una regla de ILM para crear copias replicadas, especifica cuántas copias se deben crear, dónde deben ubicarse y cuánto tiempo deben almacenarse las copias en cada ubicación.

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



Cuando StorageGRID coincide con los objetos de esta regla, crea dos copias del objeto, colocando cada copia en un nodo de almacenamiento diferente en el pool de almacenamiento. Las dos copias pueden colocarse en 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. Debido a que hay dos copias, el objeto se puede recuperar si alguno de los nodos del pool de almacenamiento falla.

> StorageGRID solo puede almacenar una copia replicada de un objeto en un nodo de almacenamiento dado. Si el grid incluye tres nodos de almacenamiento y se crea una regla de gestión del ciclo de vida de la información de 4 copias, solo se crearán tres copias: Una por cada nodo de almacenamiento. Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

Información relacionada

- Qué es un pool de almacenamiento
- Utilice varios pools de almacenamiento para la replicación entre sitios

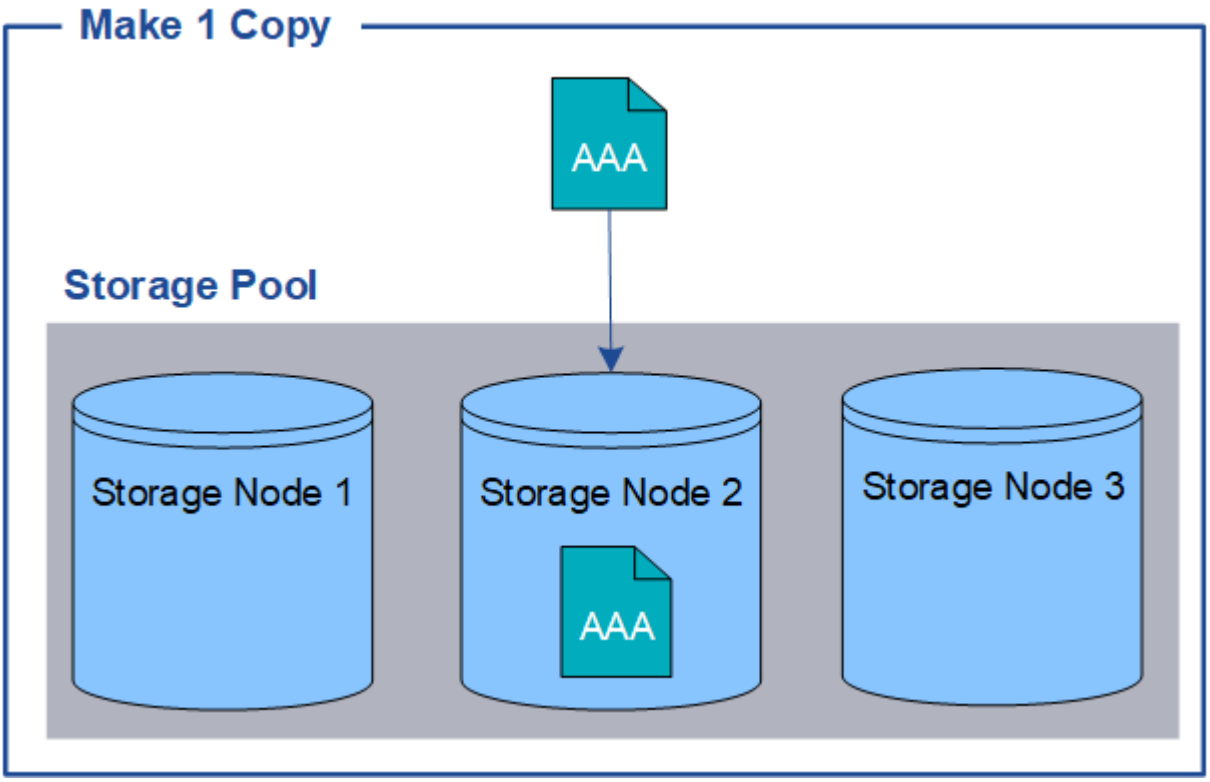
Por qué no se debe utilizar la replicación de copia única

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

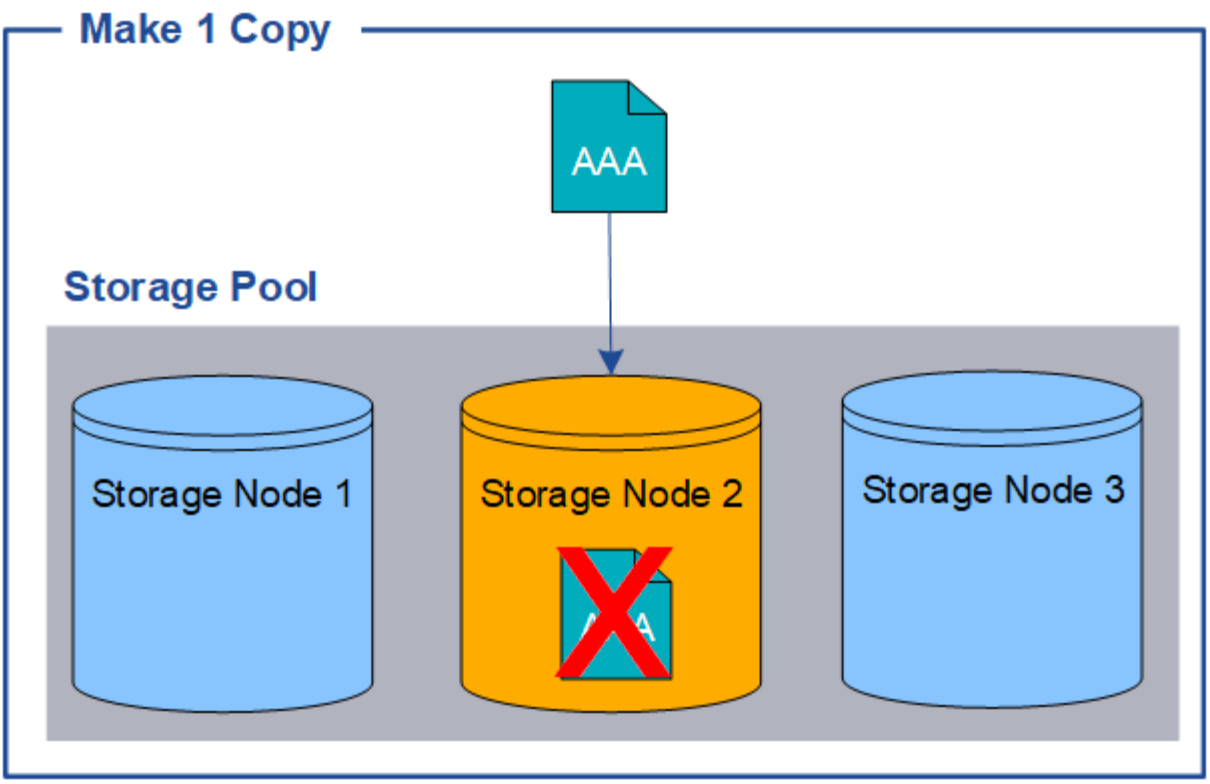
> No utilice una regla de ILM que solo cree una copia replicada durante un periodo de tiempo. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

En el ejemplo siguiente, la regla Make 1 Copy ILM especifica que una copia replicada de un objeto se coloca en un pool de almacenamiento que contiene tres nodos de almacenamiento. Cuando se ingiere un objeto que

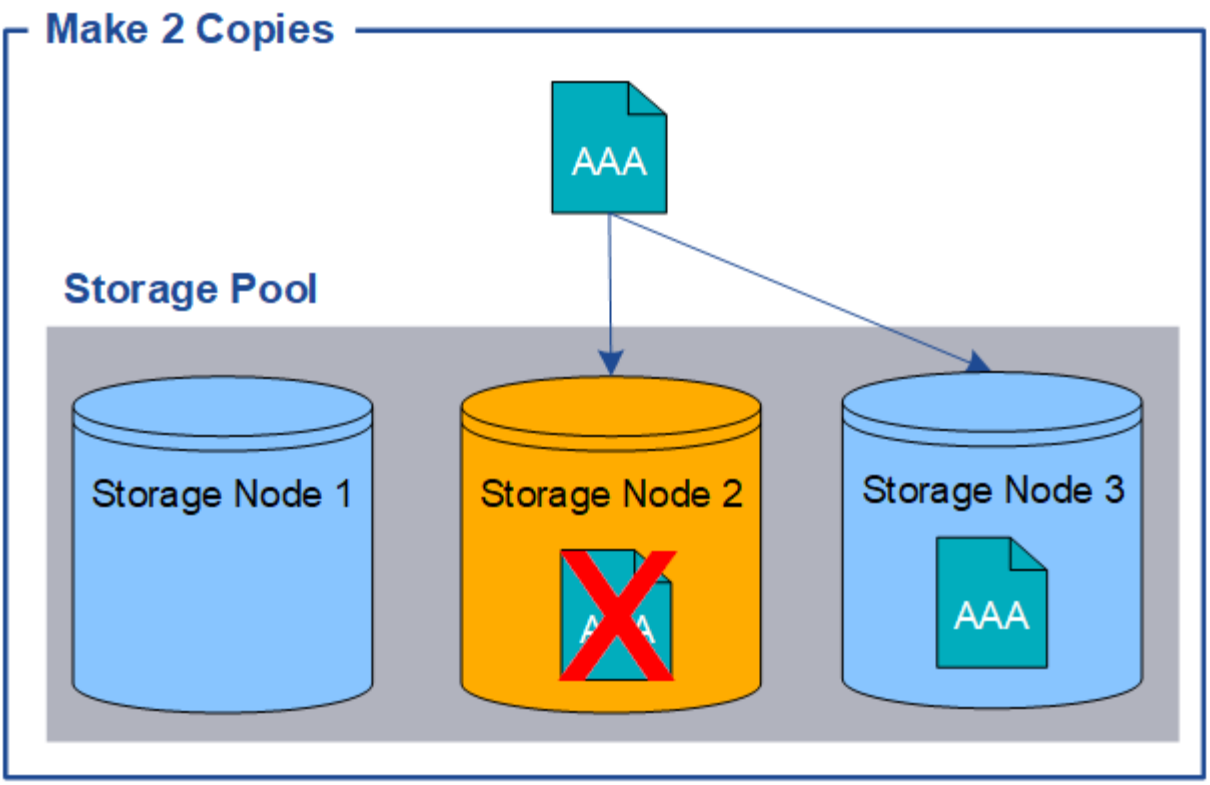
coincida con esta regla, StorageGRID coloca una sola copia en un solo nodo de almacenamiento.



Cuando una regla de ILM crea solo una copia replicada de un 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 desconectado, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA completamente si falla el nodo de almacenamiento 2.



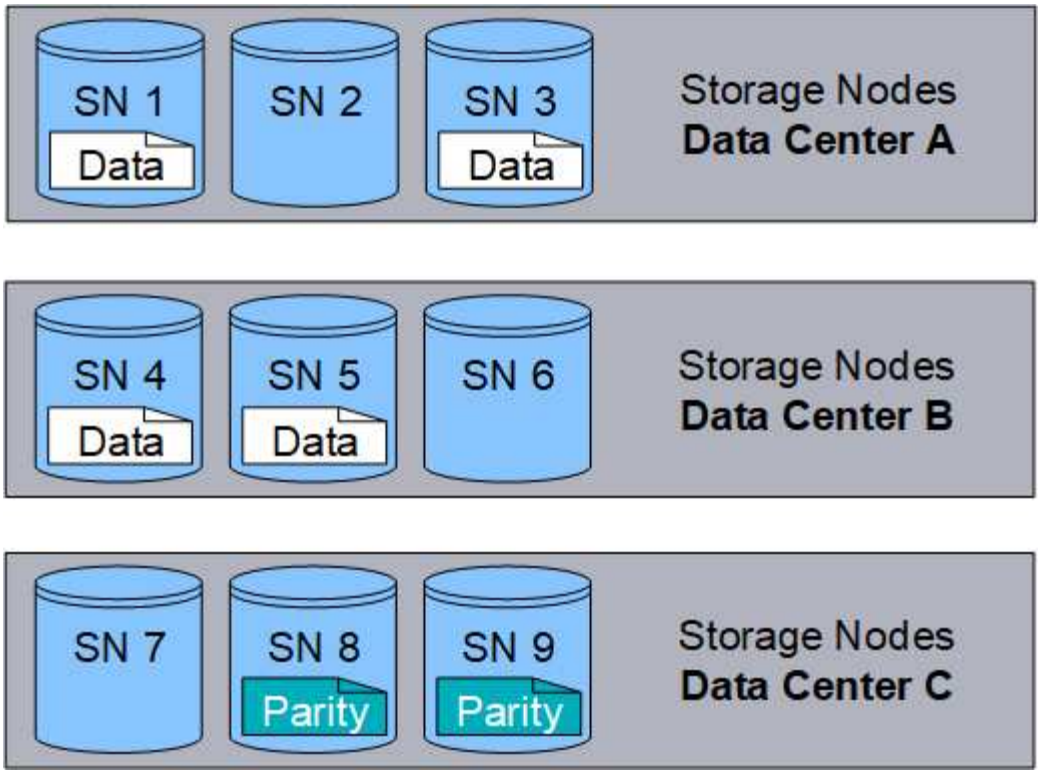
Para evitar la pérdida de datos de objetos, siempre debe realizar al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, puede seguir teniendo acceso al objeto si un nodo de almacenamiento falla o se desconecta.



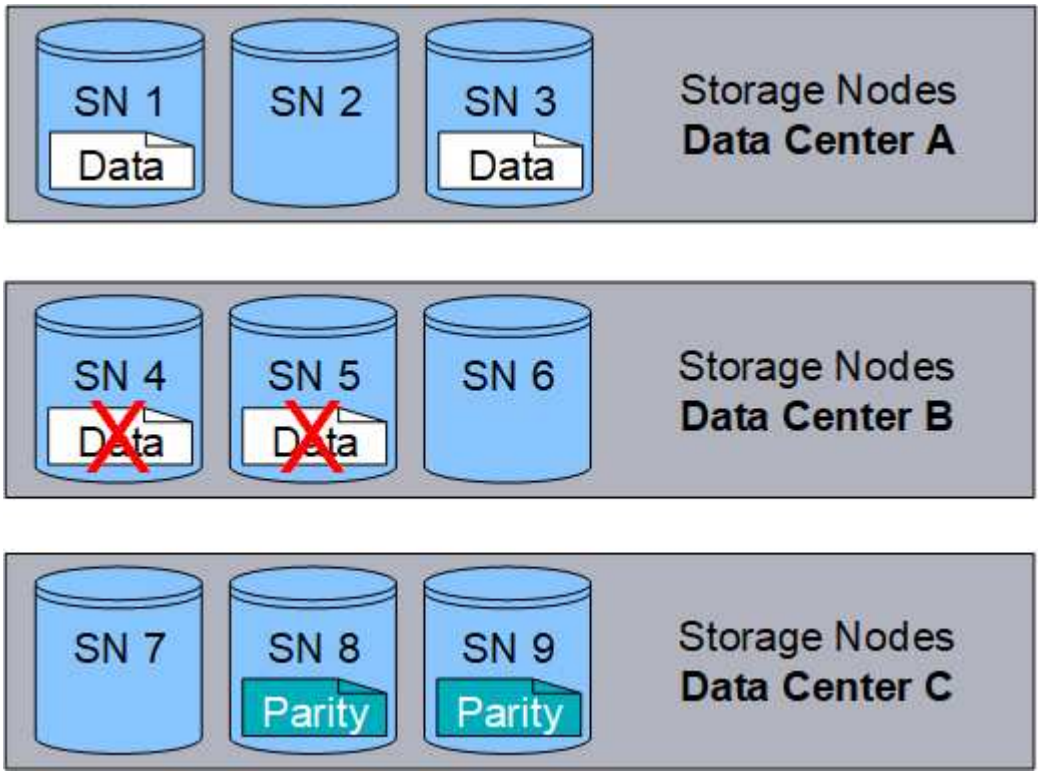
Qué es la codificación de borrado

El código de borrado es el segundo método que utiliza StorageGRID para almacenar datos de objetos. Cuando StorageGRID enlaza objetos con una regla de ILM que se configura para crear copias con código de borrado, corta los datos de objetos en fragmentos de datos, calcula fragmentos de paridad adicionales y almacena cada fragmento en un nodo de almacenamiento diferente. Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un dato o un fragmento de paridad se corrompen o se pierden, el algoritmo de código de borrado puede recrear ese fragmento con un subconjunto de los datos restantes y los fragmentos de paridad.

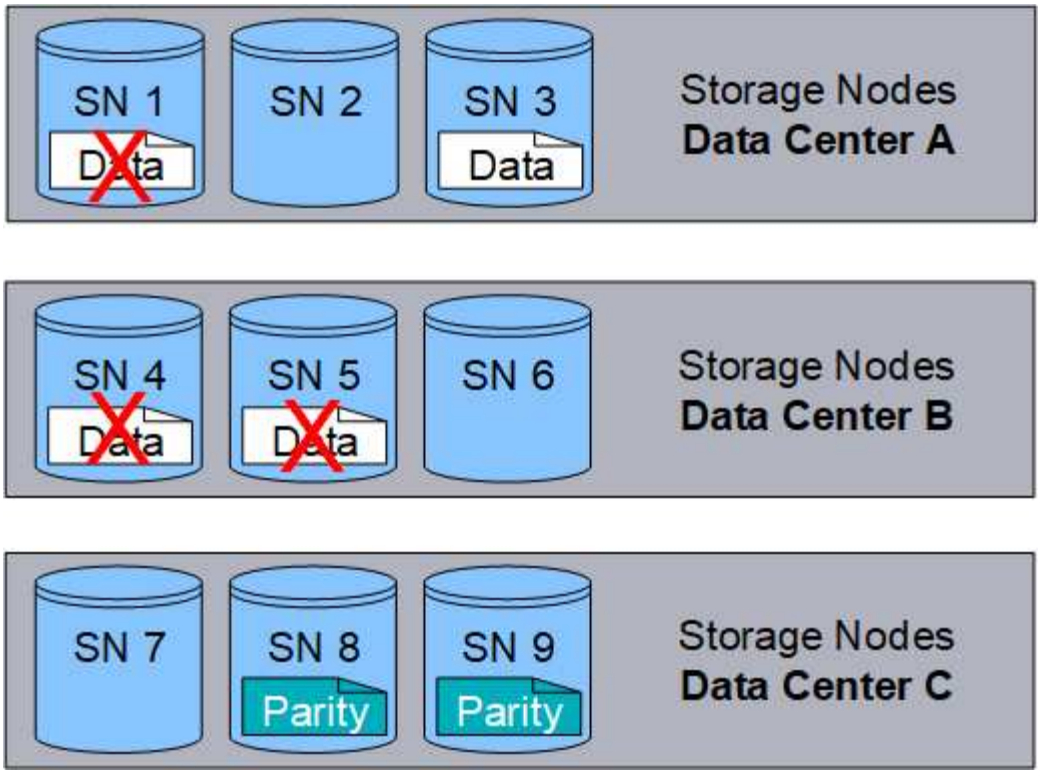
En el siguiente ejemplo, se muestra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir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



El esquema de codificación de borrado 4+2 requiere un mínimo de nueve nodos de almacenamiento, con tres nodos de almacenamiento en cada uno de tres sitios diferentes. Un objeto se puede recuperar 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 completo del centro de datos, aún se puede recuperar o reparar el objeto, siempre que todos los demás fragmentos permanezcan accesibles.



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



Información relacionada

- Qué es un pool de almacenamiento
- Qué son los esquemas de codificación de borrado
- Cree un perfil de código de borrado

Qué son los esquemas de codificación de borrado

Cuando configura el perfil de código de borrado para una regla de ILM, debe seleccionar un esquema de codificación de borrado disponible basado en la cantidad de nodos y sitios de almacenamiento que componen el pool de almacenamiento que planea utilizar. Los esquemas de codificación de borrado controlan cuántos fragmentos de datos se crean y cuántos fragmentos de paridad se crean para cada objeto.

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo corta un objeto en fragmentos de datos k y calcula fragmentos de paridad m. Los fragmentos k + m = n se distribuyen en n nodos de almacenamiento para proporcionar protección de datos. Un objeto puede sostener hasta m fragmentos perdidos o corruptos. se necesitan fragmentos k para recuperar o reparar un objeto.

Al configurar un perfil de código de borrado, siga las siguientes directrices para los pools de almacenamiento:

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

  > No es posible configurar un perfil de código de borrado si el pool de almacenamiento incluye dos sitios.

  - Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios
  - Esquemas de codificación de borrado para pools de almacenamiento in situ

- No utilice el pool de almacenamiento predeterminado, todos los nodos de almacenamiento ni un grupo de almacenamiento que incluya el sitio predeterminado, todos los sitios.
- El pool de almacenamiento debe incluir al menos *k*+*m* +1 nodos de almacenamiento.

  La cantidad mínima de nodos de almacenamiento necesarios es *k*+*m*. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a evitar fallos de ingesta o errores de gestión de la vida útil si un nodo de almacenamiento necesario no está disponible temporalmente.

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

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

Por ejemplo, si almacena un objeto de 10 MB mediante el esquema 4+2 (que tiene un 50% de sobrecarga de almacenamiento), el objeto consume 15 MB de almacenamiento de cuadrícula. Si almacena el mismo objeto de 10 MB con el esquema 6+2 (que tiene un 33% de sobrecarga de almacenamiento), el objeto consume aproximadamente 13.3 MB.

Seleccione el esquema de código 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 suelen ser más eficientes desde el punto de vista computacional, ya que se crean y distribuyen (o se recuperan) por objeto, pueden mostrar un mejor rendimiento debido al mayor tamaño de fragmento y pueden requerir menos nodos en una expansión cuando se necesita más almacenamiento. (Consulte las instrucciones para ampliar StorageGRID para obtener información sobre cómo planificar una ampliación de almacenamiento.)

Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios

En la siguiente tabla se describen los esquemas de codificación de borrado que admite actualmente StorageGRID para pools de almacenamiento que incluyen tres o más sitios. Todos estos esquemas proporcionan protección contra pérdida de sitio. Se puede perder un sitio y el objeto seguirá siendo accesible.

En el caso de los esquemas de codificación de borrado que proporcionan protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el pool de almacenamiento supera *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 %

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
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 usar cinco nodos de almacenamiento por sitio.

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

- **Número de fragmentos**: El rendimiento y la flexibilidad de expansión son generalmente 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 superior).
- **Tráfico de red**: Cuando se recupera de fallos, usando 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 mayor sobrecarga requieren más espacio de almacenamiento por objeto.

Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3 (que ambos tienen un 50% de gastos generales de almacenamiento), seleccione el esquema 6+3 si se requiere tolerancia a fallos 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 usar, seleccione 4+2 o 6+3, o póngase en contacto con el servicio de asistencia técnica.

Esquemas de codificación de borrado para pools de almacenamiento in situ

Un pool de almacenamiento in situ admite todos los esquemas de codificación de borrado definidos para tres o más sitios, siempre y cuando el sitio tenga suficientes nodos de almacenamiento.

La cantidad mínima de nodos de almacenamiento necesarios es *k*+*m*, pero se recomienda un pool de almacenamiento con nodos *k*+*m*+1. Por ejemplo, el esquema de codificación de borrado 2+1 requiere un pool 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 %

Información relacionada

Amplíe su grid

Ventajas, desventajas y requisitos de codificación de borrado

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

Ventajas de la codificación de borrado

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

- **Confiabilidad**: La fiabilidad se mide en términos de tolerancia a fallos, es decir, el número de fallos simultáneos que se pueden sostener sin pérdida de datos. Con la replicación, se almacenan varias copias idénticas en diferentes nodos y entre sitios. Con el código de borrado, un objeto se codifica en fragmentos de datos y de paridad, y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección frente a fallos del sitio y del nodo. En comparación con la replicación, la codificación de borrado proporciona una mayor fiabilidad con costes 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 con costes de almacenamiento comparables.
- **Eficiencia del almacenamiento**: Para niveles similares de disponibilidad y fiabilidad, los objetos protegidos mediante codificación de borrado consumen menos espacio en disco que los mismos objetos si están 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 se elimina 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 los objetos codificados de borrado se calcula como el tamaño del objeto más la sobrecarga del almacenamiento. El porcentaje de sobrecarga del almacenamiento es el número de fragmentos de paridad dividido por el número de fragmentos de datos.

Desventajas del código de borrado

En comparación con la replicación, los códigos de borrado tienen las siguientes desventajas:

- Se requiere un mayor número de nodos y sitios de almacenamiento. Por ejemplo, si utiliza un esquema de código de borrado de 6+3, debe tener al menos tres nodos de almacenamiento en tres sitios diferentes. Por el contrario, si simplemente replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia.
- Aumento del coste y de la complejidad de las ampliaciones del almacenamiento. Para ampliar una puesta en marcha que usa la replicación, solo tiene que agregar capacidad de almacenamiento en cada ubicación donde se realicen copias de objetos. Para ampliar una puesta en marcha que utilice código de borrado, debe tener en cuenta el esquema de codificación de borrado y el grado de llenado de los nodos de almacenamiento existentes. Por ejemplo, si espera que los nodos existentes estén llenos al 100 %, debe añadir al menos *k+m* nodos de almacenamiento, pero si expande cuando los nodos existentes están llenos al 70 %, puede añadir dos nodos por sitio y seguir maximizando la capacidad de almacenamiento útil. Para obtener más información, consulte Añada capacidad de almacenamiento para objetos codificados de borrado.
- Al utilizar códigos de borrado en ubicaciones distribuidas geográficamente, aumenta la latencia de recuperación. Los fragmentos de objeto para un objeto que se codifica con borrado y se distribuyen en sitios remotos tardan más en recuperarse a través de conexiones WAN que los objetos que se replican y están disponibles localmente (el mismo sitio al que se conecta el cliente).
- Al utilizar la codificación de borrado en ubicaciones distribuidas geográficamente, se está utilizando más el tráfico de red WAN para restauraciones y reparaciones, especialmente en objetos que se recuperan con frecuencia o para reparaciones de objetos a través de conexiones de red WAN.
- Cuando se utiliza la codificación de borrado en varios sitios, el rendimiento máximo del objeto se reduce drásticamente a medida que aumenta la latencia de red entre sitios. Esta disminución se debe a la correspondiente disminución del rendimiento de la red TCP, que afecta a la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objeto.
- Mayor uso de recursos de computación.

Cuándo se debe utilizar la codificación de borrado

El código de borrado se ajusta mejor a los siguientes requisitos:

- Los objetos tienen un tamaño superior a 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

- Almacenamiento a largo plazo o en frío para contenido que se recupera con poca frecuencia.
- Alta disponibilidad y fiabilidad de los datos.
- Protección frente a fallos completos de sitios y nodos.

- Eficiencia del almacenamiento.
- Puestas en marcha de un único sitio que requieren protección de datos eficiente con solo una copia codificada por borrado en lugar de múltiples copias replicadas.
- Puestas en marcha de varios sitios en las que la latencia entre sitios es inferior a 100 ms.

Cómo se determina la retención de objetos

StorageGRID ofrece opciones tanto para los administradores de grid como para los usuarios individuales de inquilino para especificar el tiempo que se tarda en 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 grid.

Cómo los usuarios de inquilinos controlan la retención de objetos

Los usuarios de inquilinos tienen tres formas principales de controlar cuánto tiempo se almacenan los objetos en StorageGRID:

- Si la configuración global de Object Lock está habilitada para el grid, los usuarios inquilinos S3 pueden crear bloques con S3 Object Lock habilitado y, a continuación, utilizar la API REST de S3 para especificar la configuración de retención hasta la fecha y la conservación legal de cada versión de objeto añadida a ese bloque.
  - Cualquier método no puede eliminar una versión de objeto que esté bajo una retención legal.
  - Antes de que se alcance la fecha de retención de una versión de objeto, dicha versión no se puede eliminar mediante ningún método.
  - Los objetos en bloques con S3 Object Lock habilitado son mantenidos por ILM "'eternamente'". Sin embargo, una vez alcanzada la fecha de retención hasta la fecha, una solicitud de cliente puede eliminar una versión de objeto o la expiración del ciclo de vida de la cuchara. Consulte Gestione objetos con S3 Object Lock.
- Los usuarios de inquilinos S3 pueden añadir una configuración del ciclo de vida a sus bloques que especifica una acción de caducidad. Si existe un ciclo de vida de un bloque, StorageGRID almacena un objeto hasta que se cumpla la fecha o el número de días especificados en la acción Expiración, a menos que el cliente elimine primero el objeto. Consulte Cree una configuración del ciclo de vida de S3.
- Un cliente S3 o Swift puede emitir una solicitud de eliminación de objeto. StorageGRID siempre prioriza las solicitudes de eliminación de clientes por encima del ciclo de vida de los bloques S3 o ILM al determinar si se debe eliminar o conservar un objeto.

Cómo los administradores de grid controlan la retención de objetos

Los administradores de grid utilizan las instrucciones de colocación de ILM para controlar la duración de los objetos almacenados. Cuando una regla de ILM coincide con los objetos, StorageGRID almacena esos objetos hasta que haya transcurrido el último periodo de tiempo de la regla de ILM. Los objetos se conservan indefinidamente si se especifica "'eternamente'" para las instrucciones de colocación.

Independientemente de quién controle cuánto tiempo se retienen los objetos, la configuración de ILM controla qué tipos de copias de objetos (replicadas o codificadas de borrado) se almacenan y dónde se encuentran las copias (nodos de almacenamiento, pools de almacenamiento en cloud o nodos de archivado).

Cómo interaccionan el ciclo de vida de bloque y ILM de S3

La acción de caducidad en un ciclo de vida de bloque de S3 siempre anula la configuración de ILM. Como resultado, es posible que un objeto se conserve en la cuadrícula aunque hayan caducado las instrucciones de gestión del ciclo de vida de la información relativas a la ubicación del objeto.

Ejemplos para la retención de objetos

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

Ejemplo 1: El ciclo de vida de un bloque de S3 mantiene los objetos durante más tiempo que ILM

ILM

Almacene dos copias por 1 año (365 días)

Ciclo de vida del cucharón

Caducidad de objetos en 2 años (730 días)

Resultado

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

> Si el ciclo de vida de un bloque especifica que los objetos se deben conservar durante más tiempo del ciclo de vida de la información especificado por ILM, StorageGRID sigue usando las instrucciones de colocación de ILM al determinar el número y el tipo de copias que se deben almacenar. En este ejemplo, se seguirán almacenando dos copias del objeto en StorageGRID de los días 366 a 730.

Ejemplo 2: El ciclo de vida de bloque de S3 caduca los objetos antes de ILM

ILM

Almacene dos copias durante 2 años (730 días)

Ciclo de vida del cucharón

Caducar objetos en un año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: La eliminación de clientes anula el ciclo de vida del bloque y el ILM

ILM

Almacenar dos copias en nodos de almacenamiento «para siempre»

Ciclo de vida del cucharón

Caducidad de objetos 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 de S3

La fecha de retención hasta la versión de un objeto es 2026-03-31. No existe un derecho legal.

Regla de ILM que cumpla con las normativas

Almacenar dos copias en nodos de almacenamiento «para siempre».

Solicitud de eliminación de cliente

Emitido el 2024-03-31.

Resultado

StorageGRID no eliminará la versión del objeto porque la fecha de retención hasta todavía está a 2 años.

Cómo se eliminan los objetos

StorageGRID puede eliminar objetos en respuesta directa a una solicitud del cliente o de forma automática como resultado del vencimiento del ciclo de vida de un bloque de S3 o de los requisitos de la política de ILM. Comprender las diferentes formas en que se pueden eliminar los objetos y el modo en que StorageGRID gestiona las solicitudes de eliminación puede ayudarle a gestionar los objetos de forma más eficaz.

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

- Eliminación síncrona: Cuando StorageGRID recibe una solicitud de eliminación de cliente, todas las copias de los objetos se eliminan de inmediato. Se informa al cliente de que la eliminación se ha realizado correctamente una vez eliminadas las copias.
- Los objetos se ponen en cola para eliminación: Cuando StorageGRID recibe una solicitud de eliminación, el objeto se pone en cola para su eliminación y se informa al cliente inmediatamente de que esta se ha eliminado correctamente. Las copias de objetos se eliminan más adelante mediante el procesamiento de ILM en segundo plano.

Cuando se eliminan objetos, StorageGRID utiliza el método que optimiza el rendimiento de eliminación, minimiza las posibles acumulaciones de eliminación y libera espacio que se libera con mayor rapidez.

La tabla resume cuándo StorageGRID utiliza cada método.

Método de eliminación	Cuando se utilice
Los objetos se mantienen en la cola para su eliminación	Cuando **cualquiera** de las siguientes condiciones se cumple: • La eliminación automática de objetos ha sido activada por uno de los siguientes eventos: ◦ Se ha alcanzado la fecha de caducidad o el número de días en la configuración del ciclo de vida de un bloque de S3. ◦ El último periodo de tiempo especificado en una regla de ILM transcurre. **Nota:** los objetos de un contenedor que tiene habilitado el bloqueo de objetos S3 no se pueden eliminar si están en una reserva legal o si se ha especificado una fecha de retención, pero aún no se ha cumplido. • Un cliente de S3 o Swift solicita la eliminación y se debe cumplir una o varias de estas condiciones: ◦ Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, una ubicación de objeto no está disponible temporalmente. ◦ Las colas de eliminación en segundo plano están inactivas.
Los objetos se quitan de inmediato (eliminación síncrona)	Cuando un cliente S3 o Swift realiza una solicitud de eliminación y **se cumplen todas** las siguientes condiciones: • Todas las copias se pueden eliminar en 30 segundos. • Las colas de eliminación en segundo plano contienen objetos que se van a procesar.

Cuando los clientes de S3 o Swift realizan solicitudes de eliminación, StorageGRID comienza agregando una serie de objetos a la cola de eliminación. A continuación, cambia a realizar una eliminación síncrona. Asegurarse de que la cola de eliminación en segundo plano tiene objetos que procesar permite a StorageGRID procesar las eliminaciones de forma más eficaz, especialmente en los clientes de baja concurrencia, mientras que ayuda a evitar que los clientes eliminen las copias de seguridad.

Cuánto tiempo se tarda en eliminar objetos

La forma en que StorageGRID elimina los objetos puede afectar a la forma en la que aparece el sistema:

- Cuando StorageGRID realiza la eliminación síncrona, StorageGRID puede tardar hasta 30 segundos en devolver un resultado al cliente. Esto significa que la eliminación puede parecer más lenta, aunque en realidad se eliminan copias más rápidamente de lo que están cuando StorageGRID pone en cola objetos para su eliminación.
- Si supervisa de cerca el rendimiento de eliminación durante una eliminación masiva, puede observar que la tasa de eliminación aparece como lenta después de eliminar un cierto número de objetos. Este cambio ocurre cuando StorageGRID pasa de poner objetos en cola para su eliminación a realizar una eliminación síncrona. La reducción aparente en la tasa de eliminación no significa que las copias de objetos se van a eliminar más lentamente. Por el contrario, indica que, en promedio, ahora se libera espacio con más rapidez.

Si elimina un gran número de objetos y la prioridad es liberar espacio rápidamente, considere la posibilidad de usar una solicitud de cliente para eliminar objetos en lugar de eliminarlos con ILM u otros métodos. En general, el espacio se libera más rápidamente cuando los clientes lo eliminan, ya que StorageGRID puede utilizar la eliminación síncrona.

Debe tener en cuenta que la cantidad de tiempo necesario para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de objetos se eliminan de forma síncrona o se ponen en cola para su eliminación más adelante (para solicitudes de eliminación de clientes).
- Otros factores, como el número de objetos de la cuadrícula o la disponibilidad de los recursos de grid cuando las copias de objetos se colocan en cola para su eliminación (tanto para los eliminaciones del cliente como para otros métodos).

Cómo se eliminan los objetos con versiones de S3

Cuando se habilita el control de versiones para un bloque de S3, StorageGRID sigue el comportamiento de Amazon S3 al responder a las solicitudes de eliminación, ya provenga de un cliente S3, el vencimiento de un ciclo de vida de un bloque de S3 o los requisitos de la política de ILM.

Cuando se crea una versión de los objetos, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto y no liberan espacio. En su lugar, una solicitud de eliminación de objetos simplemente crea un marcador de borrado como la versión actual del objeto, que hace que la versión anterior del objeto sea "'no actual'".

Aunque el objeto no se haya quitado, 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 los datos de objeto no actuales no se han eliminado, las solicitudes que especifican una versión no actual del objeto pueden tener éxito.

Para liberar espacio al eliminar objetos con versiones, debe realizar una de las siguientes acciones:

- **Solicitud de cliente S3**: Especifique el número de versión del objeto en la solicitud DE ELIMINACIÓN de objeto S3 (`DELETE /object?versionId=ID`). Tenga en cuenta que esta solicitud sólo elimina copias de objetos para la versión especificada (las otras versiones todavía ocupan espacio).
- **Ciclo de vida del cucharón**: Utilice `NoncurrentVersionExpiration` acción en la configuración del ciclo de vida del bloque. Cuando se cumple el número de días sin currentDays especificado, StorageGRID elimina permanentemente todas las copias de las versiones de objetos no actuales. Estas versiones de objeto no se pueden recuperar.
- **ILM**: Agregue dos reglas ILM a su política de ILM. Utilice **tiempo no corriente** como tiempo de referencia en la primera regla para coincidir con las versiones no actuales del objeto. Utilice **tiempo de procesamiento** en la segunda regla para que coincida con la versión actual. La regla **tiempo no corriente** debe aparecer en la directiva por encima de la regla **tiempo de ingesta**.

Información relacionada

- Use S3
- Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3

Qué es una política de ILM

Una política de gestión de ciclo de vida de la información (ILM) es un conjunto ordenado de reglas de ILM que determinan el modo en que el sistema StorageGRID gestiona los

datos de objetos a lo largo del tiempo.

¿Cómo evalúa objetos una política de ILM?

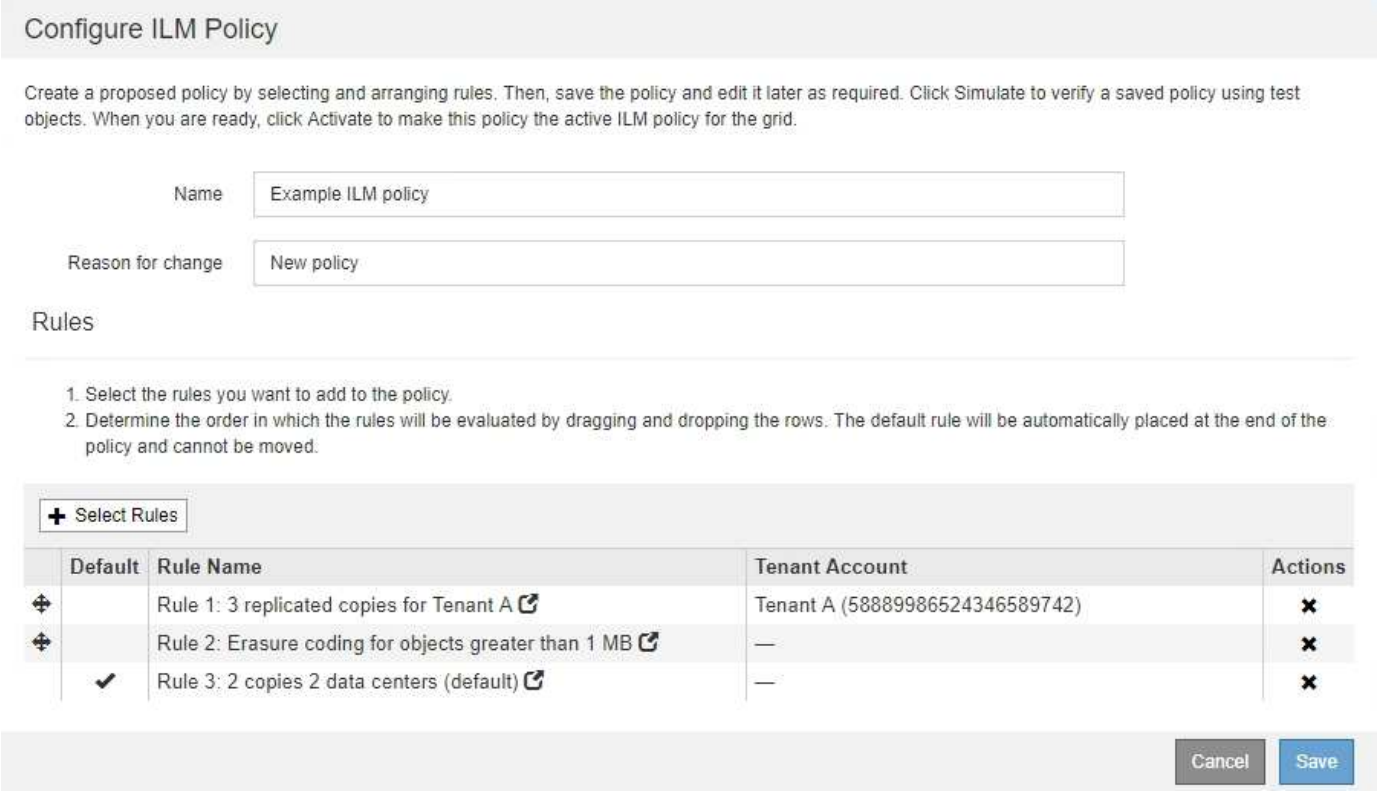
La política activa de ILM para su sistema StorageGRID controla la ubicación, la duración y la protección de datos de todos los objetos.

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

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se procesa según el comportamiento de procesamiento de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa en función de cada regla posterior de la política hasta que se realice una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican las instrucciones de comportamiento de procesamiento y colocación de la regla predeterminada de la directiva. La regla predeterminada es la última regla de una directiva. La regla predeterminada debe aplicarse a todos los inquilinos, todos los bloques y todas las versiones del objeto, y no puede utilizar ningún filtro avanzado.

Ejemplo de política de ILM

Este ejemplo de política de ILM usa tres reglas de ILM.

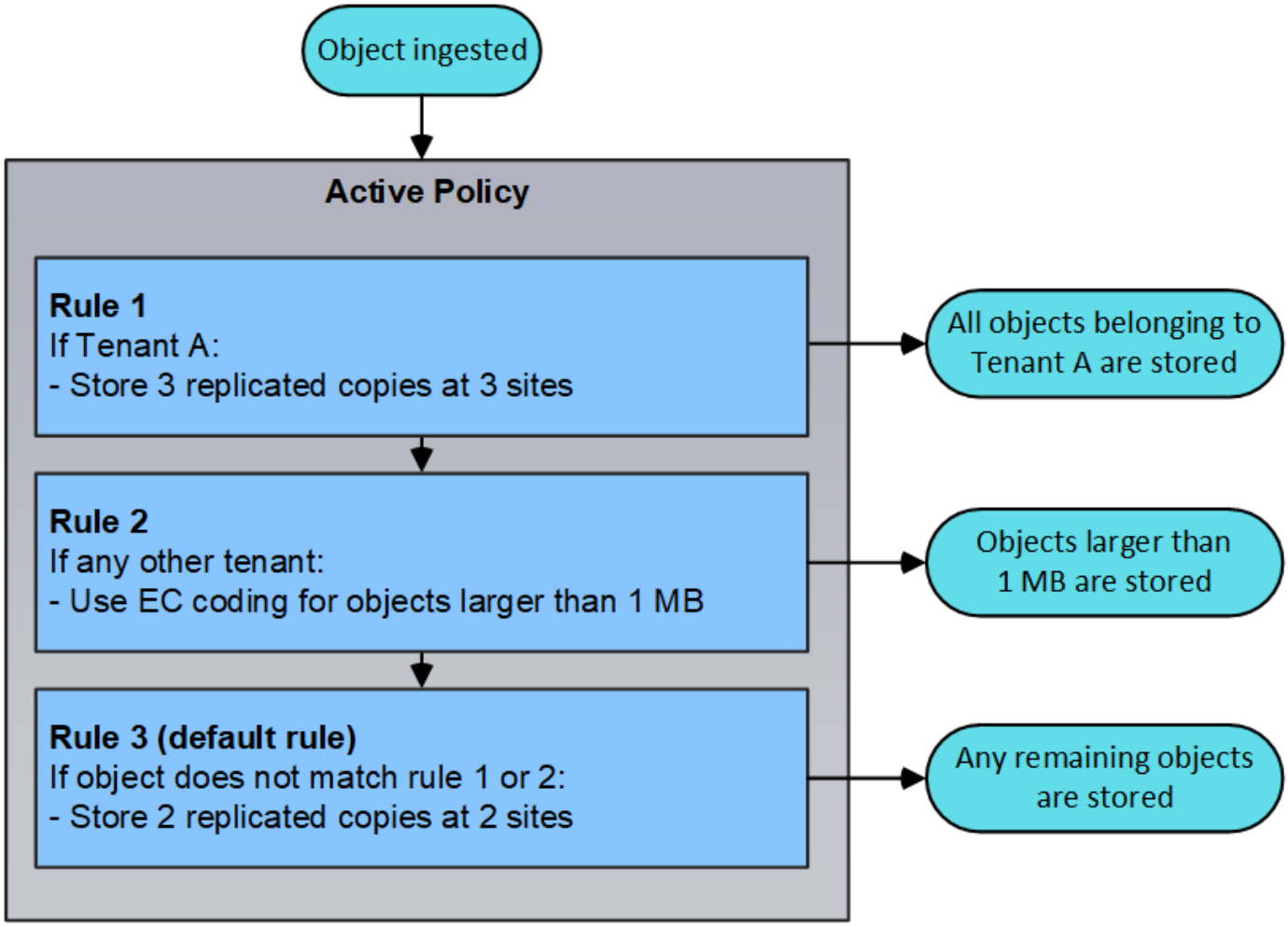


En este ejemplo, la regla 1 coincide con todos los objetos que pertenecen al arrendatario A. Estos objetos se almacenan como tres copias replicadas en tres sitios. Los objetos pertenecientes a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan en función de la Regla 2.

La regla 2 coincide con todos los objetos de otros arrendatarios, pero sólo si son superiores a 1 MB. Estos

objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones. La regla 2 no coincide con los objetos de 1 MB o menos, por lo que estos objetos se evalúan en función de la regla 3.

La regla 3 es la última regla y la regla predeterminada de la política y no utiliza filtros. La regla 3 realiza dos copias replicadas de todos los objetos que no coinciden en la regla 1 o la regla 2 (objetos que no pertenecen al arrendatario A que son de 1 MB o menos).



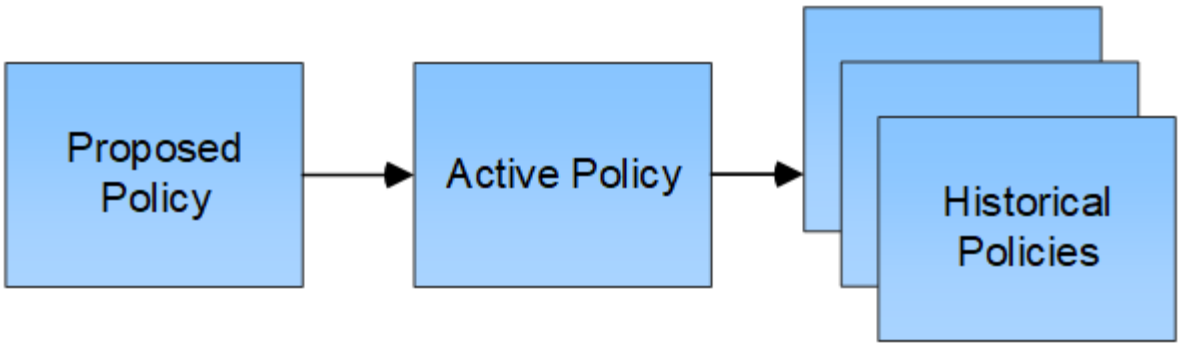
¿Qué son las políticas propuestas, activas e históricas?

Todos los sistemas StorageGRID deben tener una política de ILM activa. Un sistema StorageGRID también puede tener una política de ILM propuesta y cualquier número de políticas históricas.

Cuando se crea por primera vez una política de ILM, se crea una política propuesta seleccionando una o varias reglas de ILM y ordenándolas en un orden específico. Después de simular la política propuesta para confirmar su comportamiento, la activa para crear la política activa.

Cuando se activa una nueva política de ILM, StorageGRID utiliza esa política para gestionar todos los objetos, incluidos los objetos existentes y los objetos recién procesados. Es posible que los objetos existentes se muevan a nuevas ubicaciones cuando se implementen las reglas de ILM en la nueva política.

La activación de la directiva propuesta hace que la directiva previamente activa se convierta en una directiva histórica. No se pueden eliminar las políticas históricas de ILM.



Información relacionada

Cree una política de ILM

Qué es una regla de ILM

Para gestionar objetos, debe crear un conjunto de reglas de gestión de ciclo de vida de la información (ILM) y organizarlas en una política de ILM. Cada objeto ingerido en el sistema se evalúa según la política activa. Cuando una regla de la política coincide con los metadatos de un objeto, las instrucciones de la regla determinan las acciones que StorageGRID lleva a cabo para copiar y almacenar ese objeto.

Las reglas de ILM definen:

- Qué objetos se deben almacenar. Una regla se puede aplicar a todos los objetos o puede especificar filtros para identificar a qué objetos se aplica una regla. Por ejemplo, una regla puede aplicarse solo a los objetos asociados con determinadas cuentas de inquilino, bloques S3 específicos o contenedores Swift, o valores de metadatos específicos.
- El tipo de almacenamiento y la ubicación. Los objetos se pueden almacenar en nodos de almacenamiento, en pools de almacenamiento en cloud o en nodos de archivado.
- El tipo de copias de objeto realizadas. Las copias se pueden replicar o codificar.
- Para las copias replicadas, el número de copias realizadas.
- Para las copias codificadas de borrado, se utiliza el esquema de codificación de borrado.
- Los cambios a lo largo del tiempo en la ubicación de almacenamiento de un objeto y el tipo de copias.
- Cómo se protegen los datos de objetos cuando se ingieren los objetos en el grid (ubicación síncrona o doble registro).

Tenga en cuenta que los metadatos de objetos no están gestionados por las reglas de ILM. En su lugar, los metadatos de objetos se almacenan en una base de datos de Cassandra en lo que se conoce como almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de objetos en cada sitio para proteger los datos frente a pérdidas. Las copias se distribuyen uniformemente por todos los nodos de almacenamiento.

Elementos de una regla de ILM

Una regla de ILM consta de tres elementos:

- **Criterios de filtrado**: Los filtros básicos y avanzados de una regla definen a qué objetos se aplica la regla. Si un objeto coincide con todos los filtros, StorageGRID aplica la regla y crea las copias de objeto especificadas en las instrucciones de colocación de la regla.

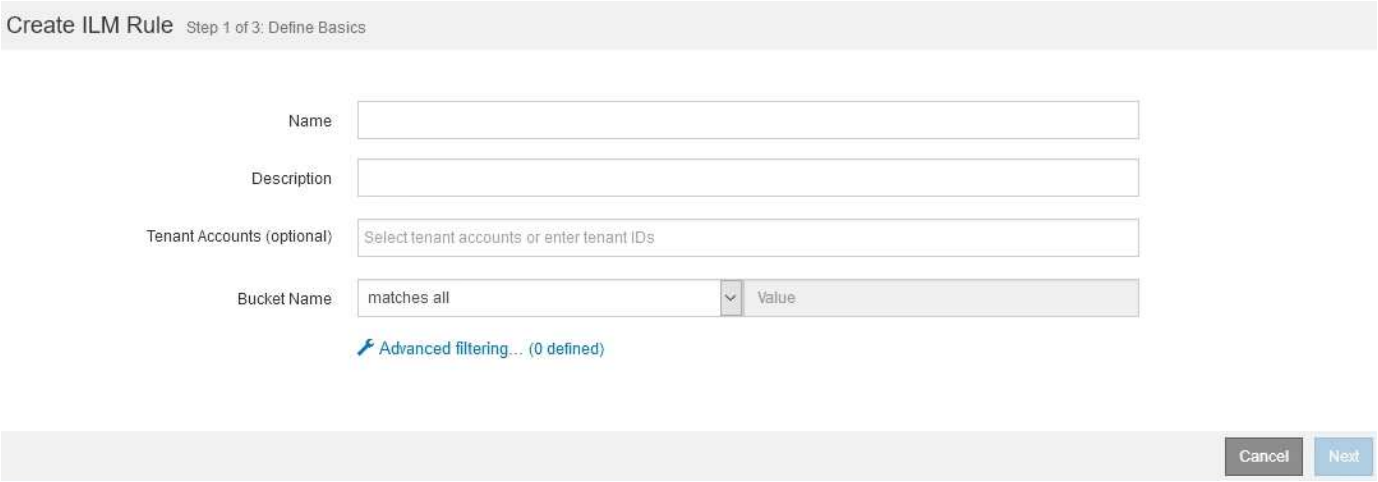
- **Instrucciones de colocación**: Las instrucciones de colocación de una regla definen el número, el tipo y la ubicación de las copias de objetos. Cada regla puede incluir una secuencia de instrucciones de colocación para cambiar el número, el tipo y la ubicación de las copias de objetos a lo largo del tiempo. Cuando expira el período de tiempo para una ubicación, la siguiente evaluación de ILM aplica automáticamente las instrucciones en la siguiente ubicación.
- **Comportamiento de procesamiento**: El comportamiento de procesamiento de una regla define lo que ocurre cuando un cliente S3 o Swift guarda un objeto en la cuadrícula. El comportamiento de la ingesta controla si las copias de objetos se colocan inmediatamente según las instrucciones de la regla o si se realizan copias provisionales y se aplican las instrucciones de colocación más adelante.

Qué es el filtrado de reglas de ILM

Al crear una regla de ILM, puede especificar filtros para identificar a qué objetos se aplica la regla.

En el caso más sencillo, 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) de una política de ILM. La regla predeterminada proporciona instrucciones de almacenamiento para los objetos que no coinciden con los filtros de otra regla.

Los filtros básicos permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Los filtros básicos de la página define Basics del asistente Create ILM Rule le permiten aplicar una regla a cuentas de inquilino específicas, bloques S3 específicos, contenedores Swift, o ambos.



Estos filtros básicos le proporcionan una forma sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que los registros financieros de su empresa deban almacenarse para cumplir con requisitos normativos; en cambio, los datos del departamento de marketing pueden necesitar almacenarse para facilitar las operaciones diarias. Tras crear cuentas de inquilino independientes para cada departamento o al separar los datos de los diferentes departamentos en bloques S3 independientes, puede crear fácilmente una regla que se aplique a todos los registros financieros y a una segunda regla que se aplique a todos los datos de marketing.

La página **filtrado avanzado** del asistente Crear regla ILM le ofrece control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades de objeto:

- Tiempo de ingesta
- Hora del último acceso
- Todo o parte del nombre del objeto (clave)
- Región de bloques de S3 (limitación de ubicación)

- Tamaño del objeto
- Metadatos del usuario
- Etiquetas de objetos de 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 de antigüedad y no suelen hacerlo después, mientras que los objetos que contienen información de visita del paciente pueden necesitar copiarse al departamento de facturación de la sede de la red sanitaria. Puede crear filtros que identifiquen cada tipo de objeto en función del nombre del objeto, el tamaño, las etiquetas de objetos de S3 o cualquier otro criterio relevante para, a continuación, crear reglas independientes para almacenar cada conjunto de objetos de la forma adecuada.

También puede combinar filtros básicos y avanzados según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imagen de gran tamaño de forma diferente a sus registros de proveedor, mientras que el departamento de recursos humanos podría necesitar almacenar registros de personal en una región específica e información de políticas de forma centralizada. En este caso, se pueden crear reglas que filtran por cuenta de arrendatario para separar los registros de cada departamento, al mismo tiempo que se utilizan filtros avanzados en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

¿Qué son las instrucciones de colocación de reglas de ILM

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

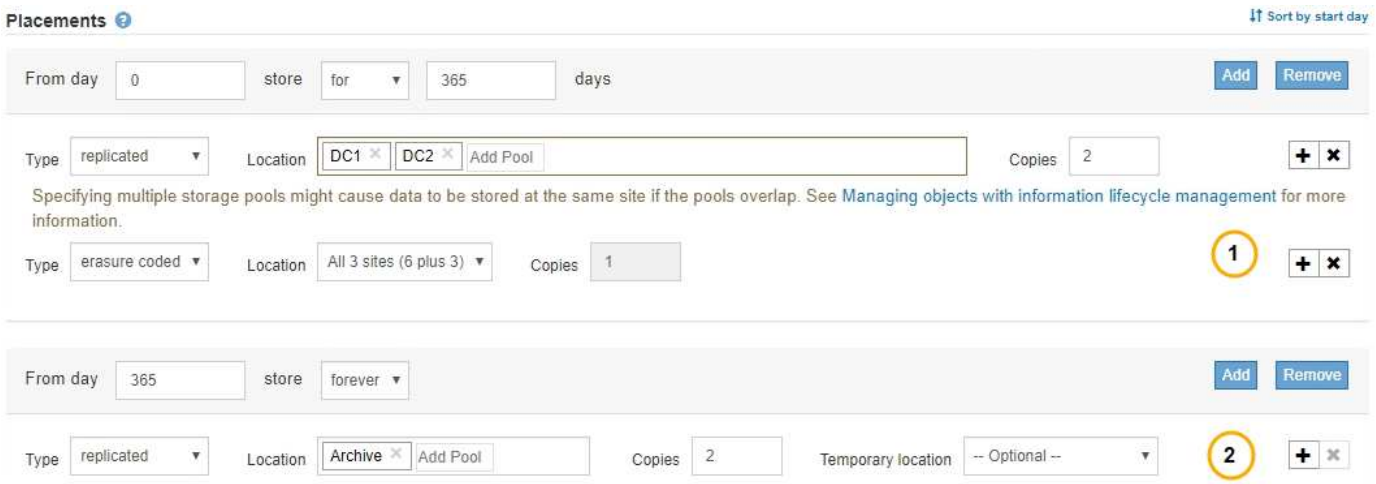
Al crear instrucciones de colocación:

- Para empezar, especifique el tiempo de referencia, que determina cuándo se inician las instrucciones de colocación. El tiempo de referencia podría ser el momento en que un objeto se ingiere, cuando se accede a un objeto, cuando un objeto con versiones se convierte en no actual o en un tiempo definido por el usuario.
- A continuación, especifique cuándo se aplicará la ubicación en relación con el tiempo de referencia. Por ejemplo, una ubicación podría comenzar en el día 0 y continuar durante 365 días, en relación con el momento en que se ingirió el objeto.
- Por último, debe especificar el tipo de copias (codificación de replicación o borrado) y la ubicación donde se almacenan las copias. Por ejemplo, puede que desee almacenar dos copias replicadas en dos sitios diferentes.

Cada regla puede definir varias ubicaciones para un único período de tiempo y ubicaciones diferentes para diferentes períodos de tiempo.

- Para colocar objetos en varias ubicaciones durante un único período de tiempo, seleccione el icono de signo más ➕ para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione el botón **Agregar** para agregar el siguiente período de tiempo. A continuación, especifique una o más líneas dentro del período de tiempo.

El ejemplo muestra la página define colocaciones del asistente Create ILM Rule.



1	La primera instrucción de colocación tiene dos líneas para el primer año: 1. La primera línea crea dos copias de objetos replicadas en dos sitios de centro de datos. 2. La segunda línea crea una copia con código de borrado de 6+3 utilizando tres centros de datos.
2	La segunda instrucción de colocación crea dos copias archivadas después de un año y mantiene esas copias para siempre.

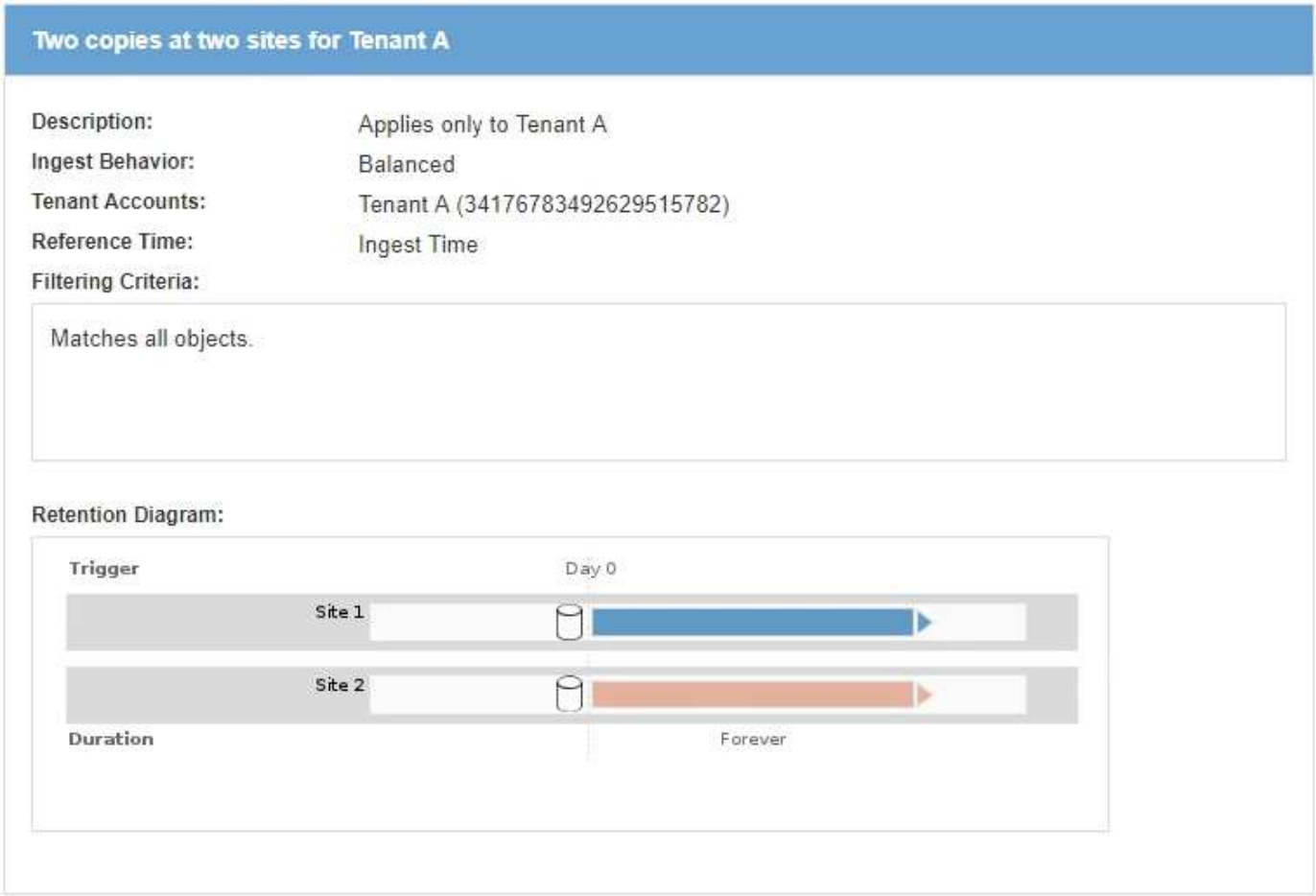
Cuando defina el conjunto de instrucciones de colocación para una regla, debe asegurarse de que al menos una instrucción de colocación comienza en el día 0, de que no haya espacios entre los períodos de tiempo definidos. y que la instrucción de colocación final continúa para siempre o hasta que ya no se requiere ninguna copia de objeto.

Cuando cada período de tiempo de la regla caduca, se aplican las instrucciones de colocación del contenido para el próximo período de tiempo. Se crean nuevas copias de objetos y se eliminan todas las copias innecesarias.

Regla de ILM de ejemplo

Esta regla de ILM de ejemplo se aplica a los objetos que pertenecen al inquilino A. Realiza dos copias replicadas de esos objetos y almacena cada copia en un sitio diferente. Las dos copias se conservan «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que se eliminen mediante una solicitud de eliminación del cliente o cuando finalice el ciclo de vida de un bloque.

Esta regla utiliza la opción equilibrada para el comportamiento de procesamiento: La instrucción de colocación de dos sitios se aplica tan pronto como el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar de inmediato ambas copias necesarias. Por ejemplo, si el sitio 2 no se puede acceder cuando el inquilino A guarda un objeto, StorageGRID realizará dos copias provisionales en los nodos de almacenamiento del sitio 1. En cuanto el sitio 2 esté disponible, StorageGRID realizará la copia necesaria en ese sitio.



Información relacionada

- Opciones de protección de datos para consumo
- Qué es un pool de almacenamiento
- Qué es un pool de almacenamiento cloud

Crear grados de almacenamiento, pools de almacenamiento, perfiles de EC y regiones

Crear y asignar grados de almacenamiento

Los grados de almacenamiento identifican el tipo de almacenamiento que utiliza un nodo de almacenamiento. Puede crear grados de almacenamiento si desea que las reglas de ILM colocan ciertos objetos en ciertos nodos de almacenamiento, en lugar de en todos los nodos del sitio. Por ejemplo, quizás desee almacenar determinados objetos en los nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash StorageGRID.

Lo que necesitará

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

Acerca de esta tarea

Si utiliza más de un tipo de almacenamiento, puede crear, opcionalmente, un nivel de almacenamiento para identificar cada tipo. La creación de grados de almacenamiento permite seleccionar un tipo específico de nodo de almacenamiento al configurar pools de almacenamiento.

Si el grado de almacenamiento no es un problema (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y utilizar el grado de almacenamiento predeterminado todos los nodos al configurar pools de almacenamiento.

Cuando se añade un nuevo nodo de almacenamiento en una ampliación, dicho nodo se añade al nivel de almacenamiento predeterminado de todos los nodos de almacenamiento. Como resultado:

- Si una regla de ILM utiliza un pool de almacenamiento con el nivel All Storage Nodes, se puede usar el nodo nuevo inmediatamente después de que finalice la ampliación.
- Si una regla de ILM usa un pool de almacenamiento con un grado de almacenamiento personalizado, no se usará el nuevo nodo hasta que se asigne manualmente el grado de almacenamiento personalizado al nodo, como se describe a continuación.

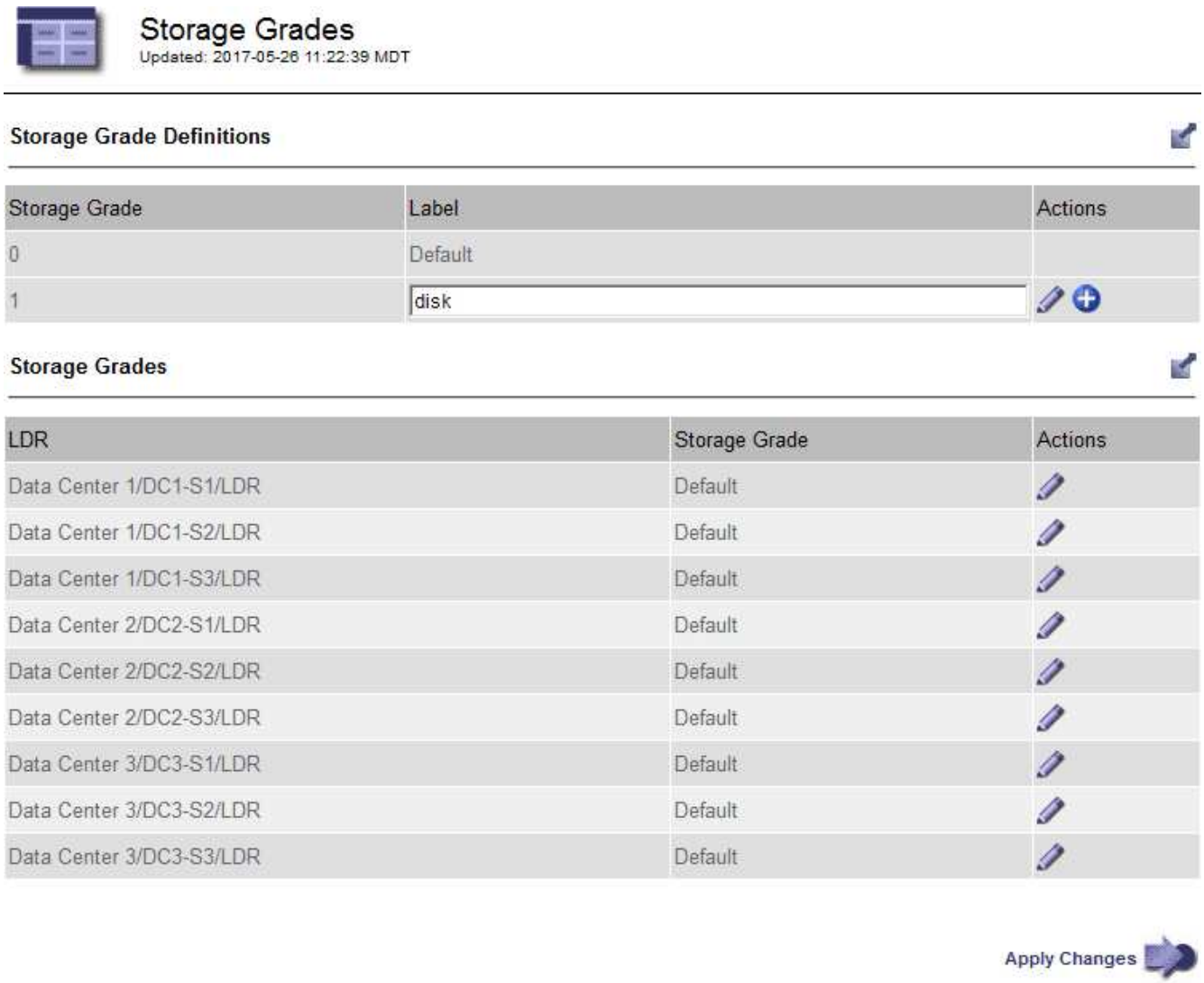
> Al crear grados de almacenamiento, no cree más grados de almacenamiento del necesario. Por ejemplo, no cree un grado de almacenamiento para cada nodo de almacenamiento. En su lugar, asigne cada grado de almacenamiento a dos o más nodos. Las leyes de almacenamiento asignadas a un solo nodo pueden provocar reversiones de ILM si ese nodo deja de estar disponible.

Pasos

1. Seleccione **ILM** > **grados de almacenamiento**.
2. Crear un grado de almacenamiento:

   a. Para cada grado de almacenamiento que necesita definir, seleccione **Insertar** para agregar una fila e introducir una etiqueta para el grado de almacenamiento.

      El grado de almacenamiento predeterminado no se puede modificar. Se reserva para los nuevos nodos de almacenamiento añadidos durante una ampliación del sistema StorageGRID.



a. Para editar un grado de almacenamiento existente, seleccione **Editar** y modifique la etiqueta según sea necesario.

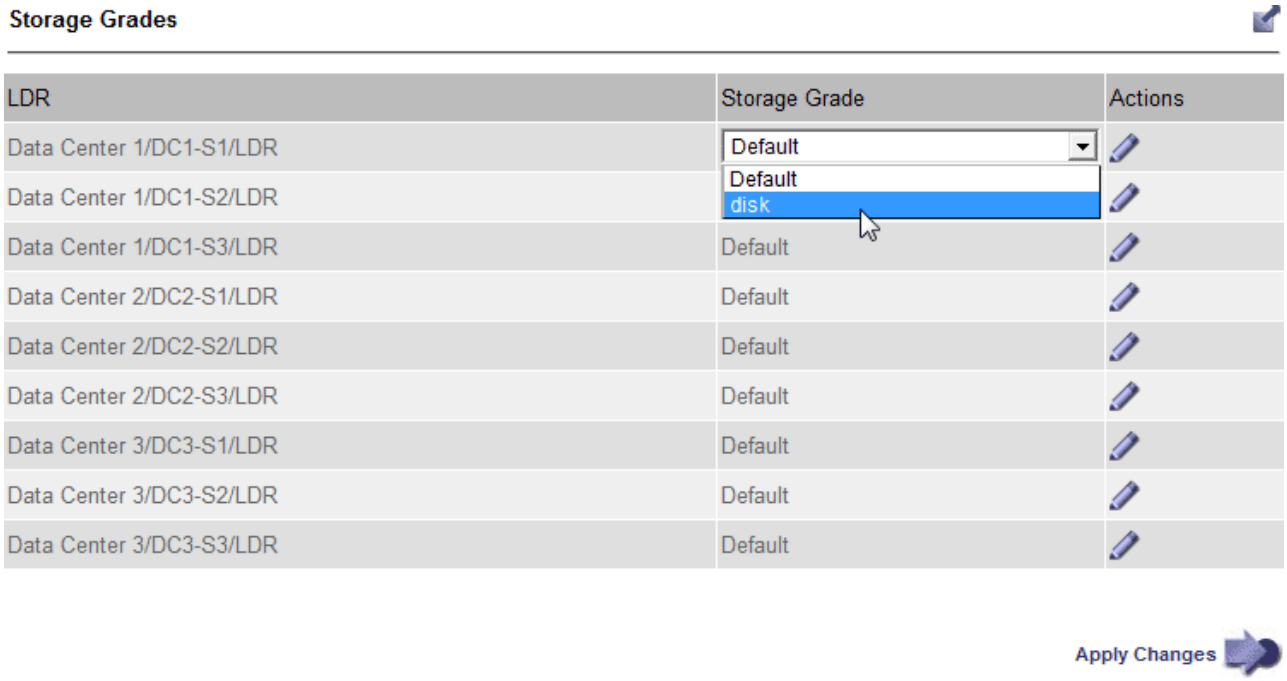
> No es posible eliminar grados de almacenamiento.

b. Seleccione **aplicar cambios**.

   Estas clases de almacenamiento ahora están disponibles para su asignación a nodos de almacenamiento.

3. Asigne un grado de almacenamiento a un nodo de almacenamiento:

   a. Para cada servicio LDR del nodo de almacenamiento, seleccione **Editar** y seleccione un grado de almacenamiento de la lista.



> Asigne un nivel de almacenamiento solo una vez a un nodo de almacenamiento determinado. Un nodo de almacenamiento recuperado del error mantiene el grado de almacenamiento anteriormente asignado. No cambie esta asignación después de activar la política de ILM. Si se modifica la asignación, los datos se almacenan según el nuevo grado de almacenamiento.

a. Seleccione **aplicar cambios**.

Configurar los pools de almacenamiento

Qué es un pool de almacenamiento

Un pool de almacenamiento es una agrupación lógica de nodos de almacenamiento o nodos de archivado. Los pools de almacenamiento se configuran para determinar dónde el sistema StorageGRID almacena los datos de objetos y el tipo de almacenamiento utilizado.

Los pools de almacenamiento tienen dos atributos:

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

Las reglas de ILM permiten utilizar los pools de almacenamiento para determinar dónde se almacenan los datos de objetos. Cuando se configuran las reglas de ILM para la replicación, se deben seleccionar uno o varios pools de almacenamiento que incluyen nodos de almacenamiento o nodos de archivado. Cuando se crean perfiles de código de borrado, se selecciona un pool de almacenamiento que incluye nodos de almacenamiento.

Directrices para crear pools de almacenamiento

Al configurar y usar pools de almacenamiento, siga estas directrices.

Directrices para todos los pools de almacenamiento

- StorageGRID incluye un pool de almacenamiento predeterminado, todos los nodos de almacenamiento, que utiliza el sitio predeterminado, todos los sitios y el nivel de almacenamiento predeterminado, todos los nodos de almacenamiento. El pool de almacenamiento de todos los nodos de almacenamiento se actualiza automáticamente cada vez que se añaden nuevos sitios de centro de datos.

> No se recomienda utilizar el grupo de almacenamiento todos los nodos de almacenamiento o el sitio todos los sitios porque estos elementos se actualizan automáticamente para incluir los sitios nuevos que agregue en una expansión, lo que podría no ser el comportamiento que desea. Antes de usar el pool de almacenamiento todos los nodos de almacenamiento o el sitio predeterminado, revise con cuidado las directrices para las copias replicadas y codificadas de borrado.

- Mantenga las configuraciones del pool de almacenamiento de la forma más sencilla posible. No cree más pools de almacenamiento de los necesarios.
- Cree pools de almacenamiento con tantos nodos como sea posible. Cada pool de almacenamiento debe contener dos o más nodos. Un pool de almacenamiento con nodos insuficientes puede provocar registros de gestión del ciclo de vida de la información si un nodo deja de estar disponible.
- Evite crear o usar pools de almacenamiento que se solapen (contienen uno o varios de los mismos nodos). Si los pools de almacenamiento se solapan, es posible que se guarden más de una copia de datos de objetos en el mismo nodo.

Directrices para los pools de almacenamiento utilizados para copias replicadas

- Cree una agrupación de almacenamiento diferente para cada sitio. A continuación, especifique uno o varios grupos de almacenamiento específicos del sitio en las instrucciones de colocación de cada regla. El uso de un pool de almacenamiento para cada sitio garantiza que las copias de objetos replicados se coloquen exactamente donde se espere (por ejemplo, una copia de cada objeto en cada sitio para la protección frente a pérdida de sitio).
- Si agrega un sitio en una expansión, cree un nuevo grupo de almacenamiento para el sitio nuevo. A continuación, actualice las reglas de ILM para controlar qué objetos están almacenados en el nuevo sitio.
- En general, no utilice el pool de almacenamiento predeterminado, todos los nodos de almacenamiento ni ningún pool de almacenamiento que incluya el sitio predeterminado, todos los sitios.

Directrices para los pools de almacenamiento utilizados para las copias con código de borrado

- No se pueden usar nodos de archivado para los datos codificados mediante borrado.
- El número de nodos de almacenamiento y sitios que contiene el pool de almacenamiento determina qué esquemas de codificación de borrado están disponibles.
- Si un pool de almacenamiento incluye solo dos sitios, no podrá utilizar dicho pool de almacenamiento para codificar el borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.
- En general, no utilice el pool de almacenamiento predeterminado, todos los nodos de almacenamiento ni ningún pool de almacenamiento que incluya el sitio predeterminado, todos los sitios en ningún perfil de código de borrado.

> Si el grid incluye un solo sitio, no se podrá utilizar el pool de almacenamiento todos los nodos de almacenamiento ni el sitio predeterminado todos los sitios en un perfil de código de borrado. Este comportamiento impide que el perfil de código de borrado no sea válido si se agrega un segundo sitio.

- Si tiene requisitos de alto rendimiento, no se recomienda crear un pool de almacenamiento que incluya varios sitios si la latencia de red entre los 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 considerablemente debido al descenso del rendimiento de la red TCP. La disminución del rendimiento afecta a las tasas máximas que se pueden lograr para la ingesta y la recuperación de objetos (cuando se seleccionan valores estrictos o equilibrados como comportamiento de procesamiento) o que podrían provocar retrasos en la cola de ILM (cuando se selecciona el Dual Commit como comportamiento de procesamiento).
- Si es posible, un pool de almacenamiento debe incluir más de 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 contar con al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuya nodos de almacenamiento en todos los sitios de la forma más equitativa posible. Por ejemplo, para admitir un esquema de codificación de borrado 6+3, configure un pool de almacenamiento que incluya al menos tres nodos de almacenamiento en tres sitios.

Directrices para los pools de almacenamiento utilizados para copias archivadas

- No es posible crear un pool de almacenamiento que incluya nodos de almacenamiento y Archivo. Las copias archivadas requieren un pool de almacenamiento que sólo incluya nodos de archivado.
- Cuando se utiliza un pool de almacenamiento que incluye nodos de archivado, también se debe mantener al menos una copia replicada o con código de borrado en un pool de almacenamiento que incluya nodos de almacenamiento.
- Si la configuración global de bloqueo de objetos de S3 está habilitada y se crea una regla de ILM compatible, no se puede usar un pool de almacenamiento que incluya los nodos de archivado. Consulte las instrucciones para gestionar objetos con el bloqueo de objetos de S3.
- Si el tipo de destino de un nodo de archivado es Cloud Tiering - simple Storage Service (S3), el nodo de archivado debe estar en su propio pool de almacenamiento. Consulte Administre StorageGRID.

Información relacionada

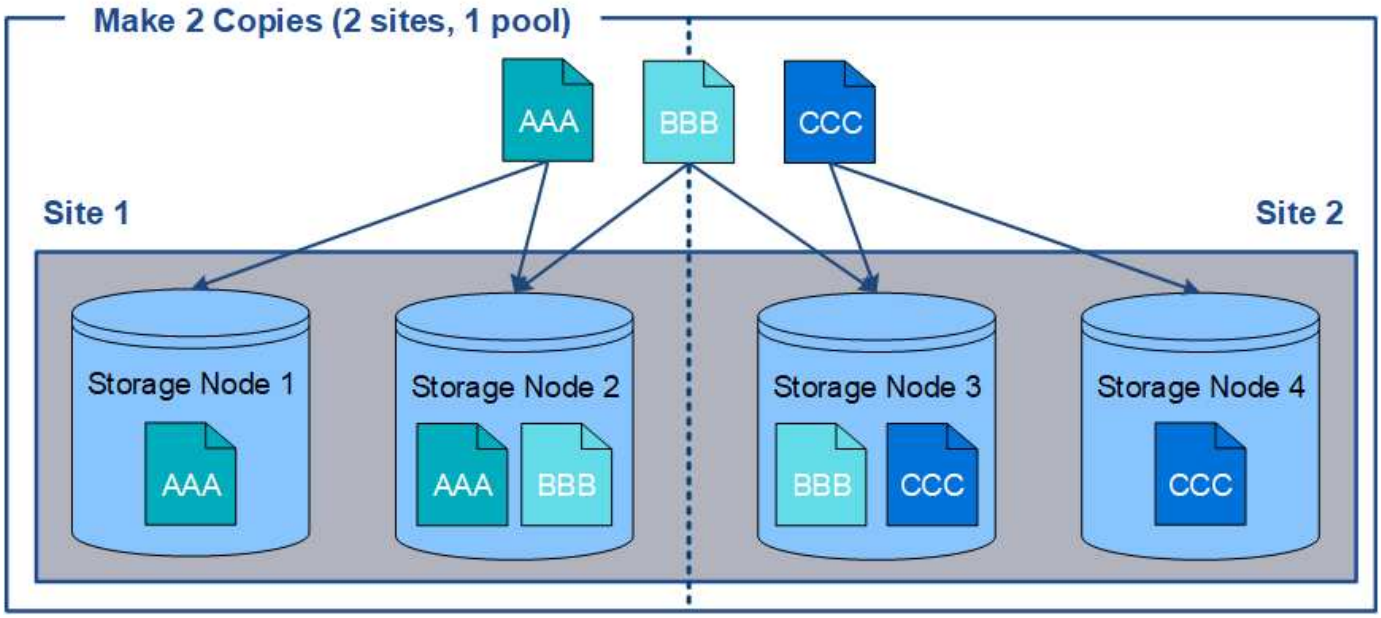
- Qué es la replicación
- Qué es la codificación de borrado
- Qué son los esquemas de codificación de borrado
- Utilice varios pools de almacenamiento para la replicación entre sitios

Utilice varios pools de almacenamiento para la replicación entre sitios

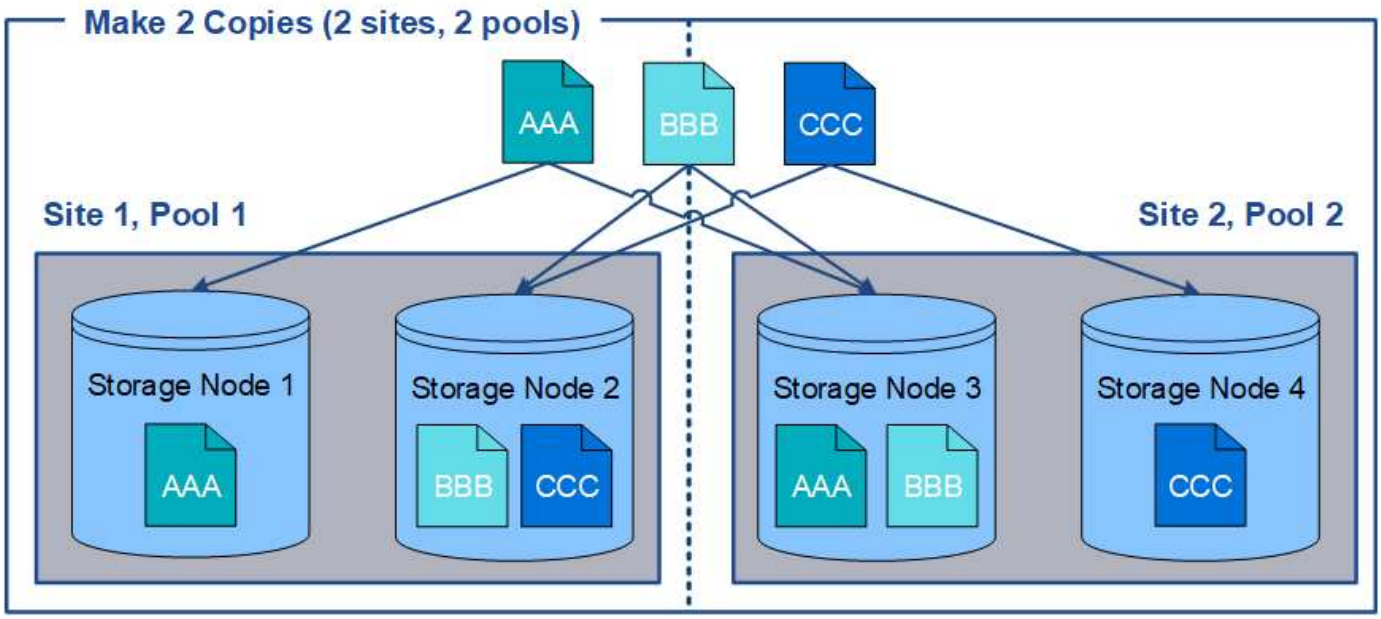
Si la implementación de StorageGRID incluye más de un sitio, puede habilitar la protección contra pérdida de sitio mediante la creación de un pool de almacenamiento para cada sitio y especificar ambos pools de almacenamiento en las instrucciones de ubicación de la regla. Por ejemplo, si configura una regla de ILM para realizar dos copias replicadas y especificar pools de almacenamiento en dos sitios, se colocará una copia de cada objeto en cada sitio. Si configura una regla para realizar dos copias y especifica

tres pools de almacenamiento, las copias se distribuyen para equilibrar el uso de disco entre los pools de almacenamiento, a la vez que se asegura de que las dos copias se almacenan en sitios diferentes.

El siguiente ejemplo ilustra qué puede suceder si una regla de ILM coloca copias de objetos replicadas en un único pool de almacenamiento que contiene nodos de almacenamiento de dos sitios. Como el sistema utiliza todos los nodos disponibles en el pool de almacenamiento cuando coloca las copias replicadas, es posible que se mantengan todas las copias de algunos objetos en solo uno de los sitios. En este ejemplo, el sistema almacenaba dos copias del objeto AAA en los nodos de almacenamiento del sitio 1 y dos copias del objeto CCC en los nodos de almacenamiento del sitio 2. Sólo se protege el objeto BBB si uno de los sitios falla o se vuelve inaccesible.



En cambio, este ejemplo muestra cómo se almacenan los objetos cuando se utilizan varios pools de almacenamiento. En el ejemplo, la regla de ILM especifica que se creen dos copias replicadas de cada objeto y que las copias se distribuyen en dos pools de almacenamiento. Cada pool de almacenamiento contiene todos los nodos de almacenamiento en un sitio. Debido a que una copia de cada objeto se almacena en cada sitio, los datos de objeto están protegidos de un fallo del sitio o falta de accesibilidad.



Al usar varios pools de almacenamiento, tenga en cuenta las siguientes reglas:

- Si crea n copias, debe añadir n o más pools de almacenamiento. Por ejemplo, si una regla está configurada para realizar tres copias, debe especificar tres o más pools de almacenamiento.
- Si el número de copias es igual al número de pools de almacenamiento, se almacena una copia del objeto en cada pool de almacenamiento.
- Si el número de copias es menor que el número de pools de almacenamiento, el sistema distribuye las copias para mantener el uso del disco entre los pools equilibrados y para garantizar que no se almacenen dos o más copias en la misma agrupación de almacenamiento.
- Si los pools de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden en un solo sitio. Debe asegurarse de que los pools de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Usar un pool de almacenamiento como ubicación temporal (obsoleto)

Cuando crea una regla de ILM con una ubicación de objetos que incluya un solo pool de almacenamiento, se le solicita que especifique un segundo pool de almacenamiento que se usará como ubicación temporal.

Las ubicaciones temporales han quedado obsoletas y se eliminarán en un lanzamiento futuro. No debe seleccionar un pool de almacenamiento como ubicación temporal para una nueva regla de ILM.

> Si selecciona el comportamiento de procesamiento estricto (paso 3 del asistente Crear regla de ILM), se omitirá la ubicación temporal.

Información relacionada

Opciones de protección de datos para consumo

Cree un pool de almacenamiento

Se crean pools de almacenamiento para determinar dónde el sistema StorageGRID almacena los datos de objetos y el tipo de almacenamiento utilizado. Cada pool de

almacenamiento incluye uno o más sitios y una o más calidades de almacenamiento.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Revisó las directrices para crear pools de almacenamiento.

Acerca de esta tarea

Los pools de almacenamiento determinan dónde se almacenan los datos de objeto. La cantidad de pools de almacenamiento que necesita depende del número de sitios del grid y de los tipos de copias que desee: Replicadas o codificadas por borrado.

- Para la replicación y la codificación de borrado a un solo sitio, cree un pool de almacenamiento para cada sitio. Por ejemplo, si desea almacenar copias de objetos replicados en tres sitios, cree tres pools de almacenamiento.
- Para la codificación de borrado en tres o más sitios, cree un pool de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si desea borrar objetos de código en tres sitios, cree un pool de almacenamiento. Seleccione el icono más ➕ para agregar una entrada para cada sitio.

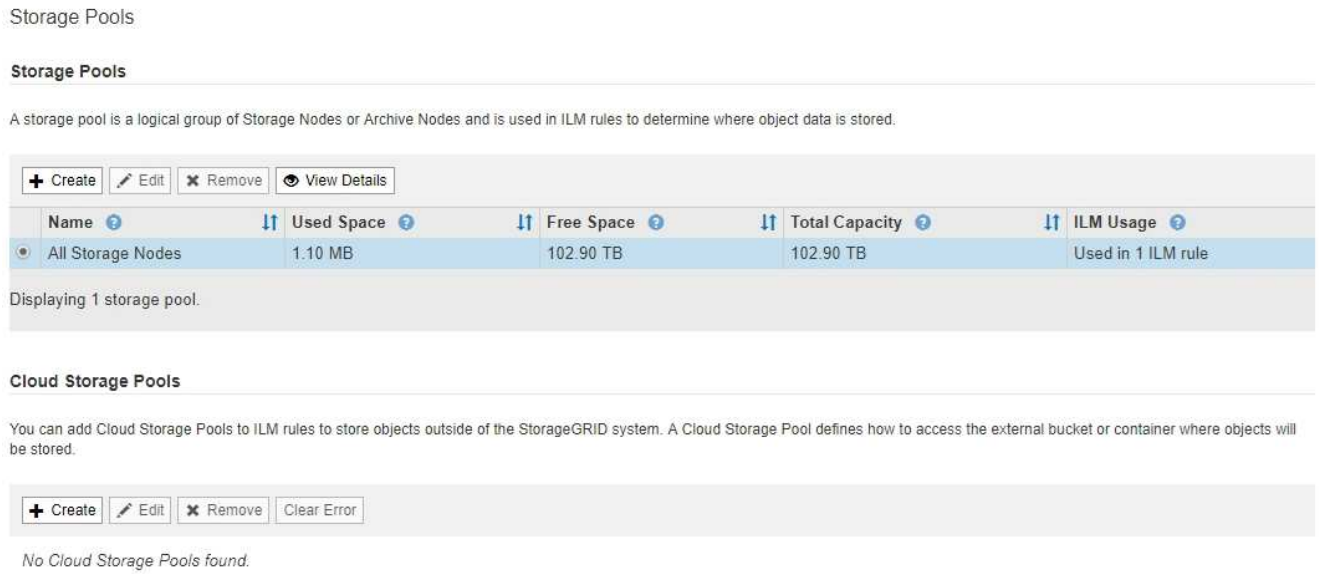
> No incluya el sitio predeterminado All Sites en un pool de almacenamiento que se utilizará en un perfil de código de borrado. En su lugar, añada una entrada independiente al pool de almacenamiento para cada instalación que almacenará los datos codificados de borrado. Consulte este paso por ejemplo.

- Si usted tiene más de un grado de almacenamiento, no cree un pool de almacenamiento que incluya diferentes grados de almacenamiento en un solo sitio. Consulte Directrices para crear pools de almacenamiento.

Pasos

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

   Se muestra la página Storage Pools, con una lista de todos los pools de almacenamiento definidos.



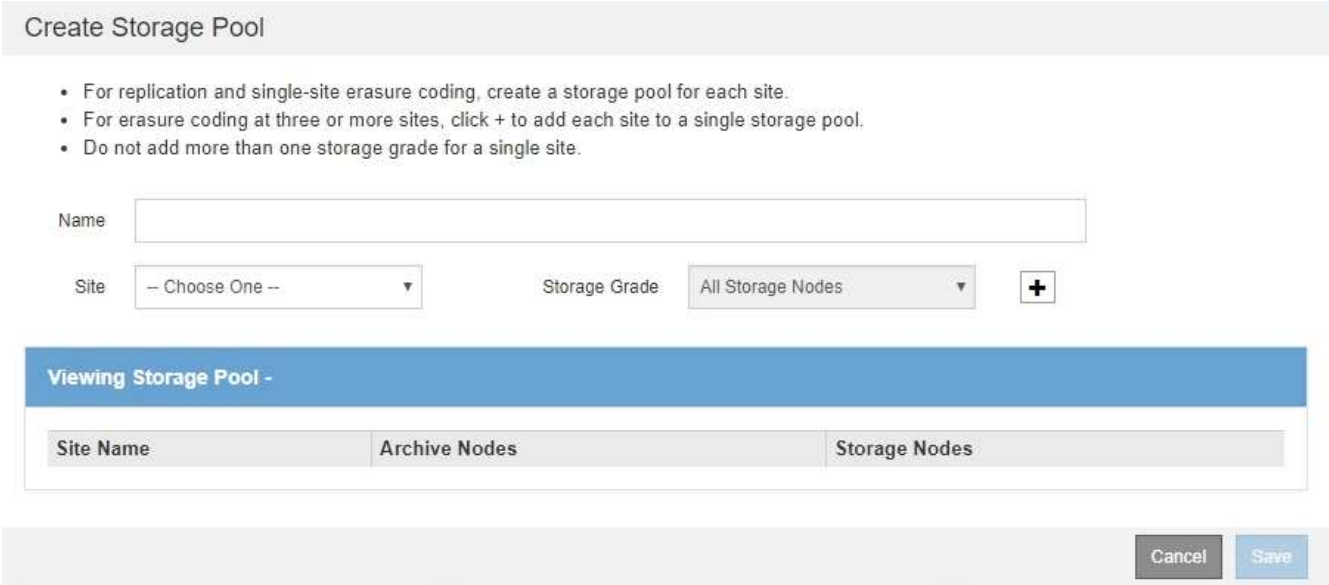
   La lista incluye el pool de almacenamiento predeterminado del sistema, todos los nodos de

almacenamiento, que utiliza el sitio predeterminado del sistema, todos los sitios y el grado de almacenamiento predeterminado, todos los nodos de almacenamiento.

> Dado que el pool de almacenamiento todos los nodos de almacenamiento se actualiza automáticamente cada vez que se agregan nuevos sitios de centros de datos, no se recomienda utilizar este pool de almacenamiento en las reglas de ILM.

2. Para crear una nueva agrupación de almacenamiento, seleccione **Crear**.

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



3. Introduzca un nombre único para el pool de almacenamiento.

   Utilice un nombre que será fácil de identificar cuando configure perfiles de código de borrado y reglas de ILM.

4. En la lista desplegable **Sitio**, seleccione un sitio para esta agrupación de almacenamiento.

   Cuando selecciona un sitio, el número de nodos de almacenamiento y nodos de archivado de la tabla se actualiza automáticamente.

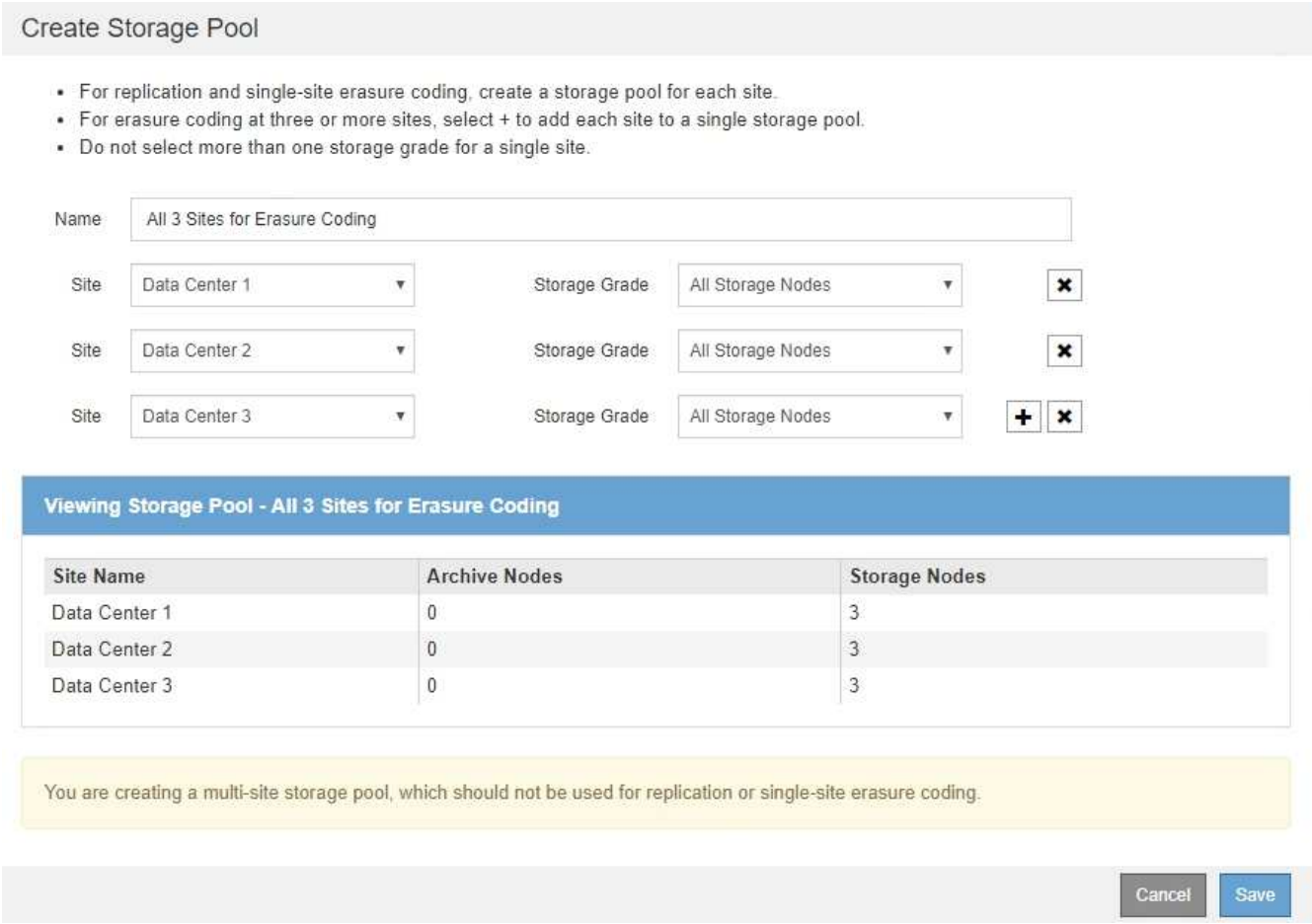
   En general, no utilice el sitio predeterminado All Sites de ningún grupo de almacenamiento. Las reglas de ILM que utilizan un pool de almacenamiento All Sites colocan los objetos en cualquier sitio disponible, lo que le otorga menos control de la ubicación de los objetos. Además, un pool de almacenamiento All Sites utiliza inmediatamente los nodos de almacenamiento en un sitio nuevo, 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 de ILM utiliza esta agrupación de almacenamiento.

   El nivel de almacenamiento predeterminado para todos los nodos de almacenamiento incluye todos los nodos de almacenamiento en el sitio seleccionado. El nivel de almacenamiento predeterminado de los nodos de archivado incluye todos los nodos de archivado en el sitio seleccionado. Si creó grados de almacenamiento adicionales para los nodos de almacenamiento del grid, estos se enumeran en el menú desplegable.

6. Si desea utilizar el pool de almacenamiento en un perfil de codificación de borrado de varios sitios,

seleccione ➕ para agregar una entrada para cada sitio al grupo de almacenamiento.



> Se le impide crear entradas duplicadas o crear una agrupación de almacenamiento que incluya el grado de almacenamiento **nodos de archivo** y cualquier grado de almacenamiento que contenga nodos de almacenamiento.
>
> Usted es advertido si usted agrega más de una entrada para un sitio pero con diferentes grados de almacenamiento.

Para eliminar una entrada, seleccione ✖.

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

   El nuevo pool de almacenamiento se añadirá a la lista.

Ver detalles del pool de almacenamiento

Es posible ver los detalles de un pool de almacenamiento para determinar dónde se usa el pool de almacenamiento y para ver qué nodos y calidades de almacenamiento se incluyen.

Lo que necesitará

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

Pasos

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

   Aparece la página Storage Pools. Esta página enumera todos los pools de almacenamiento definidos.

   Storage Pools

   Storage Pools

   A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

   + Create | Edit | ✖ Remove | View Details

	Name	Used Space	Free Space	Total Capacity	ILM Usage
◉	All Storage Nodes	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule
○	DC1	621.77 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
○	DC2	675.82 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
○	DC3	578.95 KB	932.42 GB	932.42 GB	Used in 1 ILM rule
○	All 3 Sites	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule and 1 EC profile
○	Archive	—	—	—	—

   Displaying 6 storage pools.

   Cloud Storage Pools

   You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

   + Create | Edit | ✖ Remove | Clear Error

   No Cloud Storage Pools found.

   En la tabla se incluye la siguiente información para cada pool de almacenamiento que incluye los nodos de almacenamiento:

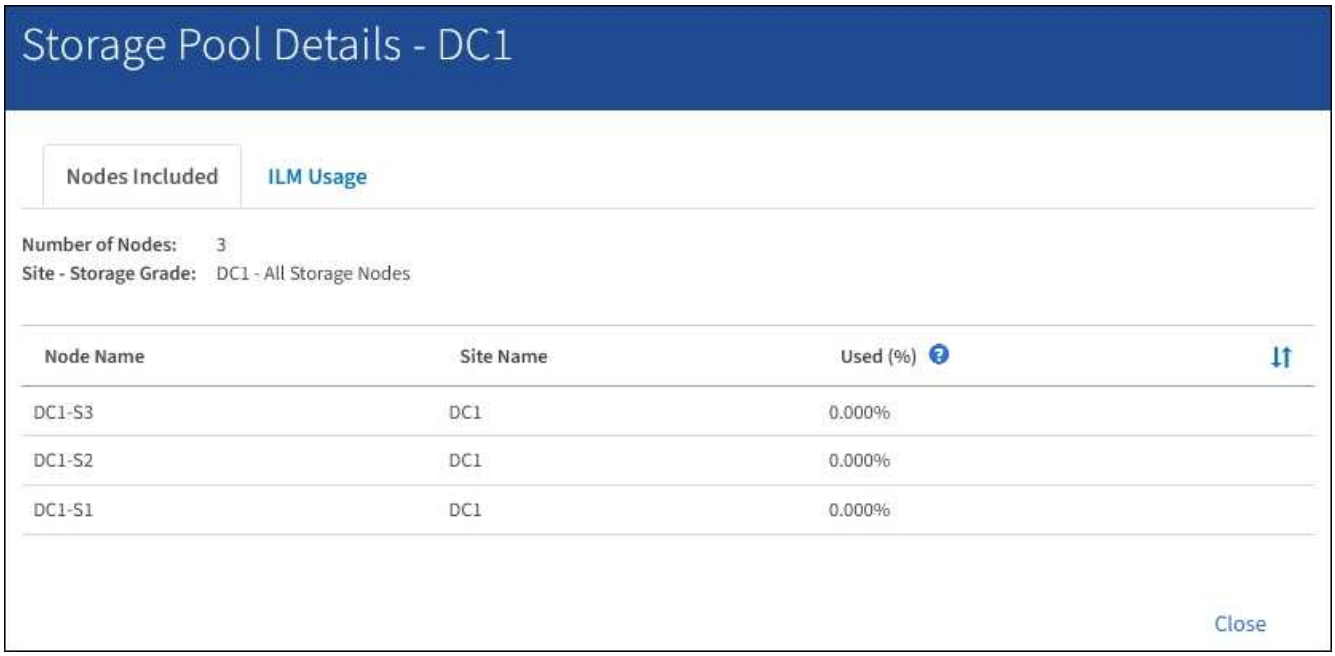
   - **Nombre**: El nombre exclusivo para mostrar de la agrupación de almacenamiento.
   - **Espacio usado**: Cantidad de espacio que se está utilizando actualmente para almacenar objetos en la agrupación de almacenamiento.
   - **Espacio libre**: La cantidad de espacio que queda disponible para almacenar objetos en la agrupación de almacenamiento.
   - **Capacidad total**: El tamaño de la agrupación de almacenamiento, que equivale a la cantidad total de espacio útil para los datos de los objetos de todos los nodos de la agrupación de almacenamiento .
   - **Uso de ILM**: Cómo se utiliza actualmente el pool de almacenamiento. Un pool de almacenamiento puede no utilizarse o utilizarse en una o varias reglas de ILM, perfiles de código de borrado o ambos.

     No se puede quitar un pool de almacenamiento si se está utilizando.

2. Para ver los detalles de una agrupación de almacenamiento específica, seleccione su botón de opción y seleccione **Ver detalles**.

   Aparecerá el mensaje Detalles del grupo de almacenamiento modal.

3. Consulte la ficha **nodos incluidos** para obtener información sobre los nodos de almacenamiento o los nodos de archivo incluidos en la agrupación de almacenamiento.



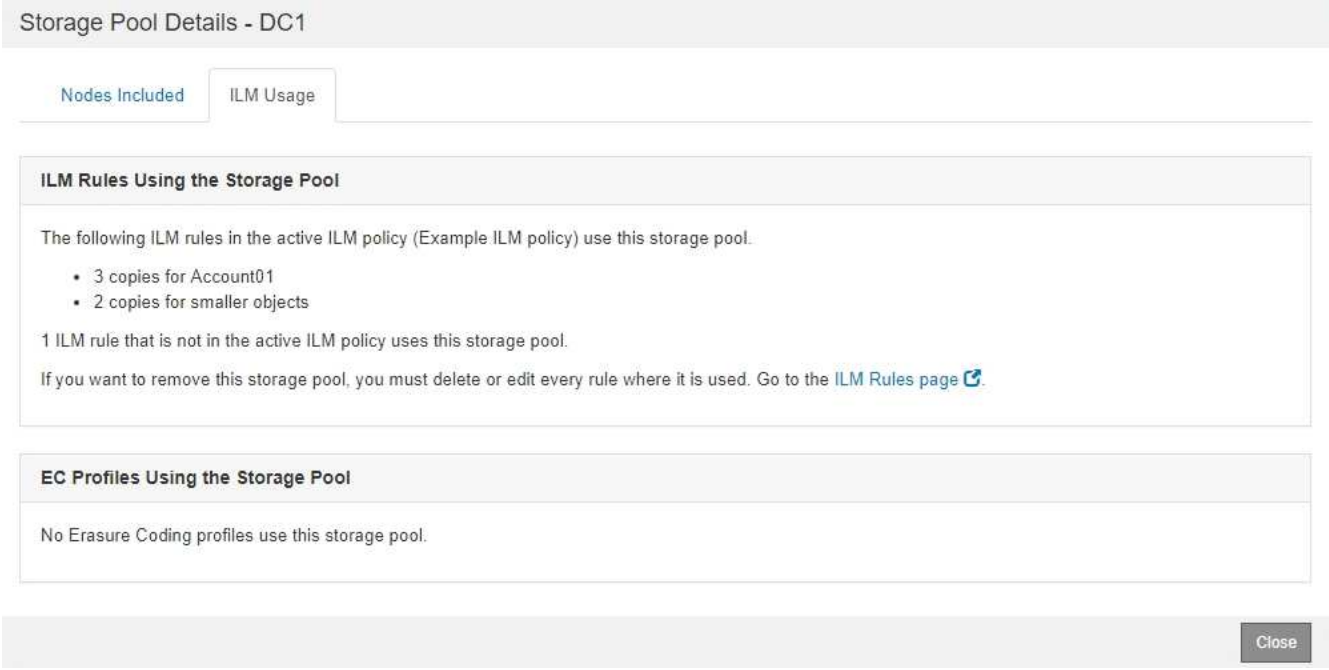
En la tabla se incluye la siguiente información para cada nodo:

- Nombre del nodo
- Nombre del sitio
- Usado (%): Para los nodos de almacenamiento, el porcentaje del espacio útil total para los datos de objeto que se han usado. Este valor no incluye metadatos de objetos.

> El mismo valor usado (%) también se muestra en el gráfico almacenamiento usado - datos de objeto para cada nodo de almacenamiento (seleccione **NODOS** > ***nodo de almacenamiento*** > **almacenamiento**).

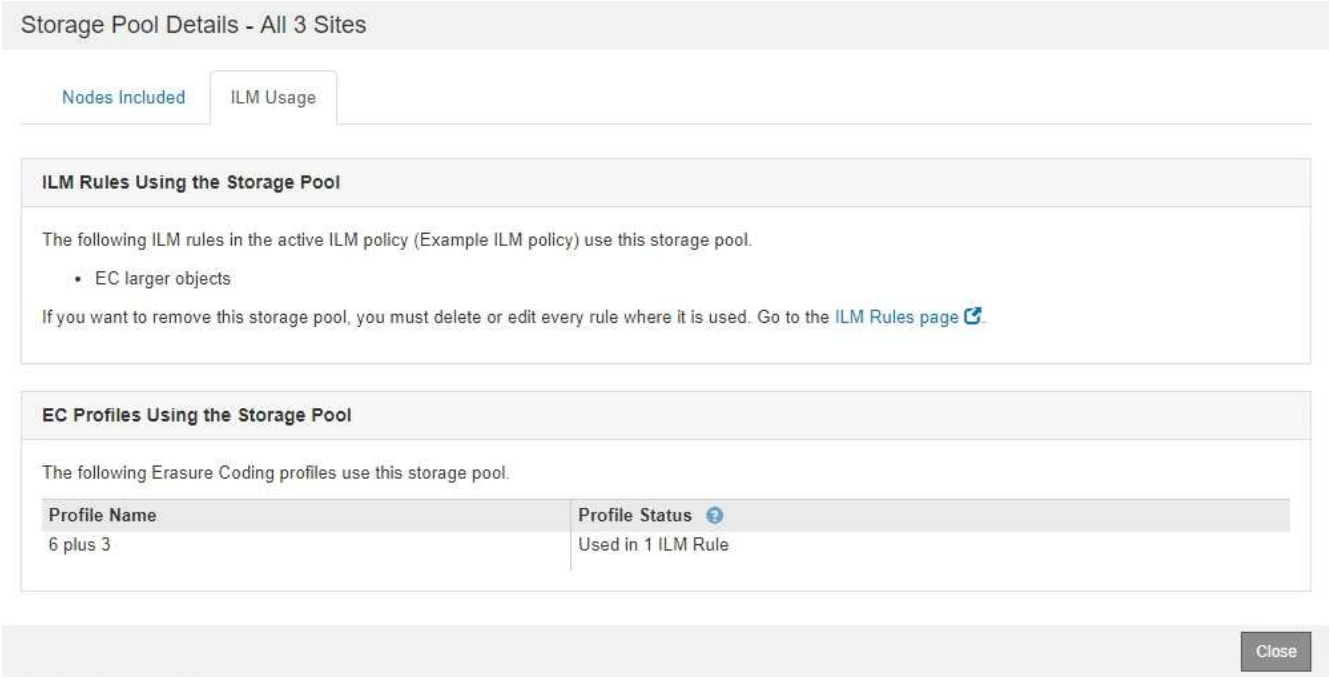
4. Seleccione la pestaña **uso de ILM** para determinar si el pool de almacenamiento se está utilizando actualmente en cualquier regla de ILM o perfil de código de borrado.

   En este ejemplo, el pool de almacenamiento de DC1 se utiliza en tres reglas de ILM: Dos reglas que están en la política de ILM activa y una regla que no está en la política activa.



No se puede quitar un pool de almacenamiento si se utiliza en una regla de ILM.

En este ejemplo, el grupo de almacenamiento All 3 Sites se utiliza en un perfil de código de borrado. A su vez, un perfil de código de borrado lo utiliza una regla de ILM en la política de ILM activa.



No se puede quitar un pool de almacenamiento si se utiliza en un perfil de código de borrado.

5. Si lo desea, visite la página **Reglas ILM** para obtener más información y administrar las reglas que utilizan el pool de almacenamiento.

   Consulte las instrucciones para trabajar con las reglas de ILM.

6. Cuando haya terminado de ver los detalles de la agrupación de almacenamiento, seleccione **Cerrar**.

Información relacionada

Trabaje con las reglas de ILM y las políticas de ILM

Editar pool de almacenamiento

Es posible editar un pool de almacenamiento para cambiar su nombre o para actualizar los sitios y las calificaciones de almacenamiento.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Revisó las directrices para crear pools de almacenamiento.
- Si prevé editar un pool de almacenamiento utilizado por una regla en la política de ILM activa, habrá pensado en cómo afectarán los cambios a la ubicación de los datos de los objetos.

Acerca de esta tarea

Si va a añadir un nuevo nivel de almacenamiento a un pool de almacenamiento que utilice la normativa de gestión del ciclo de vida de la información activa, tenga en cuenta que los nodos de almacenamiento del nuevo nivel no se utilizarán automáticamente. Para forzar a StorageGRID a usar un nuevo nivel de almacenamiento, debe activar una nueva política de ILM después de guardar el pool de almacenamiento editado.

Pasos

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

   Aparece la página Storage Pools.

2. Seleccione el botón de opción del pool de almacenamiento que desea editar.

   El pool de almacenamiento todos los nodos del almacenamiento no se puede editar.

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

   > No podrá cambiar el sitio o el grado de almacenamiento si el pool de almacenamiento se utiliza en un perfil de código de borrado y el cambio provocaría que el esquema de codificación de borrado no sea válido. Por ejemplo, si un pool de almacenamiento utilizado en un perfil de código de borrado incluye actualmente un grado de almacenamiento con un solo sitio, se le impide utilizar un grado de almacenamiento con dos sitios, ya que el cambio haría que el esquema de código de borrado no sea válido.

6. Seleccione **Guardar**.

Después de terminar

Si agregó un nuevo nivel de almacenamiento a un pool de almacenamiento usado en la política de ILM activa, active una nueva política de ILM para forzar a StorageGRID a usar el nuevo nivel de almacenamiento. Por ejemplo, Clone la política de ILM existente y luego active el clon.

Quitar un pool de almacenamiento

Es posible quitar un pool de almacenamiento que no se está usando.

Lo que necesitará

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

Pasos

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

   Aparece la página Storage Pools.

2. Observe la columna ILM Usage de la tabla para determinar si puede eliminar el pool de almacenamiento.

   No se puede quitar un pool de almacenamiento si se está utilizando en una regla de ILM o en un perfil de código de borrado. Según sea necesario, seleccione **Ver detalles** > **uso de ILM** para determinar dónde se utiliza un pool de almacenamiento.

3. Si no se está utilizando la agrupación de almacenamiento que desea quitar, seleccione el botón de opción.
4. Seleccione **Quitar**.
5. Seleccione **OK**.

Utilice Cloud Storage Pools

Qué es un pool de almacenamiento cloud

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

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

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

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

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

Ciclo de vida de un objeto de Cloud Storage Pool

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

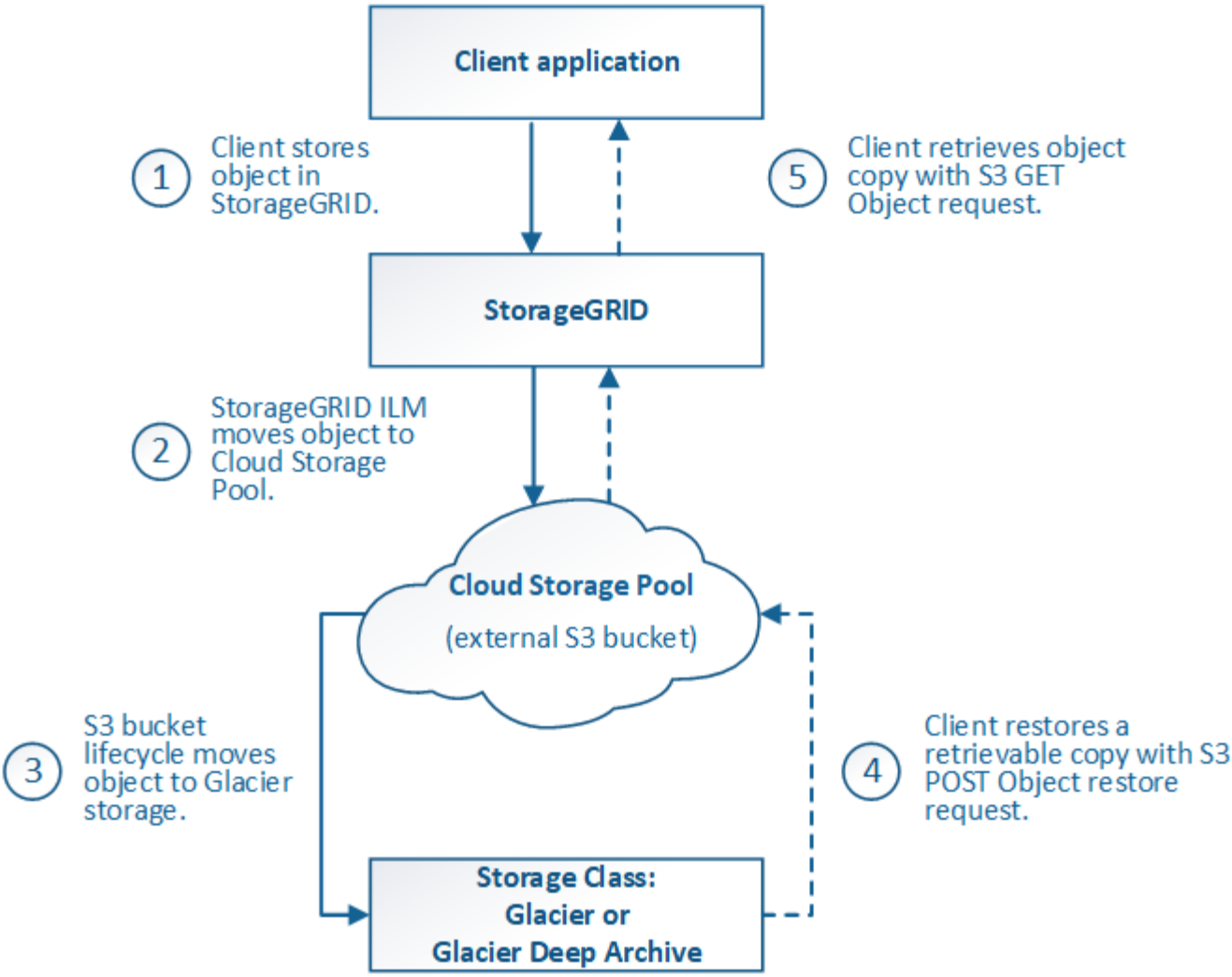
- S3: Ciclo de vida de un objeto de Cloud Storage Pool
- Azure: Ciclo de vida de un objeto de Cloud Storage Pool

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

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

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

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



1. **Objeto almacenado en StorageGRID**

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

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

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

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

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

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

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

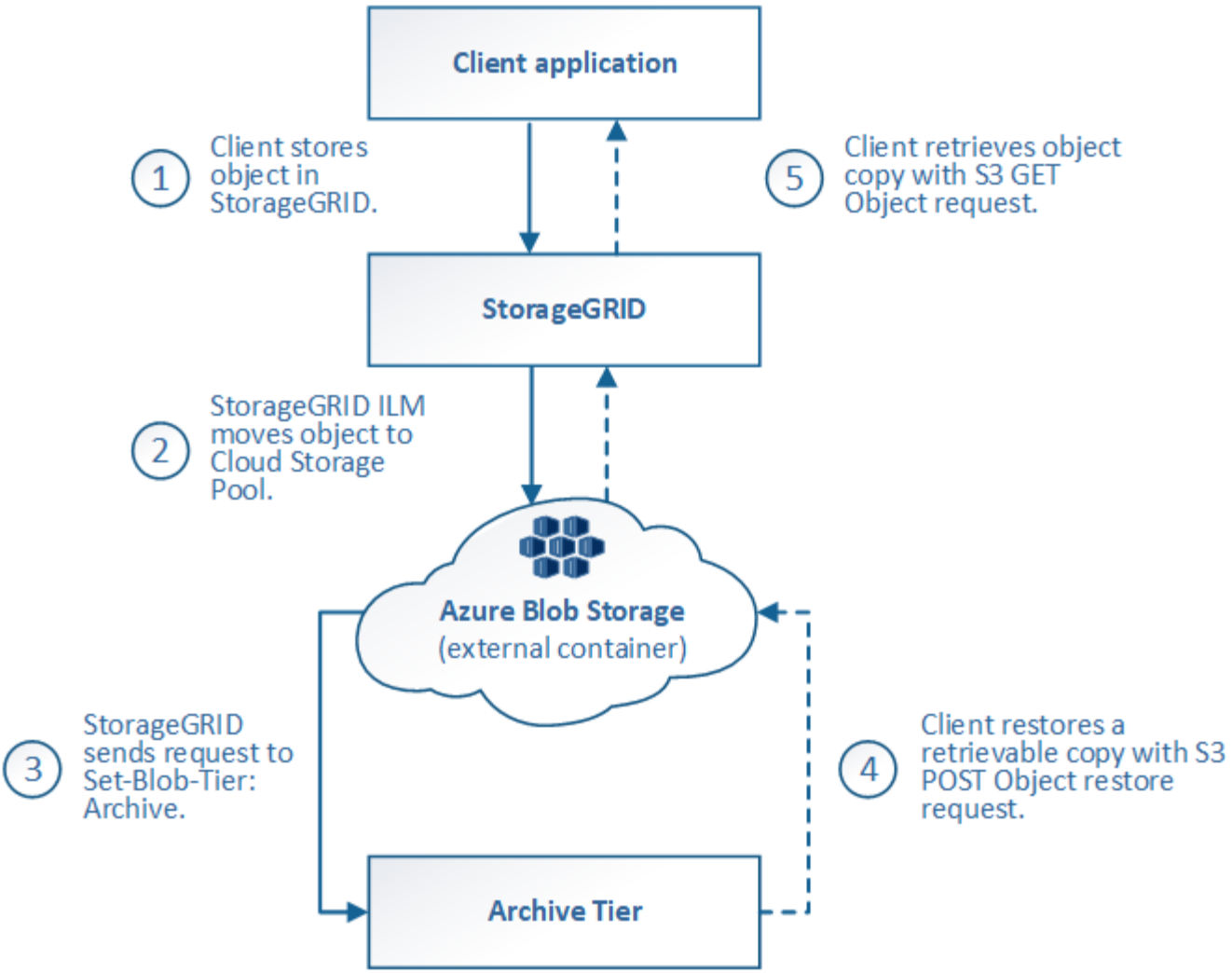
   > Si también hay una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier con una solicitud DE restauración POSTERIOR a objeto. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

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

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

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



1. **Objeto almacenado en StorageGRID**

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

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

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

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

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

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

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

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

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

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

5. **Objeto recuperado**

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

Información relacionada

Use S3

Cuándo usar Cloud Storage Pools

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

Realizar backup de los datos de StorageGRID en una ubicación externa

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

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

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

Para implantar una solución de backup:

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

Organizar en niveles los datos de StorageGRID en ubicaciones externas

Puede utilizar un pool de almacenamiento en cloud para almacenar objetos fuera del sistema StorageGRID. Por ejemplo, supongamos que tiene un gran número de objetos que necesita retener, pero espera tener acceso a esos objetos rara vez, si es que alguna vez. Puede usar un pool de almacenamiento en cloud para organizar los objetos en niveles para reducir el almacenamiento y liberar espacio en StorageGRID.

Para implementar una solución por niveles:

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

Mantenga varios extremos de cloud

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

Para implementar varios extremos de cloud:

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

Consideraciones para Cloud Storage Pools

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

Consideraciones generales

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

- No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.

Información necesaria para crear un pool de almacenamiento en cloud

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

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

Consideraciones sobre los puertos utilizados para Cloud Storage Pools

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

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

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

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

Si utiliza un servidor proxy no transparente, también debe hacerlo Configure un proxy de almacenamiento para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

Consideraciones sobre los costos

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

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

Es posible que deba incurrir en costes más significativos si necesita mover objetos desde un extremo de almacenamiento en cloud externo a StorageGRID. Los objetos pueden moverse de nuevo a StorageGRID en cualquiera de estos casos:

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

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

S3: Permisos necesarios para el bloque de Cloud Storage Pool

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

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

S3: Consideraciones para el ciclo de vida del bloque externo

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

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

Por ejemplo, supongamos que desea que se realice inmediatamente la transición de todos los objetos movidos de StorageGRID al pool de almacenamiento en cloud al almacenamiento Amazon S3 Glacier. Debe crear una configuración de ciclo de vida en el bloque S3 externo que especifique una única acción (**transición**) de la siguiente forma:

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

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

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

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

Azure: Consideraciones para el nivel de acceso

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

Azure: Gestión del ciclo de vida no compatible

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

Información relacionada

- Cree un pool de almacenamiento en el cloud

- S3: Especifique los detalles de autenticación para un pool de almacenamiento en cloud
- C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud
- Azure: Especifique detalles de autenticación para un pool de almacenamiento en cloud

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

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

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

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

Cree un pool de almacenamiento en el cloud

Cuando crea un Cloud Storage Pool, debe especificar el nombre y la ubicación del bloque o contenedor externo que StorageGRID utilizará para almacenar objetos, el tipo de proveedor cloud (Amazon S3 o Azure Blob Storage) y la información que StorageGRID necesita para acceder a la bloque o el contenedor externo.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha revisado las directrices para configurar Cloud Storage Pools.
- El bloque o contenedor externo al que hace referencia el Cloud Storage Pool ya existe.
- Tiene toda la información de autenticación necesaria para acceder al bloque o contenedor.

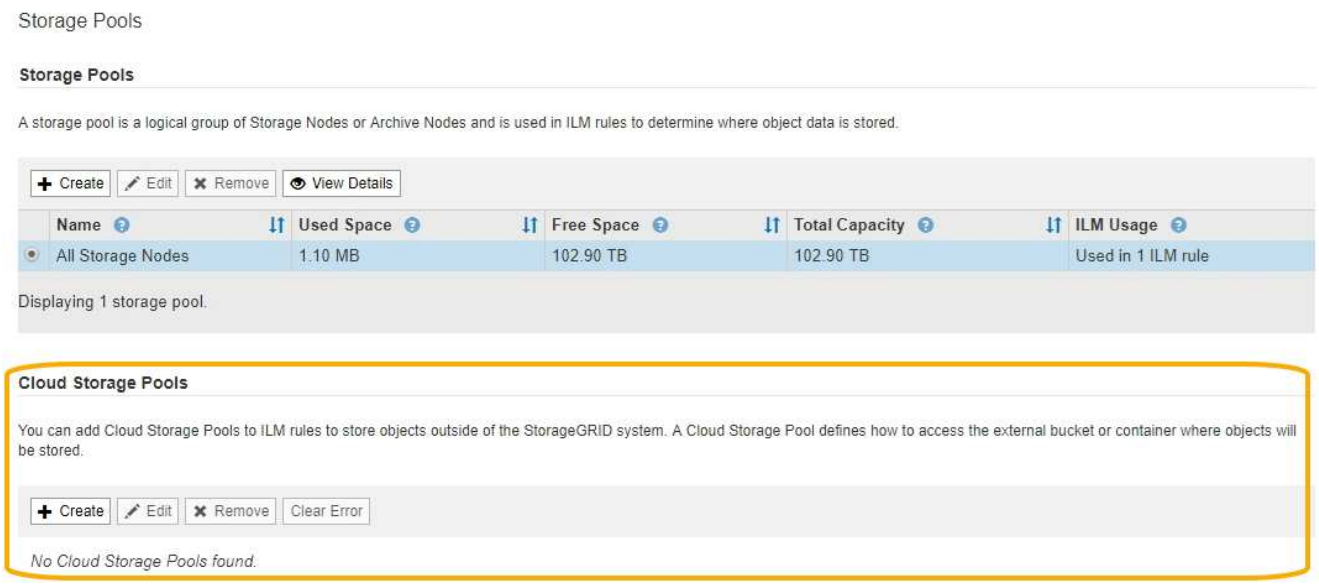
Acerca de esta tarea

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

Pasos

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

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



2. En la sección Cloud Storage Pools de la página, seleccione **Crear**.

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

3. Introduzca la siguiente información:

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

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

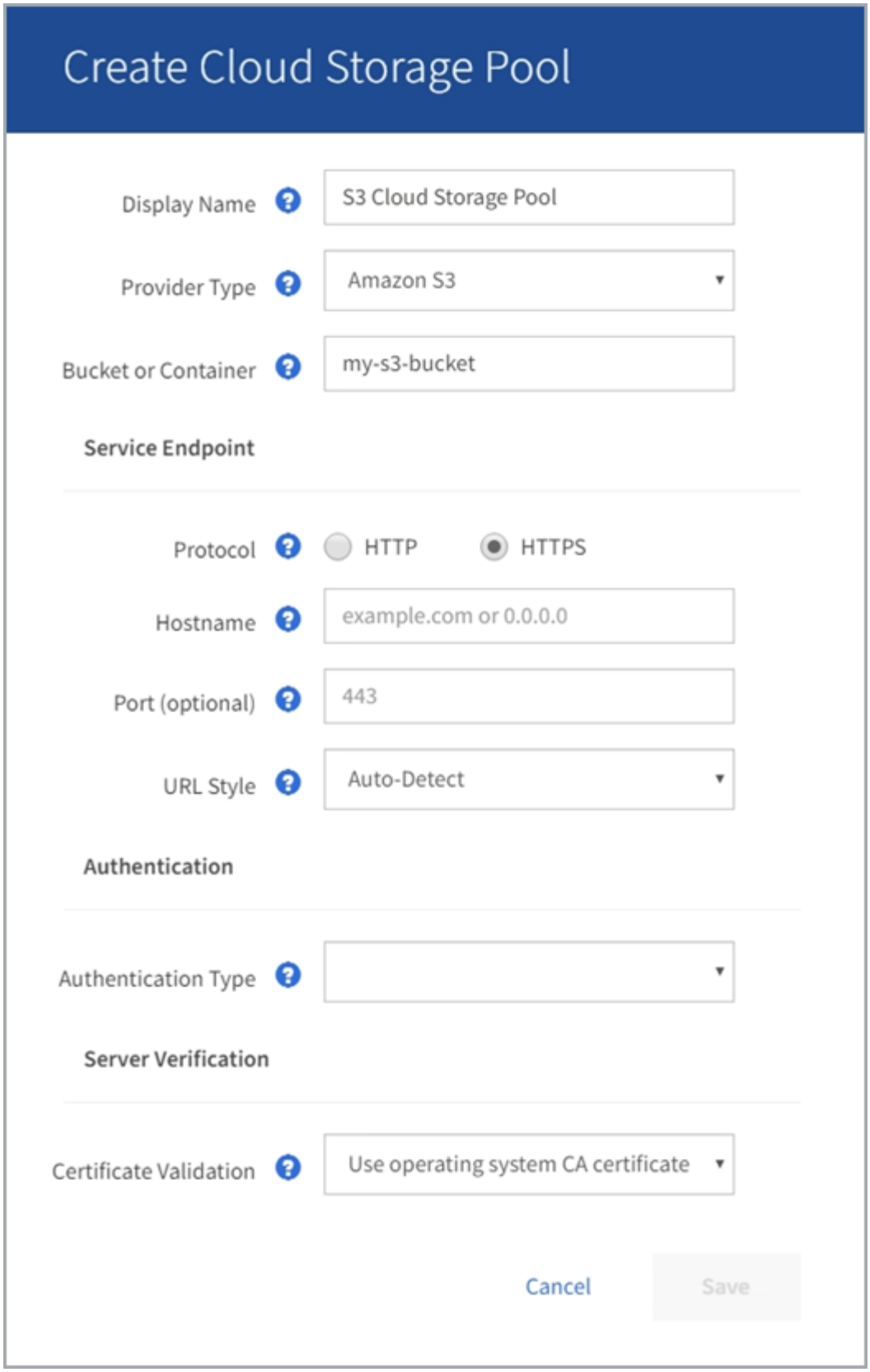
S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud

Al crear un Cloud Storage Pool para S3, debe seleccionar el tipo de autenticación

requerido para el extremo de Cloud Storage Pool. Puede especificar Anónimo o introducir un ID de clave de acceso y una clave de acceso secreta.

Lo que necesitará

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



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

Pasos

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

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

   El protocolo predeterminado es HTTPS.

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

   Por ejemplo:

   `s3-aws-region.amazonaws.com`

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

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

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

b. Seleccione el estilo de la URL para el bucket de Cloud Storage Pool:

Opción	Descripción
Estilo de alojamiento virtual	Utilice una URL de estilo alojado virtual para acceder al bloque. Las URL de estilo alojado virtual incluyen el nombre de bloque como parte del nombre de dominio, por ejemplo `https://bucket-name.s3.company.com/key-name`.
Estilo de trazado	Utilice una dirección URL de estilo de ruta para acceder al bloque. Las direcciones URL de estilo de ruta incluyen el nombre de bloque al final, por ejemplo `https://s3.company.com/bucket-name/key-name`. **Nota:** la dirección URL de estilo de ruta está en desuso.
Detección automática	Intente detectar automáticamente qué estilo de URL usar, en función de la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una dirección URL de tipo path. Seleccione esta opción sólo si no conoce el estilo específico que desea utilizar.

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

Opción	Descripción
Clave de acceso	Se requiere un identificador de clave de acceso y una clave de acceso secreta para acceder al bloque del pool de almacenamiento en cloud.

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

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

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

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

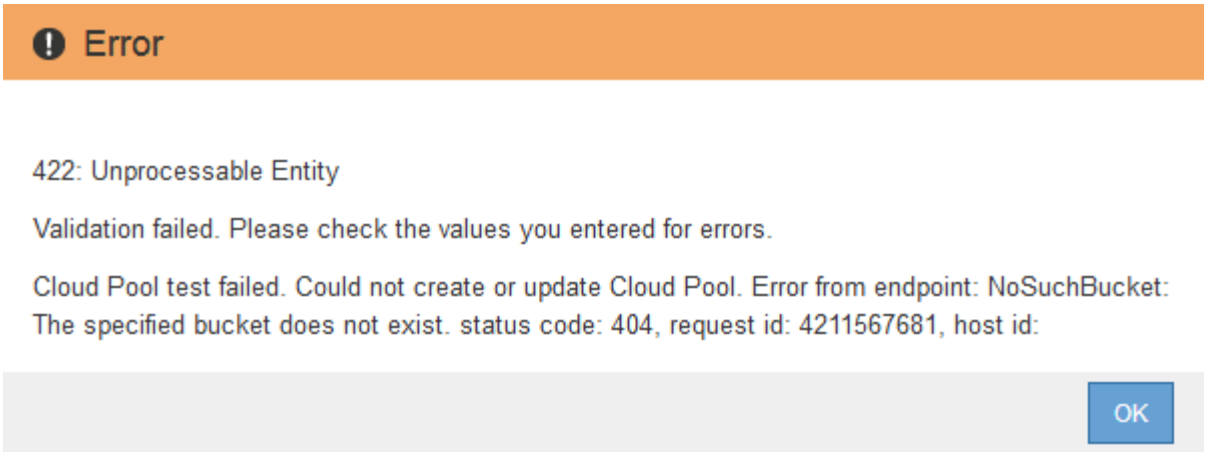
Opción	Descripción
Utilizar certificado de CA del sistema operativo	Utilice los certificados de CA de cuadrícula predeterminados instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Seleccione **Seleccionar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

5. Seleccione **Guardar**.

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

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

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



Consulte las instrucciones para Solución de problemas de Cloud Storage Pools, Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud

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

Lo que necesitará

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

Pasos

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

   Aparecen los campos de autenticación CAP C2S.

Create Cloud Storage Pool

Display Name: C2S Cloud Storage Pool

Provider Type: Amazon S3

Bucket or Container: my-c2s-bucket

Service Endpoint

Protocol: HTTP HTTPS

Hostname: s3-aws-region.amazonaws.com

Port (optional): 443

URL Style: Auto-Detect

Authentication

Authentication Type: CAP (C2S Access Portal)

Temporary Credentials URL: https://example.com/CAP/api/v1/cred

Server CA Certificate: Select New

Client Certificate: Select New

Client Private Key: Select New

Client Private Key Passphrase (optional):

Server Verification

Certificate Validation: Use operating system CA certificate

Cancel Save

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

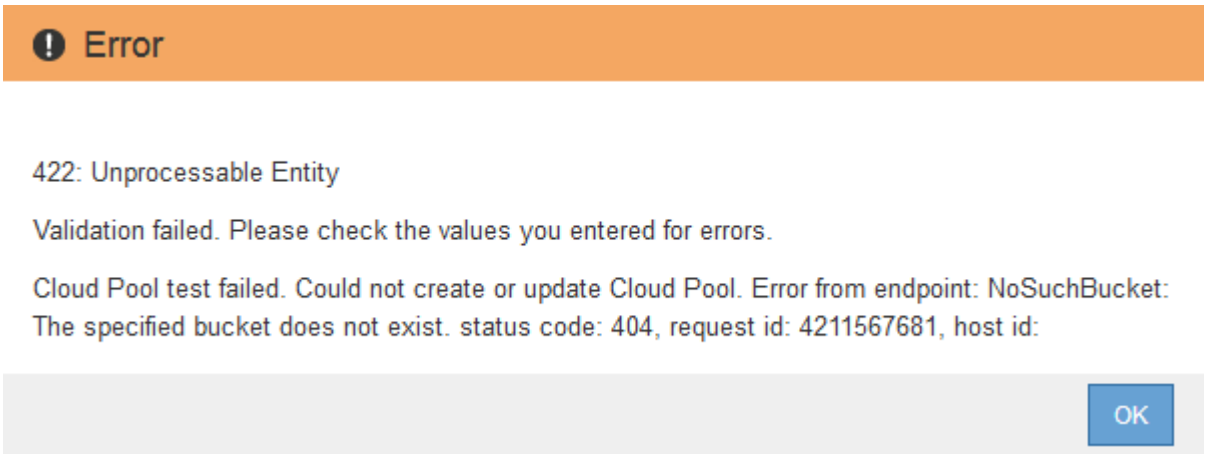
      Si la clave privada está cifrada, se debe utilizar el formato tradicional. (No se admite el formato cifrado PKCS #8).

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

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

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

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



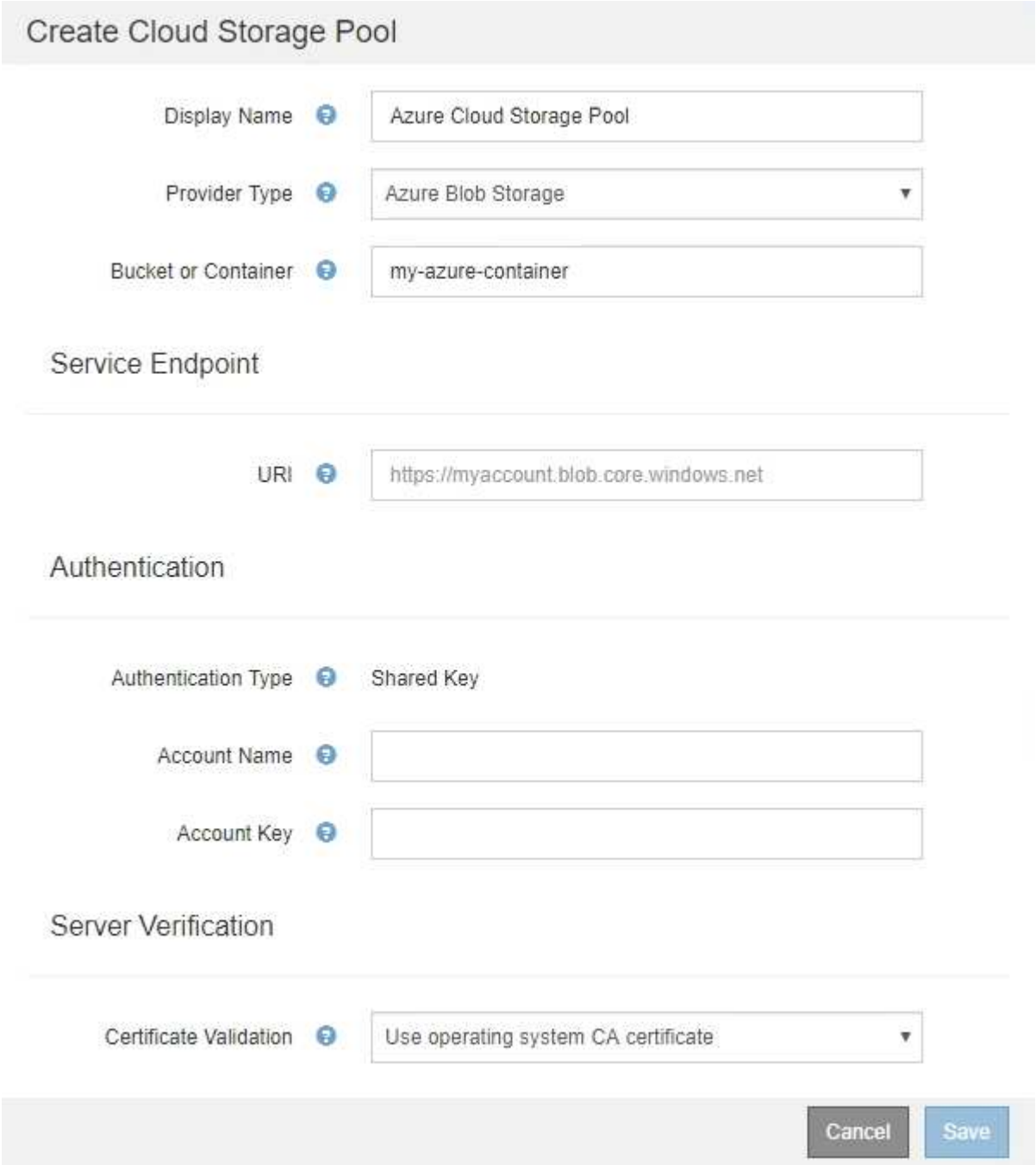
Consulte las instrucciones para Solución de problemas de Cloud Storage Pools, Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

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

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

Lo que necesitará

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



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

encontrar estos valores.

Pasos

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

   Especifique el URI en uno de los siguientes formatos:

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

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

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

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

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

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

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

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

4. Seleccione **Guardar**.

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

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

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

Consulte las instrucciones para Solución de problemas de Cloud Storage Pools, Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

Editar un pool de almacenamiento en el cloud

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

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha revisado el Consideraciones para Cloud Storage Pools.

Pasos

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

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

   Cloud Storage Pools

   You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

   + Create | Edit | Remove | Clear Error

	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
◉	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✔	
○	s3-endpoint	https://s3.amazonaws.com	s3	s1	✔	

   Displaying 2 pools.

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

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

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

5. Seleccione **Guardar**.

   Cuando guarda un pool de almacenamiento en cloud, StorageGRID valida que el bloque o el contenedor y el extremo de servicio existen, y que se pueden acceder a ellos con las credenciales especificadas.

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

   Consulte las instrucciones para Solución de problemas de Cloud Storage Pools, Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

Quitar un pool de almacenamiento en el cloud

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

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha confirmado que el bloque de S3 o el contenedor de Azure no contienen ningún objeto. Se produce un error si intenta quitar un Pool de almacenamiento en cloud si contiene objetos. Consulte Solucione problemas de Cloud Storage Pools.

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

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

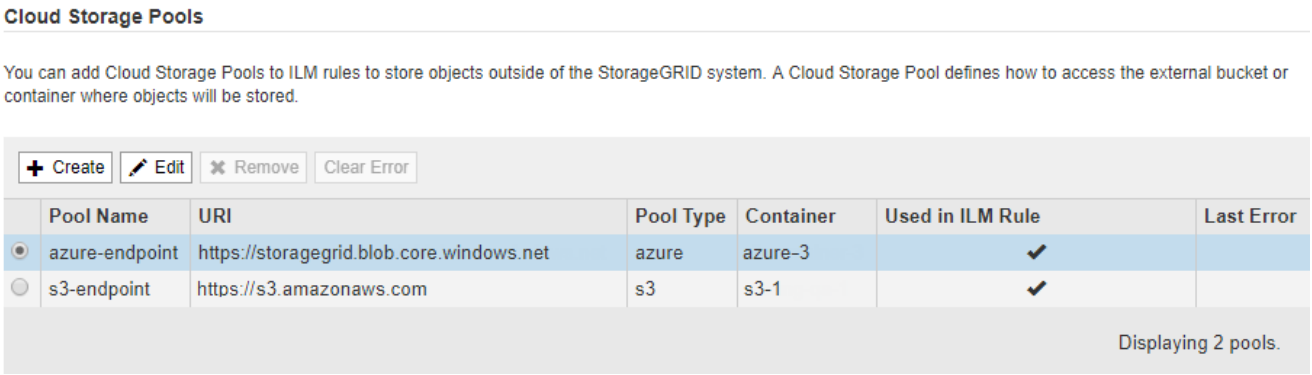
Pasos

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

   Aparece la página Storage Pools.

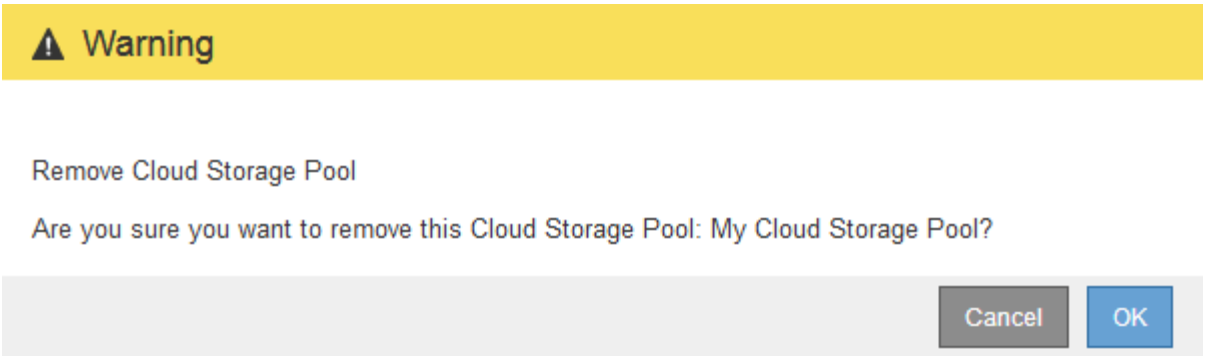
2. Seleccione el botón de opción de un pool de almacenamiento en cloud que no se utilice actualmente en una regla de ILM.

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



3. Seleccione **Quitar**.

   Aparecerá una advertencia de confirmación.



4. Seleccione **OK**.

   El pool de almacenamiento en cloud se elimina.

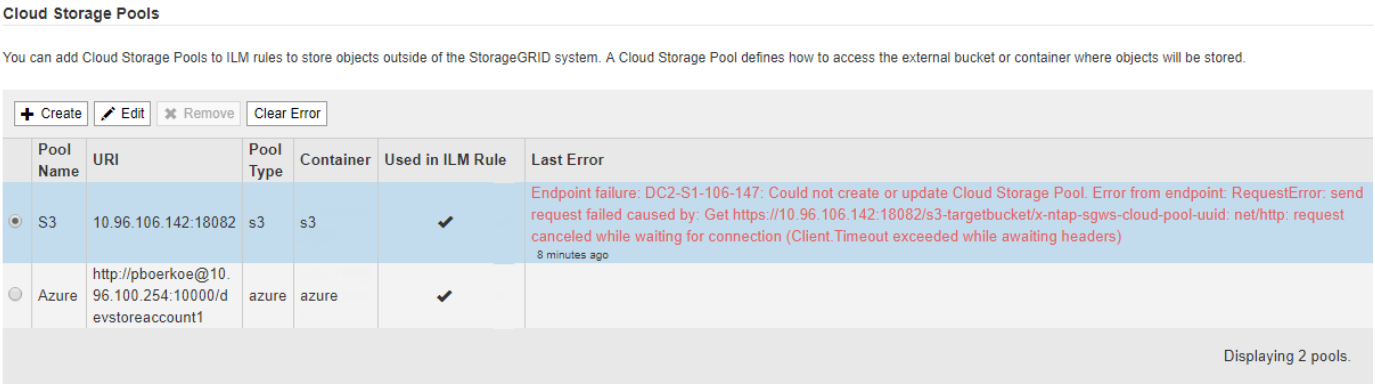
Solucione problemas de Cloud Storage Pools

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

Determine si se ha producido un error

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

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

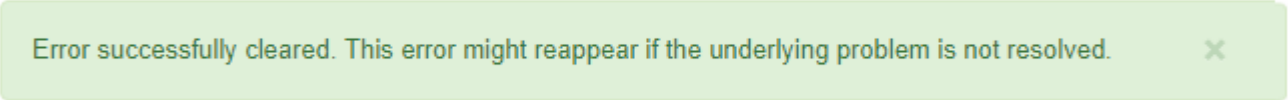


Además, se activa una alerta de error * de conectividad del grupo de almacenamiento en cloud* si la comprobación del estado detecta que se han producido uno o varios errores nuevos de Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya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

Compruebe si se ha resuelto un error

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

el cloud.



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

Error: Este pool de almacenamiento en cloud contiene contenido inesperado

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

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

Intente realizar estos pasos para corregir el problema:

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

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

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

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

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

Error: No se pudo analizar el certificado de CA

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

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

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

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

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

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

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

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

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

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

Error: Los objetos ya se han colocado en este cucharón

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. No puede eliminar un pool de almacenamiento en cloud si contiene datos que se movieron a este punto por ILM, datos que estaban en el bloque antes de configurar el Cloud Storage Pool o datos que algún otro origen colocó en el bloque después de crear el Cloud Storage Pool.

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

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

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

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

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

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

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

Información relacionada

Ciclo de vida de un objeto de Cloud Storage Pool

Configure los perfiles de código de borrado

Cree un perfil de código de borrado

Para crear un perfil de código de borrado, debe asociar un pool de almacenamiento que contiene nodos de almacenamiento con un esquema de código de borrado. Esta asociación determina el número de fragmentos de datos y de paridad creados y el lugar en el que el sistema distribuye estos fragmentos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha creado un grupo de almacenamiento que incluye exactamente un sitio o un grupo de almacenamiento que incluye tres o más sitios. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que únicamente tenga dos ubicaciones.

Acerca de esta tarea

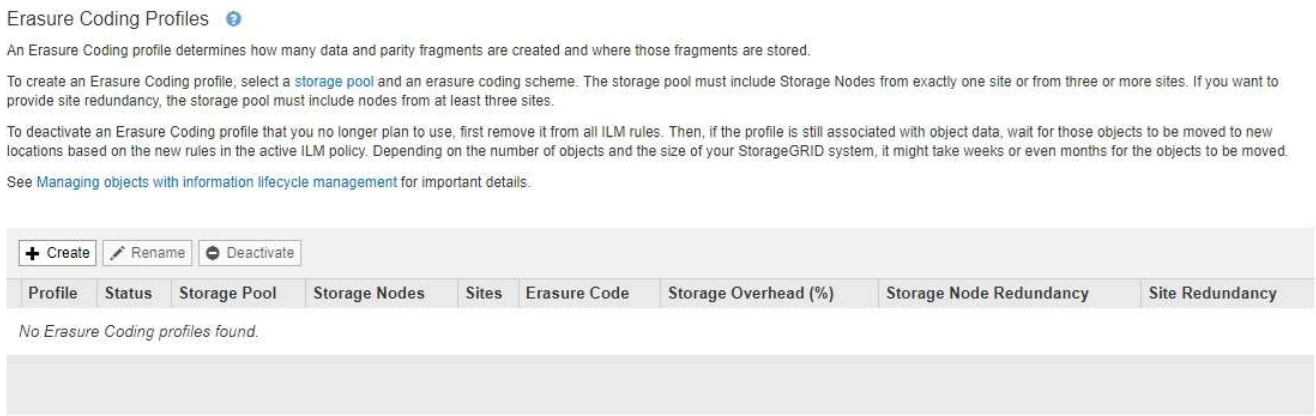
Los pools de almacenamiento utilizados en los perfiles de código de borrado deben incluir exactamente un sitio o tres o más. Si desea proporcionar redundancia del sitio, el pool de almacenamiento debe tener al menos tres sitios.

> Debe seleccionar un pool de almacenamiento que contenga nodos de almacenamiento. No se pueden usar nodos de archivado para los datos codificados mediante borrado.

Pasos

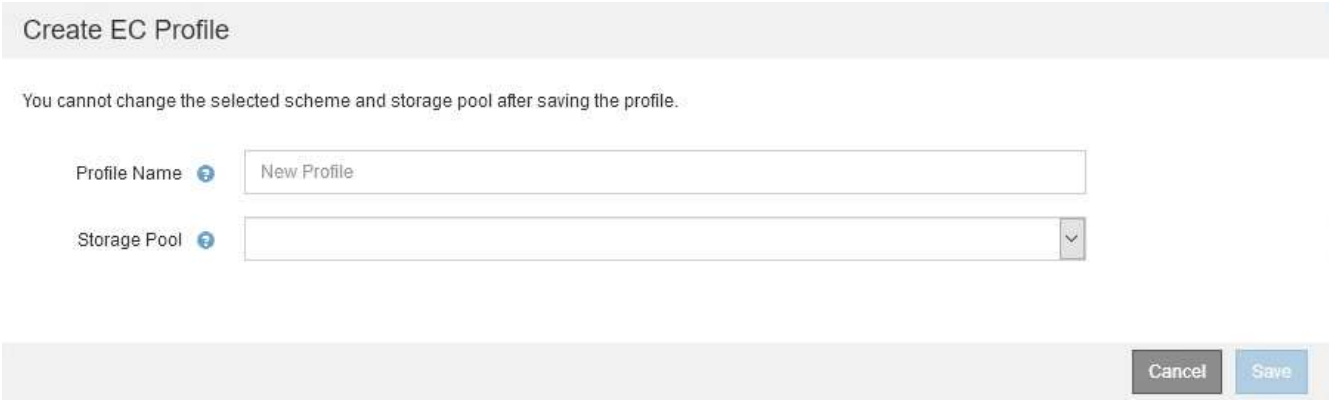
1. Seleccione **ILM** > **codificación de borrado**.

   Aparece la página Perfiles de código de borrado.



2. Seleccione **Crear**.

Aparece el cuadro de diálogo Crear perfil de EC.



3. Introduzca un nombre único para el perfil de código de borrado.

   Los nombres de perfiles de código 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.

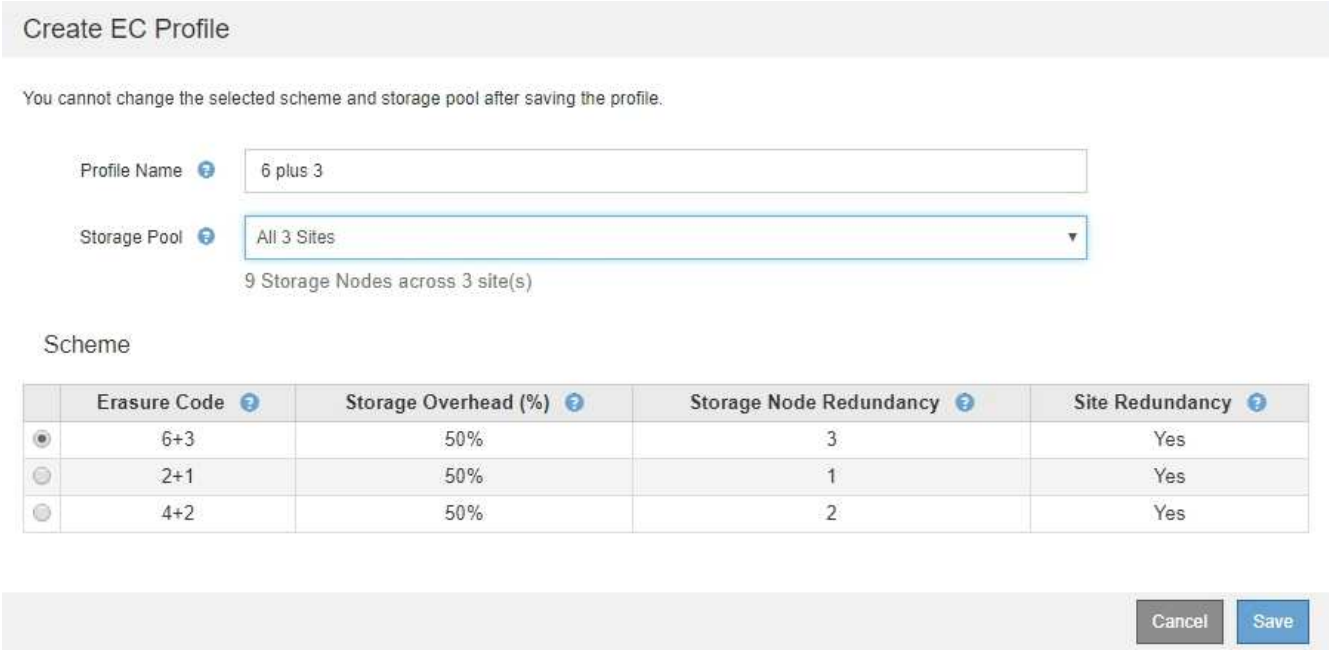
   > El nombre del perfil de código de borrado se anexa al nombre del pool de almacenamiento en la instrucción de ubicación de una regla de ILM.

4. Seleccione el pool de almacenamiento que ha creado para este perfil de código de borrado.

   > Si el grid incluye actualmente un solo sitio, no podrá utilizar el pool de almacenamiento predeterminado, todos los nodos de almacenamiento o cualquier pool de almacenamiento que incluya el sitio predeterminado, todos los sitios. Este comportamiento impide que el perfil de código de borrado no sea válido si se agrega un segundo sitio.

   > Si un pool de almacenamiento incluye exactamente dos sitios, no podrá utilizar ese pool de almacenamiento para codificar el borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.

   Cuando se selecciona un pool de almacenamiento, se muestra la lista de esquemas de codificación de borrado disponibles, según la cantidad de nodos de almacenamiento y sitios del pool.



La siguiente información se incluye para cada esquema de codificación de borrado disponible:

- **Código de borrado**: El nombre del esquema de código de borrado en el formato siguiente: Fragmentos de datos + fragmentos de paridad.
- **Gastos generales de almacenamiento (%)**: El almacenamiento adicional necesario para fragmentos de paridad en relación con el tamaño de los datos del objeto. Sobrecarga del almacenamiento = número total de fragmentos de paridad / número total de fragmentos de datos.
- **Redundancia del nodo de almacenamiento**: El número de nodos de almacenamiento que se pueden perder manteniendo la capacidad de recuperar datos del objeto.
- **Redundancia del sitio**: Si el código de borrado seleccionado permite recuperar los datos del objeto si se pierde un sitio.

  Para admitir la redundancia de sitios, el pool de almacenamiento seleccionado debe incluir varios sitios, cada uno con nodos de almacenamiento suficientes para permitir la pérdida de cualquier sitio. Por ejemplo, para admitir la redundancia del sitio con un esquema de codificación de borrado 6+3, el pool de almacenamiento seleccionado debe incluir al menos tres sitios con al menos tres nodos de almacenamiento en cada sitio.

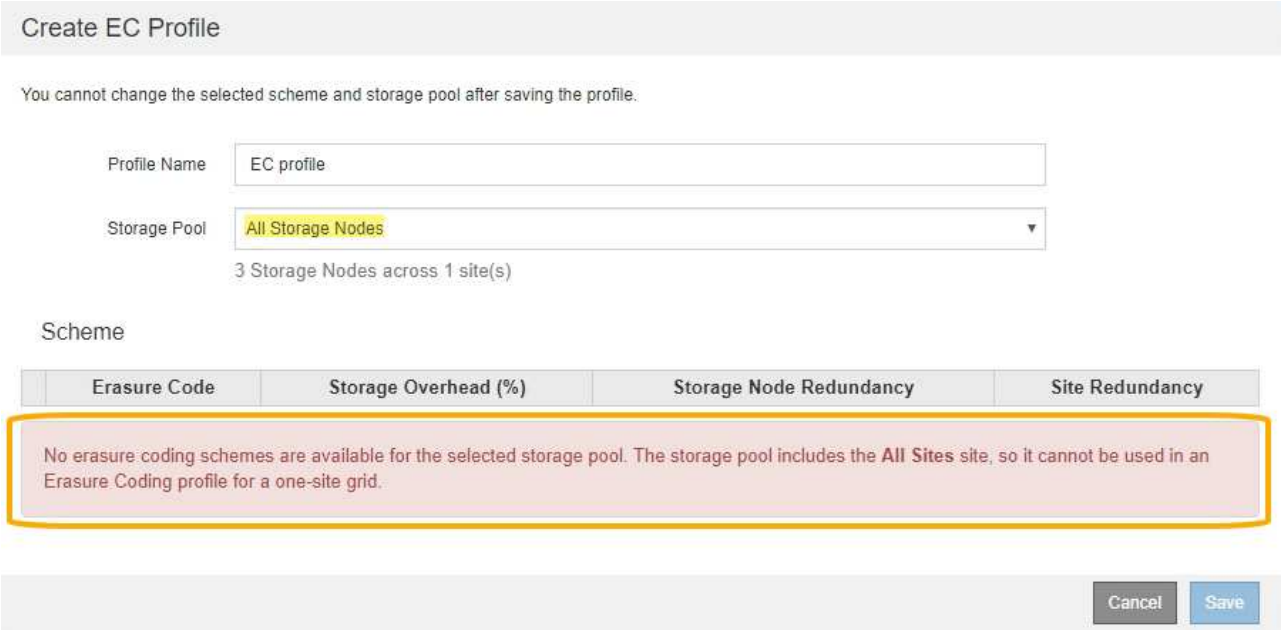
  Los mensajes se muestran en estos casos:

- El pool de almacenamiento seleccionado no proporciona redundancia de sitio. Se espera el siguiente mensaje cuando el grupo de almacenamiento seleccionado incluye sólo un sitio. Puede utilizar este perfil de código de borrado en reglas de ILM para protegerse contra fallos de nodos.

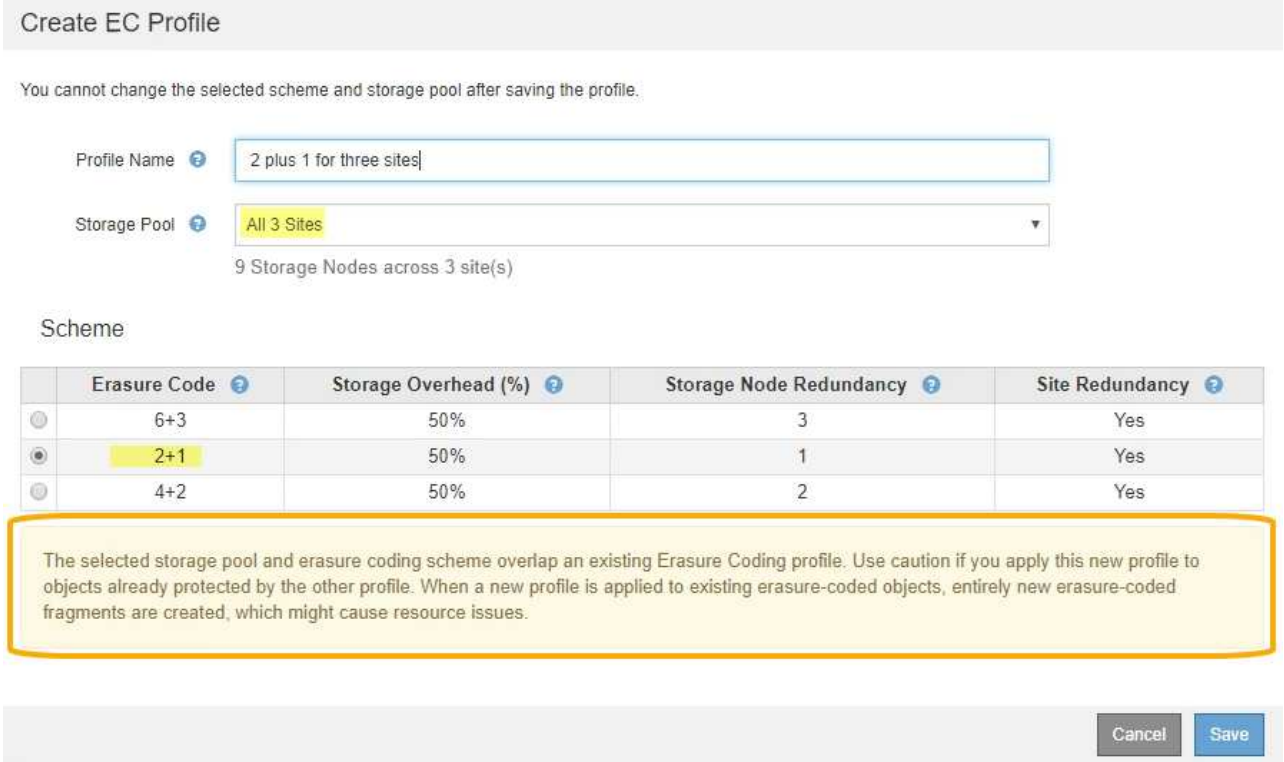
- El pool de almacenamiento seleccionado no cumple con los requisitos de ningún esquema de

codificación de borrado. Por ejemplo, se espera el siguiente mensaje cuando el grupo de almacenamiento seleccionado incluye exactamente dos sitios. Si desea utilizar la codificación de borrado para proteger los datos de los objetos, debe seleccionar un pool de almacenamiento con exactamente un sitio o un pool de almacenamiento con tres o más ubicaciones.

- El grid incluye un solo sitio y seleccionó el pool de almacenamiento predeterminado, todos los nodos de almacenamiento o cualquier pool de almacenamiento que incluya el sitio predeterminado, todos los sitios.



- El esquema de codificación de borrado y el pool de almacenamiento seleccionados se superponen con otro perfil de código de borrado.



En este ejemplo, aparece un mensaje de advertencia porque otro perfil de código de borrado está utilizando el esquema 2+1 y el grupo de almacenamiento del otro perfil también utiliza uno de los sitios del grupo de almacenamiento todos los 3 sitios.

Aunque no se le impide crear este nuevo perfil, debe tener mucho cuidado al empezar a utilizarlo en la política de ILM. Si este nuevo perfil se aplica a los objetos existentes con código de borrado ya protegidos por otro perfil, StorageGRID creará un conjunto de fragmentos de objeto completamente nuevo. No reutilizará los fragmentos 2+1 existentes. Los problemas de los recursos se pueden producir al migrar de un perfil de codificación de borrado a otro, aunque los esquemas de codificación de borrado sean los mismos.

5. Si se muestra más de un esquema de codificación de borrado, seleccione el que desee utilizar.

   Al decidir qué esquema de codificación de borrado utilizar, debe equilibrar la tolerancia a fallos (lograda mediante más segmentos de paridad) con los requisitos del tráfico de red en las reparaciones (más fragmentos equivale a más tráfico de red). Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3, seleccione el esquema 6+3 si se requiere paridad adicional y tolerancia a fallos. Seleccione el esquema 4+2 si los recursos de red están limitados para reducir el uso de la red durante las reparaciones de nodo.

6. Seleccione **Guardar**.

Cambie el nombre de un perfil de código de borrado

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

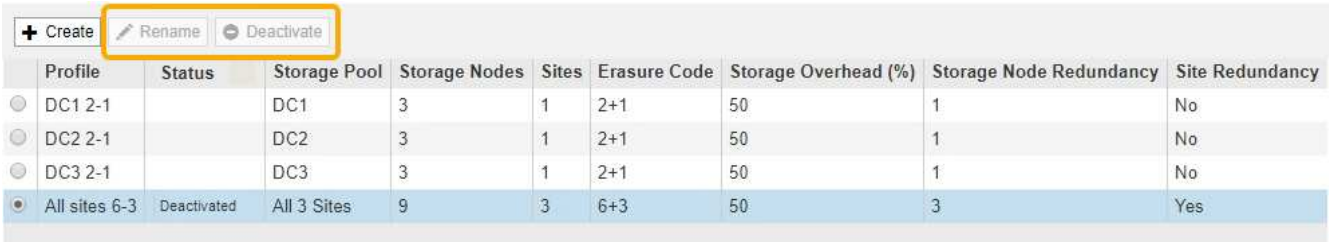
Lo que necesitará

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

Pasos

1. Seleccione **ILM** > **codificación de borrado**.

   Aparece la página Perfiles de código de borrado. Los botones **Renombrar** y **Desactivar** están desactivados.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Seleccione el perfil al que desea cambiar el nombre.

   Los botones **Renombrar** y **Desactivar** se activan.

3. Seleccione **Cambiar nombre**.

   Aparece el cuadro de diálogo Cambiar nombre de perfil EC.

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

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

   Los nombres de perfiles de código 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 código de borrado

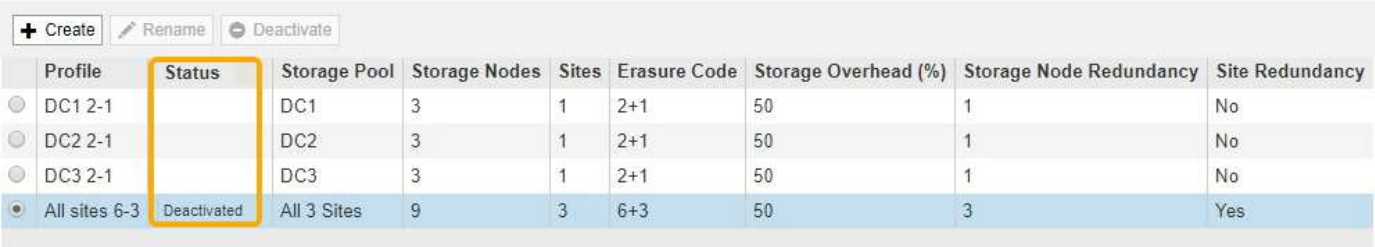
Puede desactivar un perfil de código de borrado si ya no tiene pensado utilizarlo y si el perfil no se utiliza actualmente en ninguna regla de ILM.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha confirmado que no hay operaciones de reparación de datos codificados para borrado ni procedimientos de retirada en curso. Se devuelve un mensaje de error si intenta desactivar un perfil de código de borrado mientras alguna de estas operaciones está en curso.

Acerca de esta tarea

Cuando desactiva un perfil de código de borrado, el perfil sigue apareciendo en la página Perfiles de código de borrado, pero su estado es **desactivado**.



+ Create | Rename | Deactivate

	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	DC1 2-1		DC1	3	1	2+1	50	1	No
○	DC2 2-1		DC2	3	1	2+1	50	1	No
○	DC3 2-1		DC3	3	1	2+1	50	1	No
◉	All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Ya no puede utilizar un perfil de código de borrado que se haya desactivado. No se muestra un perfil desactivado al crear las instrucciones de colocación para una regla de ILM. No puede reactivar un perfil desactivado.

StorageGRID evita la desactivación de un perfil de código de borrado si se cumple alguna de las siguientes condiciones:

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

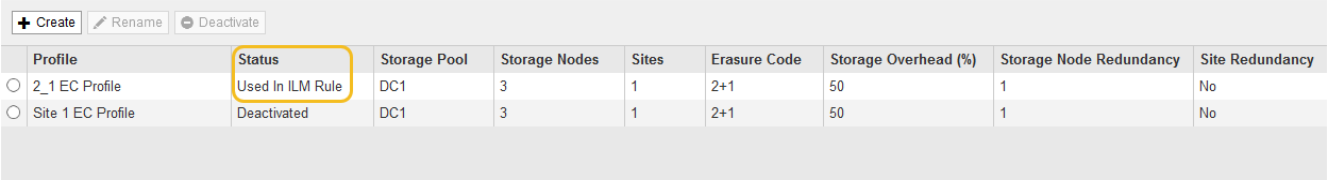
Pasos

1. Seleccione **ILM** > **código de borrado**.

   Aparece la página Perfiles de código de borrado. Los botones **Renombrar** y **Desactivar** están desactivados.

2. Revise la columna **Estado** para confirmar que el perfil de código de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

   No puede desactivar un perfil de codificación de borrado si se utiliza en cualquier regla de ILM. En el ejemplo, el **2_1 EC Profile** se utiliza en al menos una regla ILM.



+ Create | Rename | Deactivate

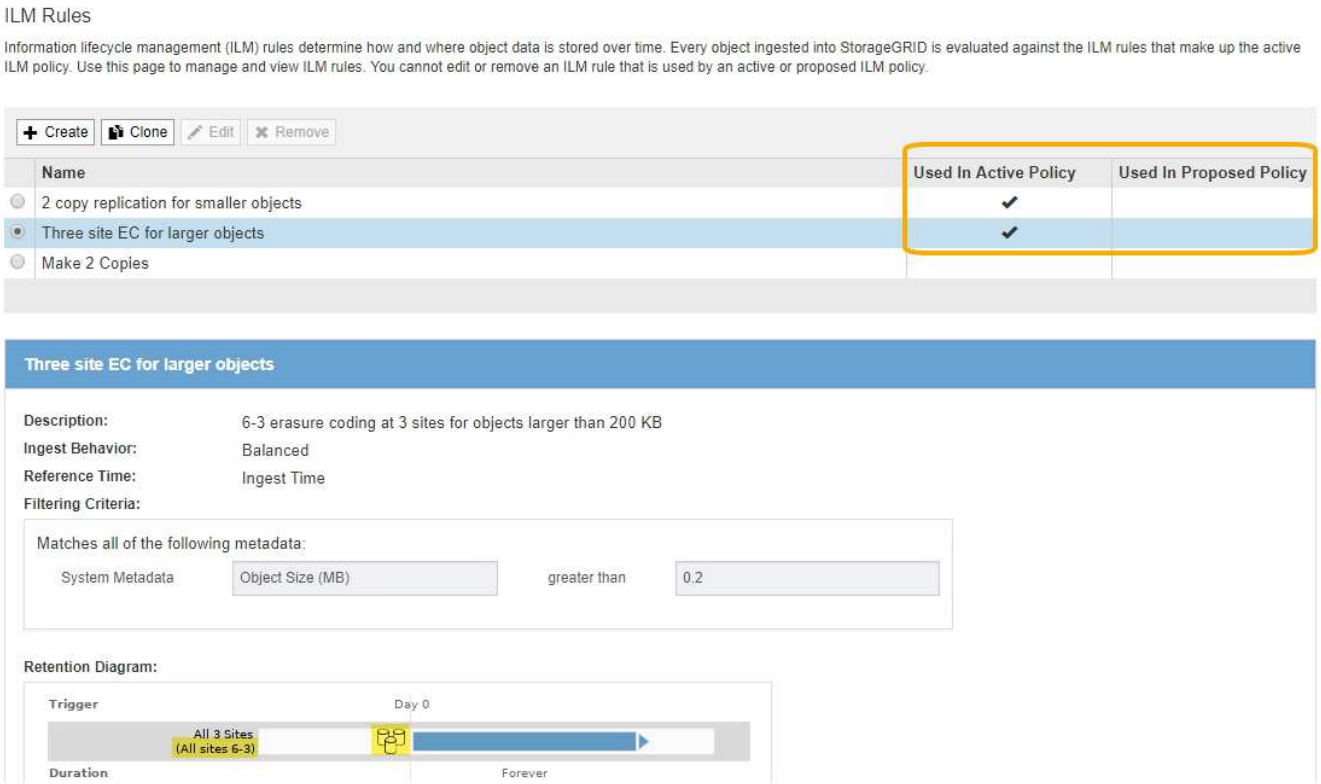
	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
○	Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. Si el perfil se utiliza en una regla de ILM, siga estos pasos:

   a. Seleccione **ILM** > **Reglas**.

b. Para cada regla de la lista, seleccione el botón de opción y revise el diagrama de retención para determinar si la regla utiliza el perfil de código de borrado que desea desactivar.

   En el ejemplo, la regla **tres sitio EC para objetos más grandes** utiliza un grupo de almacenamiento denominado **todos los 3 sitios** y el perfil de código de borrado **todos los sitios 6-3**. Los perfiles de código de borrado se representan con este icono: 



a. Si la regla de ILM utiliza el perfil de código de borrado que desea desactivar, determine si la regla se utiliza en la política de ILM activa o en una política propuesta.

   En el ejemplo, la regla **tres sitios EC para objetos más grandes** se utiliza en la política activa de ILM.

b. Complete los pasos adicionales de la tabla, según el lugar donde se utilice el perfil de código de borrado.

¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
No se usa nunca en ninguna regla de ILM	No se requieren pasos adicionales. Continúe con este procedimiento.	*Ninguno*
En una regla de ILM que nunca se haya usado en ninguna política de ILM	i. Edite o elimine todas las reglas de ILM afectadas. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. ii. Continúe con este procedimiento.	Trabaje con las reglas de ILM y las políticas de ILM

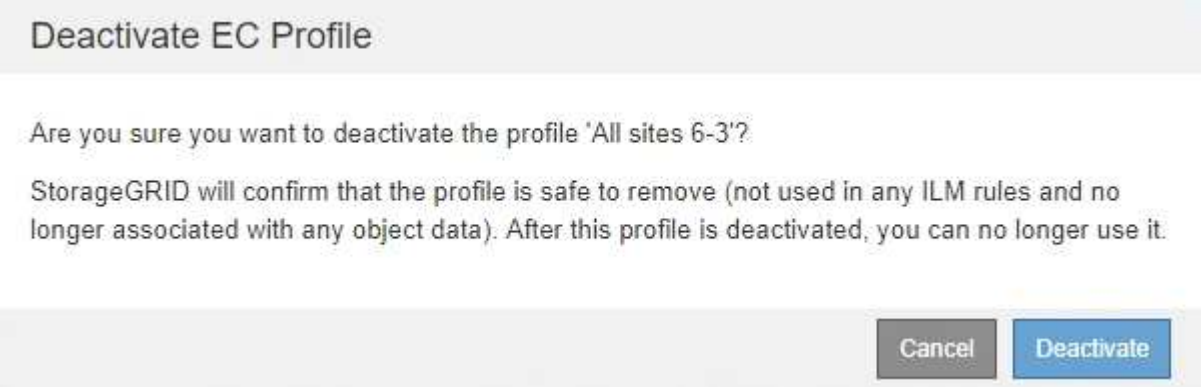
¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla de ILM que esté actualmente en la política activa de ILM	i. Clonar la política activa. ii. Quite la regla de ILM que utiliza el perfil de código de borrado. iii. Añada una o varias reglas nuevas de ILM para garantizar la protección de los objetos. iv. Guarde, simule y active la nueva directiva. v. Espere a que se aplique la nueva directiva y a que los objetos existentes se muevan a nuevas ubicaciones en función de las nuevas reglas que haya agregado. **Nota:** dependiendo del número de objetos y del tamaño de su sistema StorageGRID, las operaciones de ILM pueden tardar semanas o incluso meses en mover los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Aunque puede intentar desactivar de forma segura un perfil de código de borrado mientras sigue asociado con datos, la operación de desactivación fallará. Un mensaje de error le informará si el perfil aún no está listo para ser desactivado. vi. Edite o elimine la regla que ha eliminado de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. vii. Continúe con este procedimiento.	• Cree una política de ILM • Trabaje con las reglas de ILM y las políticas de ILM
En una regla de ILM que se encuentra actualmente en una política de ILM propuesta	i. Edite la directiva propuesta. ii. Quite la regla de ILM que utiliza el perfil de código de borrado. iii. Añada una o varias reglas nuevas de ILM para garantizar que todos los objetos estén protegidos. iv. Guarde la directiva propuesta. v. Edite o elimine la regla que ha eliminado de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. vi. Continúe con este procedimiento.	• Cree una política de ILM • Trabaje con las reglas de ILM y las políticas de ILM

¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla de ILM que está en una política histórica de ILM	i. Edite o elimine la regla. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. (La regla aparecerá ahora como una regla histórica en la política histórica.) ii. Continúe con este procedimiento.	Trabaje con las reglas de ILM y las políticas de ILM

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

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

   Aparece el cuadro de diálogo Desactivar perfil de EC.



5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.
   - Si StorageGRID puede desactivar el perfil de código de borrado, su estado será **desactivado**. Ya no puede seleccionar este perfil para ninguna regla de ILM.
   - Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto siguen asociados a este perfil. Es posible que deba esperar varias semanas antes de volver a intentar el proceso de desactivación.

Configurar regiones (opcional solo S3)

Las reglas de ILM pueden filtrar objetos en función de las regiones donde se crean bloques S3, lo que permite almacenar objetos de diferentes regiones en distintas ubicaciones de almacenamiento. Si desea usar una región de bloque de S3 como filtro de una regla, primero debe crear las regiones que pueden usar los bloques del sistema.

Lo que necesitará

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

Acerca de esta tarea

Al crear un bloque de S3, puede especificar que el bloque se cree en una región determinada. El establecimiento de una región permite que el bloque se aproxime geográficamente a los usuarios, lo que

ayuda a optimizar la latencia, minimizar los costes y cumplir con los requisitos normativos.

Cuando se crea una regla de ILM, se recomienda utilizar la región asociada con un bloque de S3 como filtro avanzado. Por ejemplo, puede diseñar una regla que solo se aplique a los objetos en cubos S3 creados en la región US-West-2. Luego, puede especificar que las copias de esos objetos se coloquen en nodos de almacenamiento en un centro de datos dentro de la región para optimizar la latencia.

Al configurar regiones, siga estas directrices:

- De forma predeterminada, se considera que todos los cucharones pertenecen a la región US-East-1.
- Debe crear las regiones mediante Grid Manager para poder especificar una región no predeterminada al crear cubos con el Administrador de inquilinos o la API de Gestión de inquilinos, o con el elemento de solicitud LocationConstraint para las solicitudes de la API PUT Bucket de S3. Se produce un error si una solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.
- Debe usar el nombre exacto de la región cuando cree el bloque de S3. Los nombres de región distinguen mayúsculas de minúsculas y deben contener al menos 2 caracteres y no más de 32. Los caracteres válidos son números, letras y guiones.

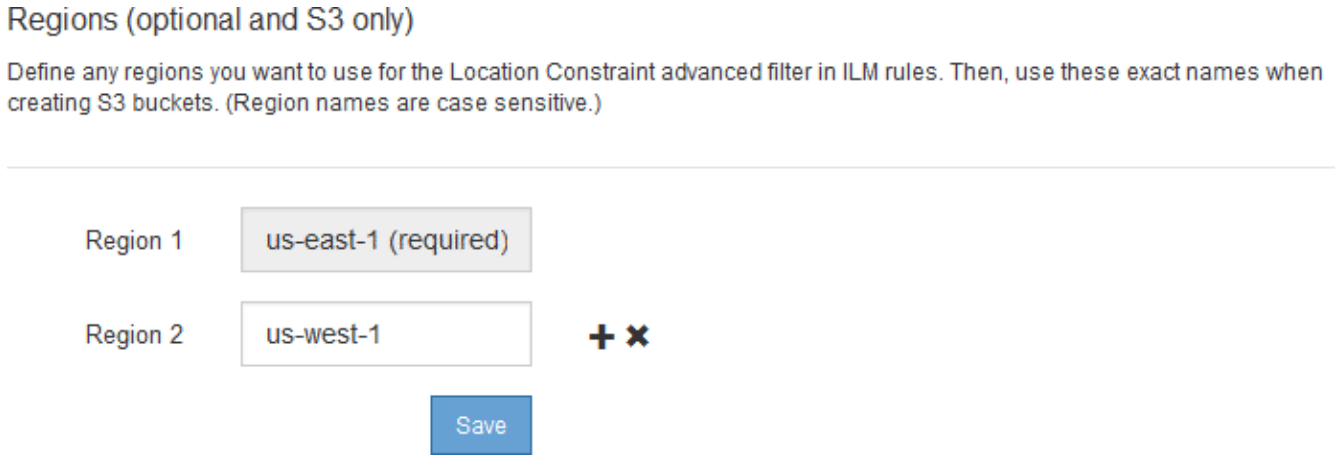
  No se considera que la UE sea un alias para la ue-oeste-1. Si desea utilizar la región UE o eu-West-1, debe usar el nombre exacto.

- No se puede eliminar ni modificar una región si actualmente se utiliza dentro de la política de ILM activa o la política de ILM propuesta.
- Si la región utilizada como filtro avanzado en una regla de ILM no es válida, todavía es posible agregar esa regla a la directiva propuesta. Sin embargo, se produce un error si intenta guardar o activar la directiva propuesta. (Una región no válida puede resultar si utiliza una región como filtro avanzado en una regla de ILM, pero después la elimina, o si utiliza la API de gestión de grid para crear una regla y especificar una región que no haya definido.)
- Si elimina una región después de utilizarla para crear un bloque de S3, deberá volver a agregar la región si alguna vez desea utilizar el filtro avanzado restricción de ubicaciones para buscar objetos en ese bloque.

Pasos

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

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

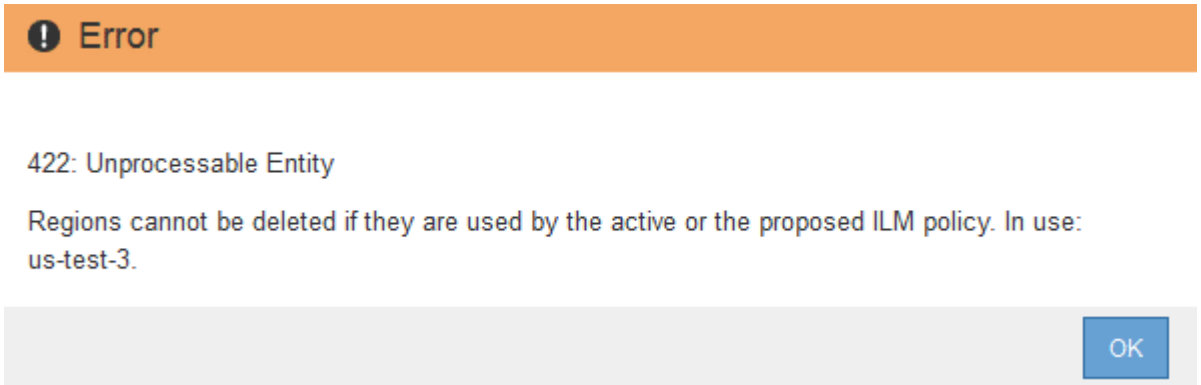
   

2. Para agregar una región:
   a. Seleccione el icono de inserción ➕ a la derecha de la última entrada.
   b. Introduzca el nombre de una región que desea utilizar al crear bloques de S3.

      Debe utilizar este nombre de región exacto como elemento de solicitud LocationConstraint al crear el bloque de S3 correspondiente.

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

   Aparece un mensaje de error si intenta eliminar una región que se utiliza actualmente en la directiva activa o la directiva propuesta.



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

   Ahora puede seleccionar estas regiones en la lista **restricción de ubicaciones** de la página filtro avanzado del asistente Crear regla ILM. ConsulteUsar filtros avanzados en las reglas de ILM.

Cree la regla de ILM

Acceda al asistente Create ILM Rule

Las reglas de ILM permiten gestionar la ubicación de los datos de objetos con el tiempo. Para crear una regla de ILM, debe usar el asistente Create ILM Rule.

> ⓘ Si crea la regla de ILM predeterminada para una política, utilice este procedimiento en su lugar: Cree una regla de ILM predeterminada.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Si desea especificar a qué cuentas de arrendatario se aplica esta regla, tiene el permiso Cuentas de arrendatario o conoce el ID de cuenta de cada cuenta.
- Si desea que la regla filtre objetos en los metadatos del último acceso, las actualizaciones de la hora del último acceso deben habilitarse en bloque para S3 o mediante contenedor para Swift.
- Si crea copias replicadas, debe configurar todos los pools de almacenamiento o los pools de almacenamiento en el cloud que planea utilizar. Consulte Cree el pool de almacenamiento y.. Cree el pool de almacenamiento en el cloud.

- Si crea copias con código de borrado, configuró un perfil de código de borrado. Consulte Cree un perfil de código de borrado.
- Usted está familiarizado con el opciones de protección de datos para consumo.
- Si necesita crear una regla conforme para usarla con el bloqueo de objetos S3, ya está familiarizado con la Requisitos para el bloqueo de objetos de S3.
- Opcionalmente, ha visto el vídeo: "Vídeo: Reglas de ILM para StorageGRID: Introducción".

Acerca de esta tarea

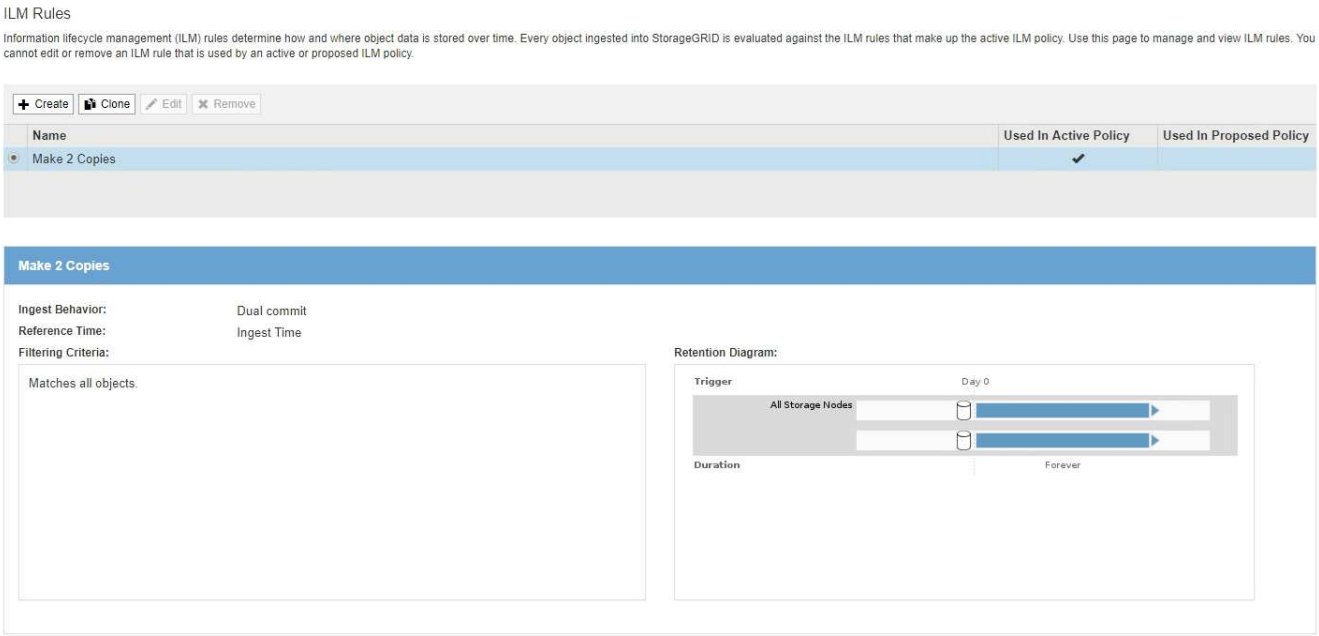
Al crear reglas de ILM:

- Considere la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Considere qué tipos de copias de objetos desea hacer (replicadas o codificadas por borrado) y el número de copias de cada objeto que se necesitan.
- Determinar qué tipos de metadatos de objetos se usan en las aplicaciones que se conectan al sistema StorageGRID. Las reglas de ILM filtran los objetos en función de sus metadatos.
- Considere dónde desea que las copias de objetos se coloquen a lo largo del tiempo.
- Decida qué opción se debe usar para la opción de protección de datos durante el procesamiento (equilibrado, estricto o Dual Commit).

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules, con la regla general, haga 2 copias, seleccionada.



La página ILM Rules tiene un aspecto ligeramente diferente si se habilitó la configuración global de bloqueo de objetos S3 para el sistema StorageGRID. La tabla de resumen incluye una columna **compatible** y los detalles de la regla seleccionada incluyen un campo **compatible**.

2. Seleccione **Crear**.

   Aparece el paso 1 (definir datos básicos) del asistente Crear regla de ILM. Utilice la página definir conceptos básicos para definir a qué objetos se aplica la regla.

Paso 1 de 3: Definir lo básico

El paso 1 (definir datos básicos) del asistente Crear regla de ILM permite definir los filtros básicos y avanzados de la regla.

Acerca de esta tarea

Al evaluar un objeto con una regla de 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 uno o más nombres de cuentas de arrendatario o de bloques, o filtros avanzados, como el tamaño del objeto o los metadatos de usuario.

Pasos

1. Introduzca un nombre único para la regla en el campo **Nombre**.

   Debe introducir entre 1 y 64 caracteres.

2. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.

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

Name	Make 3 Copies
Description	Save 1 copy at 3 sites for 1 year. Then, save EC copy forever

3. De manera opcional, seleccione una o varias cuentas de inquilino de S3 o Swift a las que se aplica esta regla. Si esta regla se aplica a todos los inquilinos, deje este campo en blanco.

   Si no dispone del permiso acceso raíz o de las cuentas de arrendatario, no podrá seleccionar arrendatarios en la lista. En su lugar, introduzca el ID de inquilino o introduzca varios ID como una cadena delimitada por comas.

4. De manera opcional, especifique los bloques de S3 o los contenedores Swift a los que se aplica esta regla.

   Si se selecciona **coincide con All** (valor predeterminado), la regla se aplica a todos los bloques S3 o contenedores Swift.

5. Opcionalmente, seleccione **filtrado 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.

   Si esta regla crea copias con código de borrado, agregue el filtro avanzado **Tamaño de objeto (MB)** y configúrelo en **mayor que 1**. El filtro de tamaño garantiza que los objetos de 1 MB o menos no se recodifiquen.

   > El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

6. Seleccione **Siguiente**.

   Aparece el paso 2 (definir ubicaciones).

Información relacionada

- Qué es una regla de ILM
- Usar filtros avanzados en las reglas de ILM
- Paso 2 de 3: Definir colocaciones

Usar filtros avanzados en las reglas de ILM

El filtrado avanzado permite crear reglas de ILM que se aplican solo a objetos específicos en función de sus metadatos. Al configurar el filtrado avanzado para una regla, debe seleccionar el tipo de metadatos que desea que coincidan, seleccionar un operador y especificar un valor de metadatos. Cuando se evalúan objetos, la regla de ILM se aplica solo a los objetos que tienen metadatos que coincidan con el filtro avanzado.

En la tabla se muestran los tipos de metadatos que se pueden especificar en los filtros avanzados, los operadores que se pueden utilizar para cada tipo de metadatos y los valores de metadatos esperados.

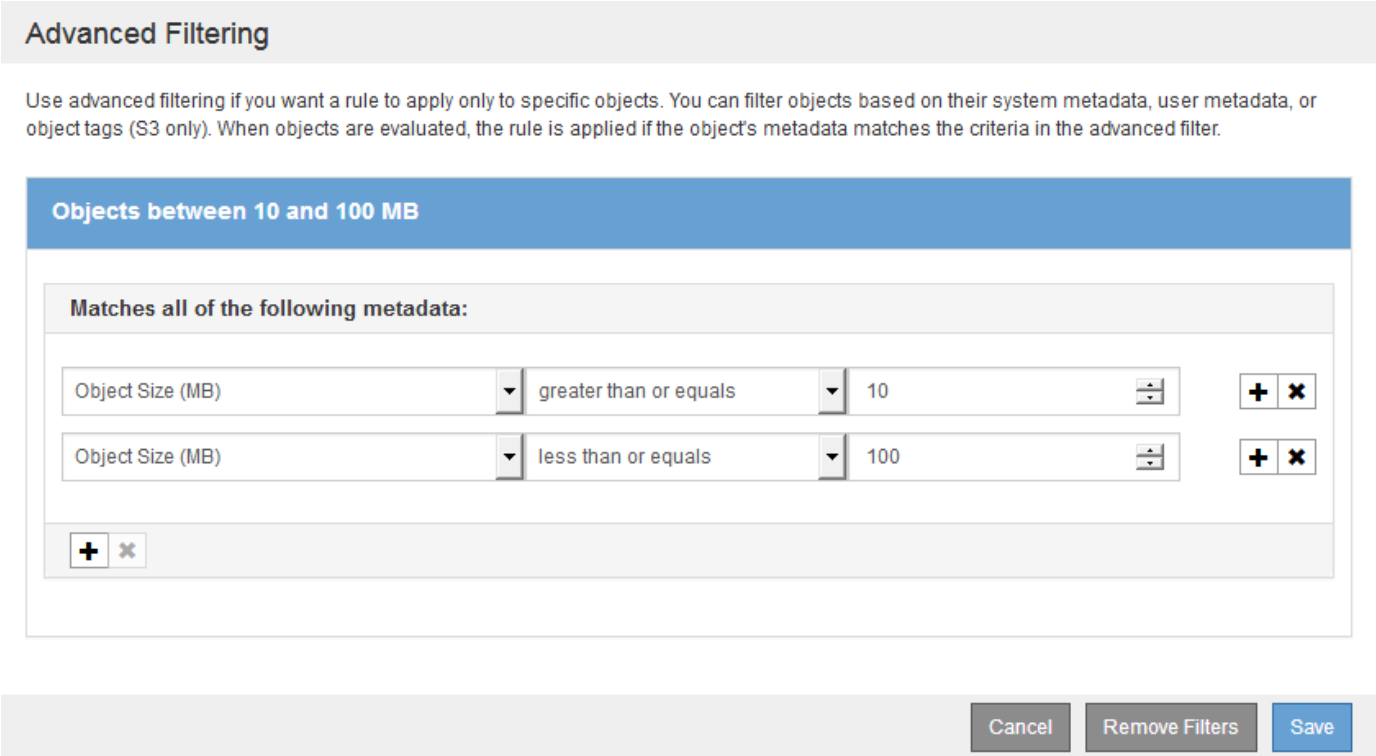
Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tiempo de consumo (microsegundos)	• es igual a • no es igual • menor que • menor que o igual • mayor que • mayor o igual que	Hora y fecha en la que se ingirió el objeto. **Nota:** para evitar problemas de recursos al activar una nueva política de ILM, puede utilizar el filtro avanzado de tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta como mayor o igual que el tiempo aproximado en el que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.
Clave	• es igual a • no es igual • contiene • no contiene • comienza con • no empieza por • termina con • no termina con	Todo o parte de una clave de objeto S3 o Swift única. Por ejemplo, quizás desee hacer coincidir los objetos que terminan con `.txt` o empiece por `test-object/`.
Hora del último acceso (microsegundos)	• es igual a • no es igual • menor que • menor que o igual • mayor que • mayor o igual que • existe • no existe	Hora y fecha en la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** Si planea utilizar la última hora de acceso como filtro avanzado, las actualizaciones de la última hora de acceso deben estar habilitadas para el contenedor S3 bucket o Swift. Utilice la hora del último acceso en las reglas de ILM
Limitación de ubicaciones (solo S3)	• es igual a • no es igual	Región en la que se creó un bloque de S3. Utilice **ILM** > **Regiones** para definir las regiones que se muestran. **Nota:** un valor de US-East-1 coincidirán con objetos en cubos creados en la región US-East-1 así como con objetos en cubos que no tienen una región especificada. Configurar regiones (opcional solo S3)

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tamaño del objeto (MB)	• es igual a • no es igual • menor que • menor que o igual • mayor que • mayor o igual que	Tamaño del objeto en MB. El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño. **Nota:** para filtrar en tamaños de objeto menores de 1 MB, escriba un valor decimal. El tipo de navegador y la configuración regional controlan si necesita utilizar un punto o una coma como separador decimal.
Metadatos del usuario	• contiene • termina con • es igual a • existe • no contiene • no termina con • no es igual • no existe • no empieza por • comienza con	Par clave-valor, donde **Nombre de metadatos de usuario** es la clave y **valor de metadatos de usuario** es el valor. Por ejemplo, para filtrar objetos con metadatos de usuario de `color=blue`, especifique `color` Para **Nombre de metadatos de usuario**, `equals` para el operador, y. `blue` Para **valor de metadatos de usuario**. **Nota:** los nombres de metadatos del usuario no distinguen entre mayúsculas y minúsculas; los valores de metadatos del usuario distinguen entre mayúsculas y minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual a • existe • no contiene • no termina con • no es igual • no existe • no empieza por • comienza con	Par clave-valor, donde **Nombre de etiqueta de objeto** es la clave y **valor de etiqueta de objeto** es el valor. Por ejemplo, para filtrar objetos que tienen una etiqueta de objeto de `Image=True`, especifique `Image` Para **Nombre de etiqueta de objeto**, `equals` para el operador, y. `True` Para **valor de etiqueta de objeto**. **Nota:** los nombres de las etiquetas de objeto y los valores de las etiquetas de objeto distinguen entre mayúsculas y minúsculas. Debe introducir estos elementos exactamente como se definieron para el objeto.

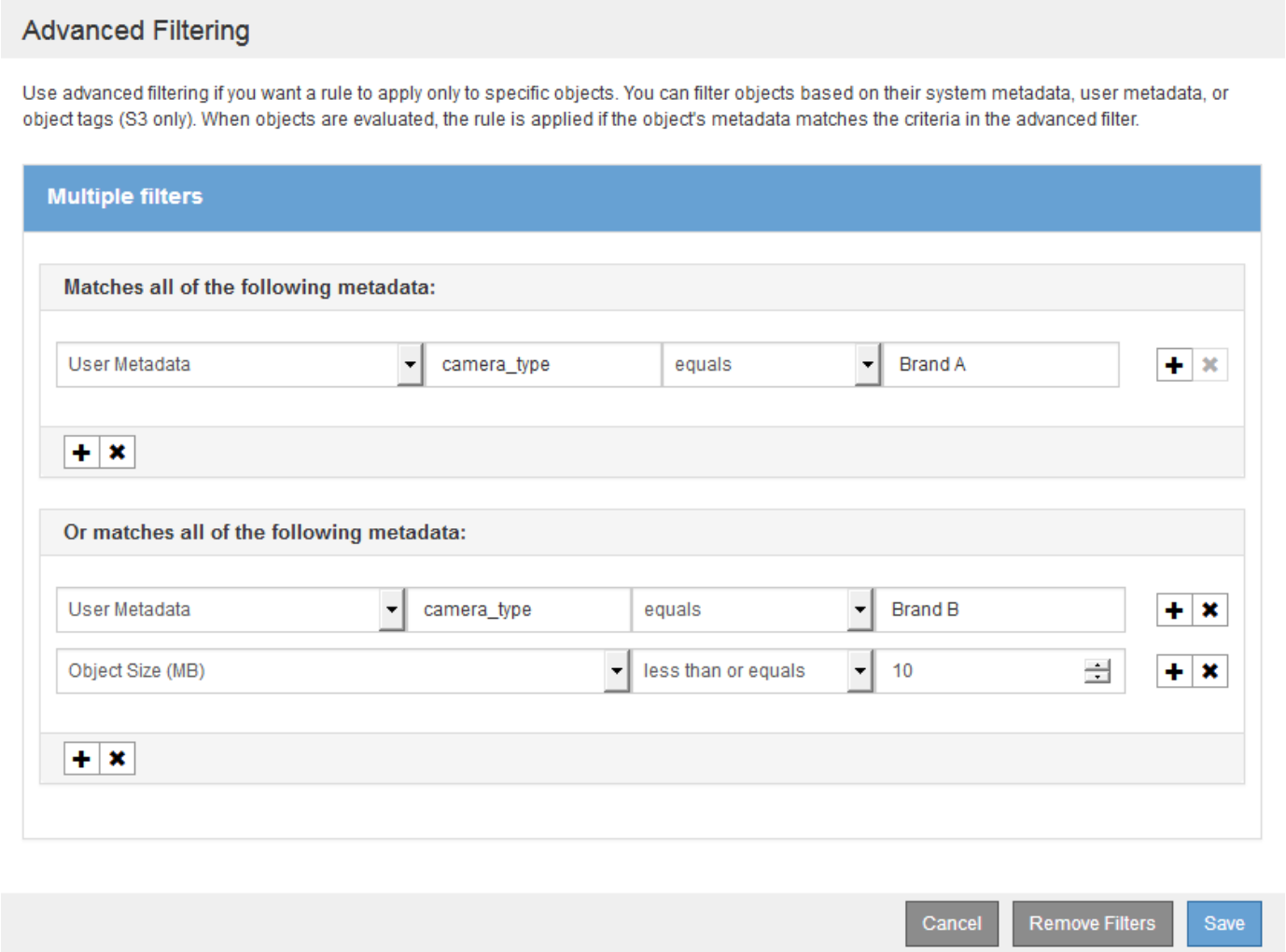
Especifique varios tipos de metadatos y valores

Al definir un filtrado avanzado, es posible especificar varios tipos de metadatos y varios valores de metadatos. Por ejemplo, si desea que una regla coincida con objetos de entre 10 MB y 100 MB de tamaño, debe seleccionar el tipo de metadatos **Tamaño de 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 inferiores o iguales a 100 MB.



El uso de múltiples entradas permite tener un control preciso sobre qué objetos coinciden. En el ejemplo siguiente, la regla se aplica a los objetos que tienen una Marca A o una Marca B como valor de los metadatos de usuario camera_TYPE. Sin embargo, la regla sólo se aplica a los objetos de Marca B que son menores de 10 MB.



Paso 2 de 3: Definir colocaciones

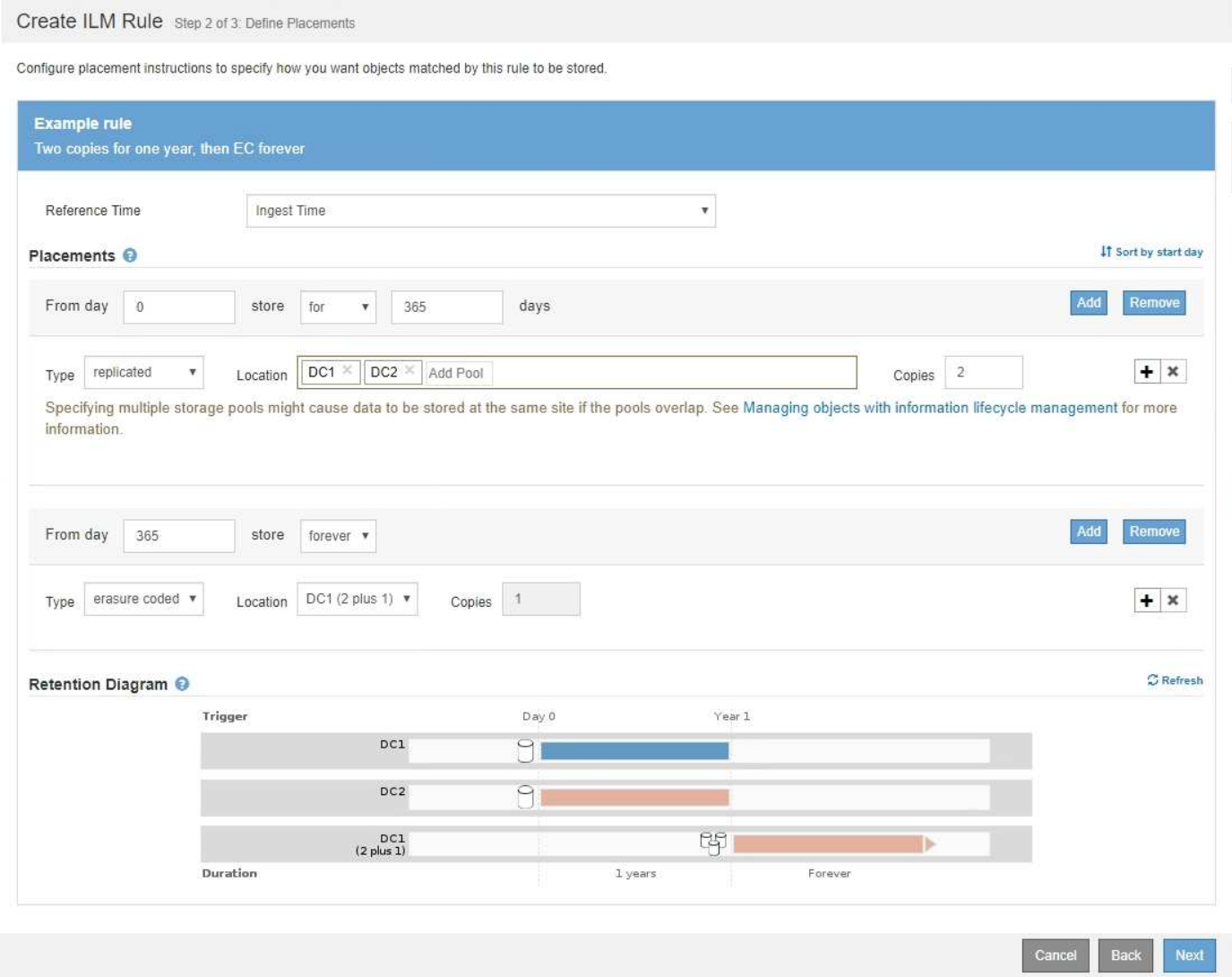
El paso 2 (definir ubicaciones) del asistente para crear regla de ILM permite definir las instrucciones de ubicación que determinan la cantidad de objetos que se almacenan, el tipo de copias (replicadas o codificadas para borrado), la ubicación del almacenamiento y el número de copias.

Acerca de esta tarea

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

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

Esta regla de ILM de ejemplo crea dos copias replicadas para el primer año. Cada copia se guarda en una agrupación de almacenamiento de un sitio diferente. Después de un año, se realiza y se guarda una copia con código de borrado al 2+1 en una sola instalación.



Pasos

1. En **tiempo de referencia**, seleccione el tipo de tiempo que se utilizará al calcular la hora de inicio de una instrucción de colocación.

Opción	Descripción
Tiempo de ingesta	Hora a la que se ingirió el objeto.
Hora del último acceso	Hora a la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** para utilizar esta opción, las actualizaciones de la hora de último acceso deben estar habilitadas para el contenedor S3 bucket o Swift. Consulte Utilice la hora del último acceso en las reglas de ILM.

Opción	Descripción
Hora no actual	El tiempo que una versión de objeto se volvió no actual porque se ingirió una nueva versión y la reemplazó como la versión actual. **Nota:** el tiempo no corriente se aplica sólo a los objetos S3 en bloques habilitados para versionado. Puede utilizar esta opción para reducir el impacto del almacenamiento de objetos con versiones mediante el filtrado de versiones de objetos no actuales. Consulte Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3.
Hora de creación definida por el usuario	Hora especificada en los metadatos definidos por el usuario.

> Si desea crear una regla compatible, debe seleccionar **tiempo de procesamiento**.

2. En la sección **colocaciones**, seleccione un tiempo 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 ("días 0 durante 365 días"). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:
   a. En la lista desplegable **Tipo**, seleccione **replicado**.
   b. En el campo **ubicación**, seleccione **Agregar pool** para cada pool de almacenamiento que desee agregar.

      Si especifica sólo un pool de almacenamiento, tenga en cuenta que StorageGRID sólo puede almacenar una copia replicada de un objeto en un nodo de almacenamiento dado. Si su grid incluye tres nodos de almacenamiento y selecciona 4 como el número de copias, solo se realizarán tres copias: Una copia para cada nodo de almacenamiento.

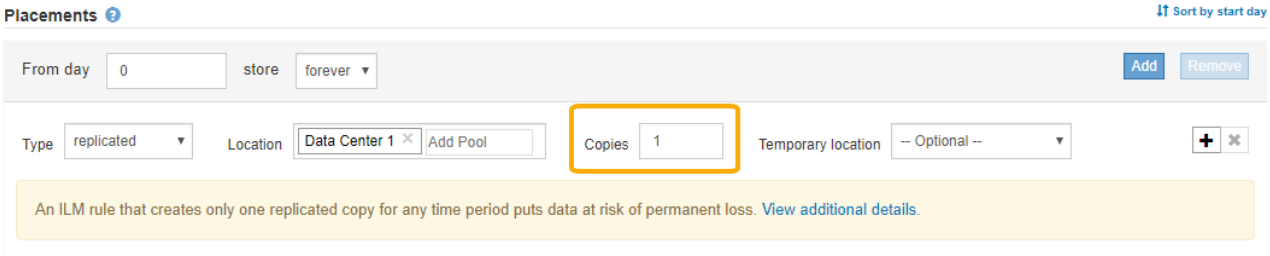
      > Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

      Si especifica más de una agrupación de almacenamiento, tenga en cuenta estas reglas:

      - La cantidad de copias no puede ser mayor que la cantidad de pools de almacenamiento.
      - Si el número de copias es igual al número de pools de almacenamiento, se almacena una copia del objeto en cada pool de almacenamiento.
      - Si el número de copias es inferior al número de pools de almacenamiento, se almacena una copia en el sitio de procesamiento y, a continuación, el sistema distribuye las copias restantes para mantener el uso del disco entre los pools equilibrados, a la vez que se garantiza que ningún sitio obtenga más de una copia de un objeto.
      - Si los pools de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden en un solo sitio. Por este motivo, no especifique el pool de almacenamiento predeterminado todos los nodos de almacenamiento y otro pool de almacenamiento.

c. Seleccione el número de copias que desea realizar.

   Aparecerá una advertencia si cambia el número de copias a 1. Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Consulte Por qué no se debe utilizar la replicación de copia única.



   Para evitar estos riesgos, siga uno o varios de estos procedimientos:

   - Aumentar el número de copias durante el período de tiempo.
   - Seleccione el icono de signo más ➕ para crear copias adicionales durante el período de tiempo. A continuación, seleccione un pool de almacenamiento diferente o un pool de almacenamiento cloud.
   - Seleccione **Código de borrado** para Tipo, en lugar de **replicado**. Puede ignorar con toda tranquilidad esta advertencia si esta regla ya crea varias copias para todos los períodos de tiempo.

d. Si ha especificado sólo una agrupación de almacenamiento, ignore el campo **ubicación temporal**.

   > ⓘ Las ubicaciones temporales están obsoletas y se eliminarán en un lanzamiento futuro. Consulte Usar un pool de almacenamiento como ubicación temporal (obsoleto).

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

   a. En la lista desplegable **Tipo**, seleccione **Código de borrado**.

      El número de copias cambia a 1. Aparece una advertencia si la regla no tiene un filtro avanzado para ignorar objetos de 200 KB o menos.

      > Erasure coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to any value greater than 0.2.

      > ⓘ El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

   b. Si aparece la advertencia de tamaño de objeto, seleccione **Atrás** para volver al paso 1. A continuación, seleccione **filtrado avanzado** y establezca el filtro Tamaño del objeto (MB) en cualquier valor superior a 0.2.

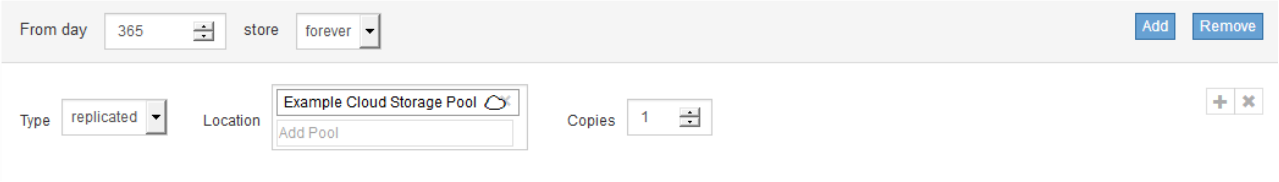
c. Seleccione la ubicación de almacenamiento.

La ubicación de almacenamiento de una copia codificada con borrado incluye el nombre del pool de almacenamiento seguido del nombre del perfil de la codificación de borrado.

5. Si lo desea, puede agregar periodos de tiempo diferentes o crear copias adicionales en diferentes ubicaciones:
   - Seleccione el icono más para crear copias adicionales en una ubicación diferente durante el mismo período de tiempo.
   - Seleccione **Agregar** para agregar un período de tiempo diferente a las instrucciones de colocación.

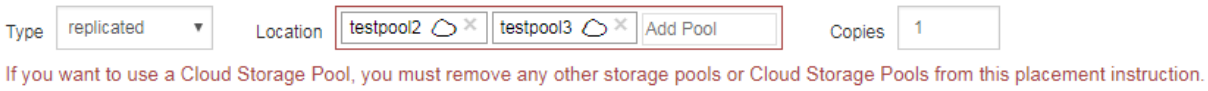
> Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que el período de tiempo final finalice con **para siempre**.

6. Si desea almacenar objetos en un pool de almacenamiento en cloud:
   a. En la lista desplegable **Tipo**, seleccione **replicado**.
   b. En el campo **ubicación**, seleccione **Agregar grupo**. A continuación, seleccione un pool de almacenamiento en el cloud.

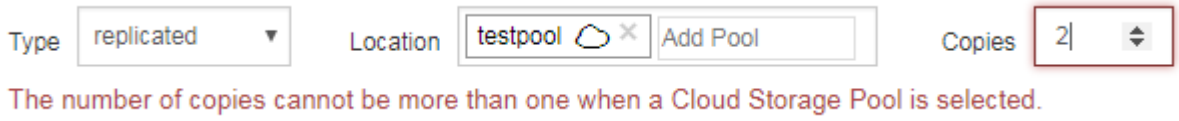


Cuando utilice Cloud Storage Pools, tenga en cuenta estas reglas:

- No puede seleccionar más de un pool de almacenamiento en cloud mediante una única instrucción de colocación. De forma similar, no puede seleccionar un pool de almacenamiento en cloud ni un pool de almacenamiento en la misma instrucción de ubicación.

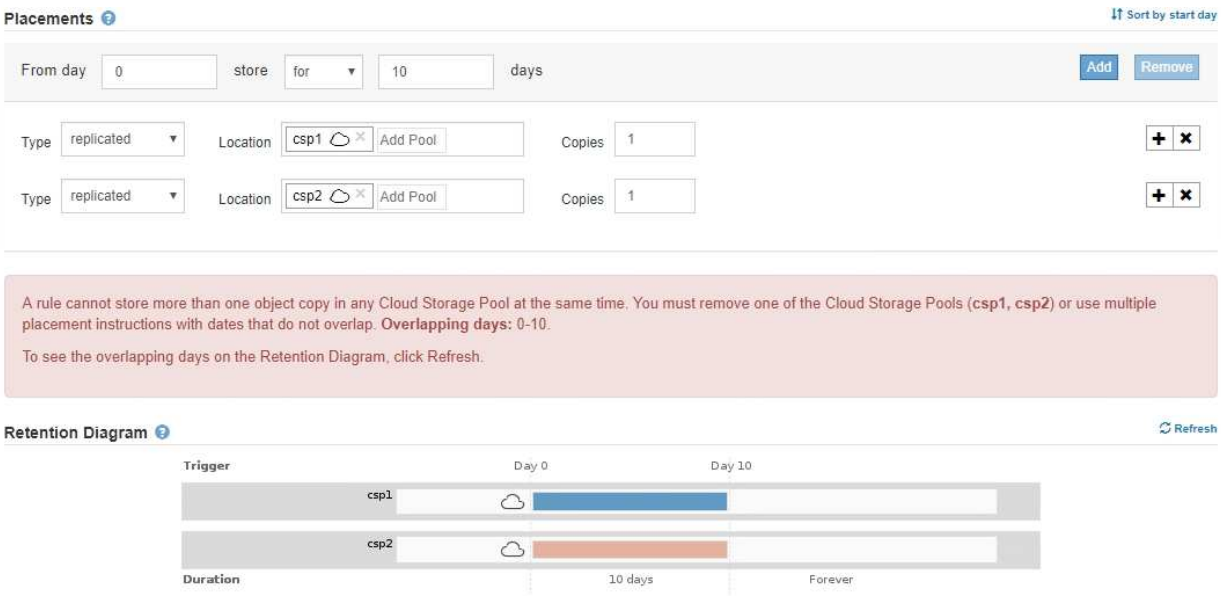


- Solo puede almacenar una copia de un objeto en cualquier Cloud Storage Pool en concreto. Aparece un mensaje de error si configura **copias** en 2 o más.

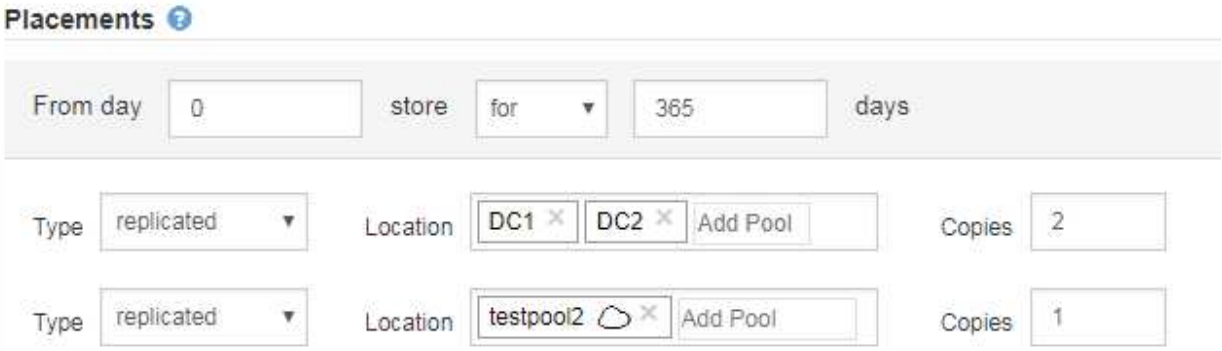


- No puede almacenar más de una copia de objetos en ningún pool de almacenamiento en cloud al mismo tiempo. Aparecerá un mensaje de error si varias ubicaciones que utilizan un Cloud Storage

Pool tienen fechas superpuestas o si varias líneas en la misma ubicación utilizan un Cloud Storage Pool.



- Puede almacenar un objeto en un pool de almacenamiento en cloud al mismo tiempo que el objeto se almacena como copias replicadas o codificadas de borrado en StorageGRID. Sin embargo, como se muestra en este ejemplo, debe incluir más de una línea en la instrucción de colocación para el período de tiempo, de modo que pueda especificar el número y los tipos de copias para cada ubicación.



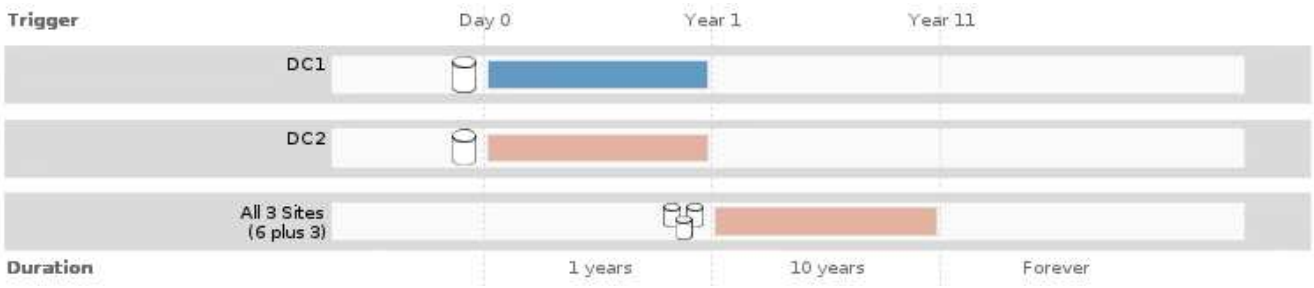
7. Seleccione **Actualizar** para actualizar el Diagrama de retención y confirmar las instrucciones de colocación.

   Cada línea del diagrama muestra dónde y cuándo se colocarán las copias de objeto. El tipo de copia está representado por uno de los siguientes iconos:

	Copia replicada
	Copia con código de borrado
	Copia de Cloud Storage Pool

   En este ejemplo, se guardarán dos copias replicadas en dos agrupaciones de almacenamiento (DC1 y DC2) durante un año. A continuación, se guardará una copia codificada con borrado durante 10 años

adicionales utilizando un esquema de codificación de borrado de 6+3 en tres ubicaciones. Transcurridos 11 años, los objetos se eliminarán de StorageGRID.



8. Seleccione **Siguiente**.

   Aparece el paso 3 (definir comportamiento de procesamiento).

Información relacionada

- Qué es una regla de ILM
- Gestione objetos con S3 Object Lock
- Paso 3 de 3: Definir el comportamiento de la ingesta

Utilice la hora del último acceso en las reglas de ILM

Puede usar la hora de Last Access como hora de referencia en una regla de ILM. Por ejemplo, quizás desee dejar objetos que se han visto en los últimos tres meses en nodos de almacenamiento local, mientras mueve objetos que no se han visto recientemente a una ubicación externa. También puede usar la hora de última acceso como filtro avanzado si desea que una regla de ILM se aplique sólo a los objetos a los que se accedió por última vez en una fecha determinada.

Acerca de esta tarea

Antes de utilizar la hora del último acceso en una regla de ILM, revise las siguientes consideraciones:

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

  Tenga en cuenta esta latencia al crear reglas de ILM basadas en el tiempo del último acceso y evite ubicaciones que usan breves periodos de tiempo (menos de un mes).

- Cuando se utiliza la hora de última acceso como filtro avanzado o como hora de referencia, debe habilitar actualizaciones del último tiempo de acceso para bloques S3. Se puede usar el Administrador de inquilinos o la API de gestión de inquilinos.

  > Las actualizaciones del último tiempo de acceso siempre están habilitadas para contenedores Swift, pero están deshabilitadas de forma predeterminada en bloques S3.

> Tenga en cuenta que habilitar las actualizaciones del tiempo de último 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 marcas de tiempo nuevas cada vez que se recuperan los objetos.

En la tabla siguiente se resume si se actualiza la hora del último acceso para todos los objetos del bloque para los diferentes tipos de peticiones.

Tipo de solicitud	Si la hora de último acceso se actualiza cuando se desactivan las actualizaciones de la última hora de acceso	Si la hora de último acceso se actualiza cuando se activan las actualizaciones de la última hora de 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
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Información relacionada

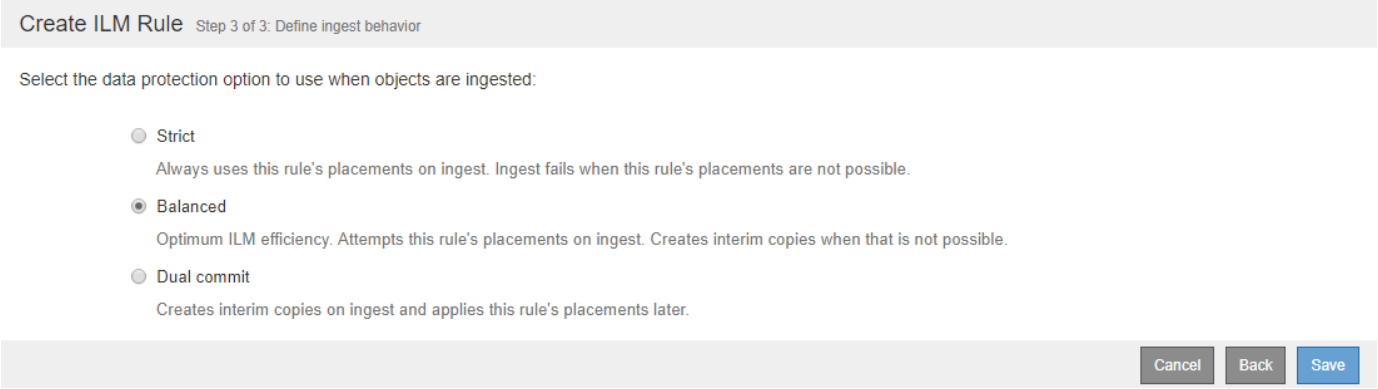
- Use S3
- Usar una cuenta de inquilino

Paso 3 de 3: Definir el comportamiento de la ingesta

El paso 3 (definir comportamiento de la ingesta) del asistente Crear regla de ILM permite elegir cómo se protegen los objetos filtrados por esta regla mientras se ingieren.

Acerca de esta tarea

StorageGRID puede hacer copias provisionales y poner en cola los objetos para la evaluación de ILM más tarde, o puede hacer copias para cumplir las instrucciones de colocación de la regla de forma inmediata.



Pasos

1. Seleccione la opción de protección de datos que se va a utilizar cuando se ingieren los objetos:

Opción	Descripción
Estricto	Siempre utiliza las colocaciones de esta regla durante el procesamiento. La ingesta falla cuando las colocaciones de esta regla no son posibles.
Equilibrado	Eficiencia óptima de ILM. Intenta colocar esta regla en el procesamiento. Crea copias provisionales cuando eso no es posible.
Registro doble	Crea copias provisionales en el procesamiento y aplica las colocaciones de esta regla más adelante.

   Balance ofrece una combinación de seguridad de datos y eficiencia que es adecuada en la mayoría de los casos. La confirmación estricta o doble se utiliza generalmente para satisfacer requisitos específicos.

   Consulte Opciones de protección de datos para consumo y.. Ventajas, inconvenientes y limitaciones de las opciones de protección de datos si quiere más información.

   > Aparece un mensaje de error si selecciona la opción estricta o equilibrada y la regla utiliza una de estas ubicaciones:
   >
   > - Un pool de almacenamiento en cloud desde el día 0
   > - Un nodo de archivado al día 0
   > - Un pool de almacenamiento en cloud o un nodo de archivado cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia

2. Seleccione **Guardar**.

   Se guarda la regla ILM. La regla no estará activa hasta que se agregue a una política de ILM y esa política se active.

Información relacionada

- Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto
- Cree una política de ILM

Cree una regla de ILM predeterminada

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

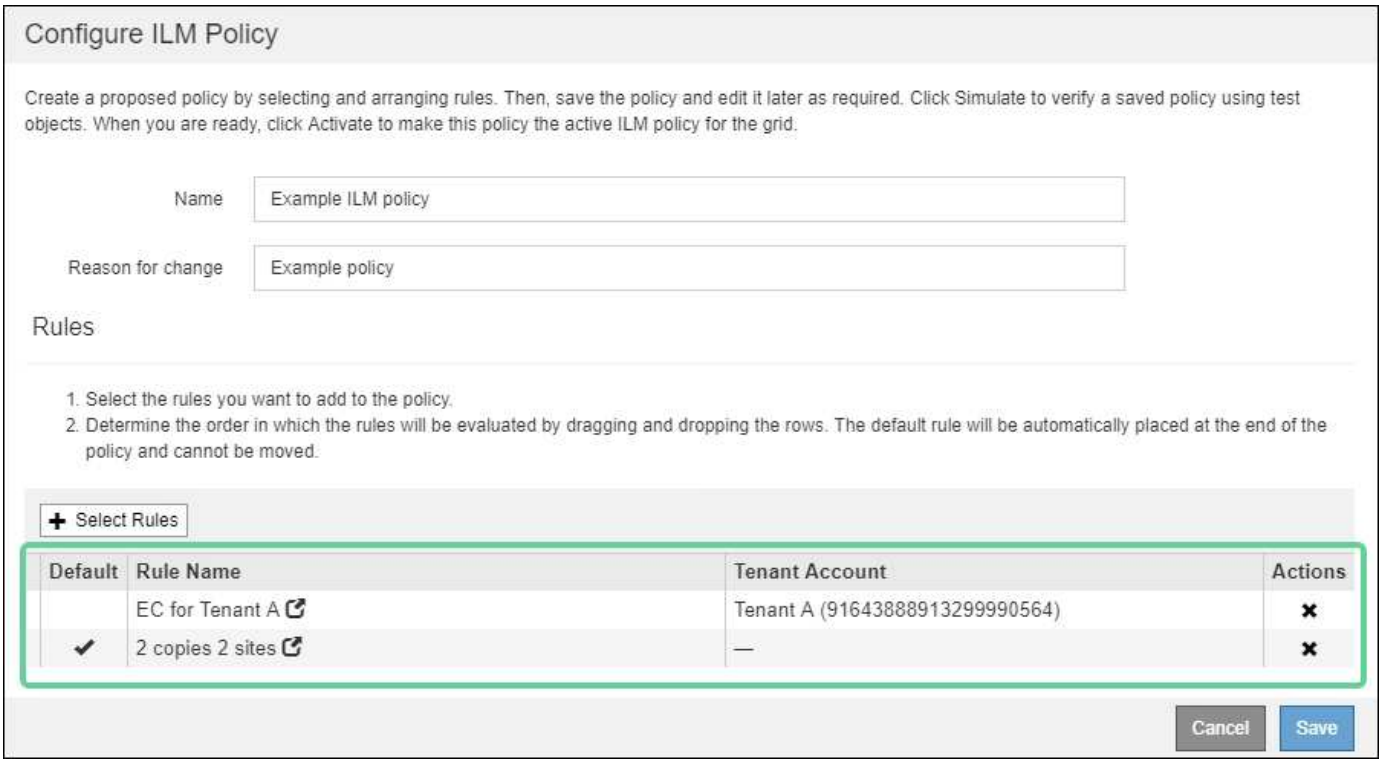
Lo que necesitará

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

Acerca de esta tarea

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

En esta política de ejemplo, la primera regla se aplica sólo a los objetos que pertenecen al arrendatario A. La regla predeterminada, que es última, se aplica a los objetos que pertenecen a todas las demás cuentas de arrendatario.



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

- La regla predeterminada se coloca automáticamente como última regla en la directiva.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones de objeto, por lo que no puede utilizar la hora de referencia no corriente.
- La regla predeterminada debe 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 deberían utilizar un filtro avanzado para evitar que los objetos más pequeños se codificen con el borrado.

- En general, la regla predeterminada debería retener objetos para siempre.
- Si está utilizando (o tiene previsto habilitar) la configuración de bloqueo de objetos global S3, la regla predeterminada para la directiva activa o propuesta debe ser compatible.

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules.

2. Seleccione **Crear**.

   Aparece el paso 1 (definir datos básicos) del asistente Crear regla de ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre**.
4. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.
5. Deje el campo **Cuentas de inquilino** en blanco.

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

6. Deje en blanco el campo **Nombre de bloque**.

   La regla predeterminada debe aplicarse a todos los bloques de S3 y contenedores Swift.

7. No seleccione **filtrado avanzado**

   La regla predeterminada no puede especificar ningún filtro.

8. Seleccione **Siguiente**.

   Aparece el paso 2 (definir ubicaciones).

9. Para tiempo de referencia, seleccione cualquier opción excepto **tiempo no corriente**.

   La regla predeterminada debe aplicar todas las versiones del objeto.

10. Especifique las instrucciones de colocación para la regla predeterminada.
    - La regla predeterminada debería retener objetos para siempre. Aparece una advertencia cuando activa una nueva directiva si la regla predeterminada no conserva objetos para siempre. Debe confirmar que éste es el comportamiento que espera.
    - La regla predeterminada debe 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 **Tamaño de objeto (MB) superior al 0.2** avanzado para evitar que los objetos más pequeños se codifican con el borrado.

    - Si está utilizando (o tiene previsto habilitar) la configuración global de bloqueo de objetos S3, la regla predeterminada debe ser compatible:

- Debe crear al menos dos copias de objetos replicados o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante todo el tiempo que dure cada línea en las instrucciones de colocación.
- Las copias de objetos no se pueden guardar en un pool de almacenamiento en cloud.
- Las copias de objetos no se pueden guardar en los nodos de archivado.
- Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, utilizando el tiempo de procesamiento como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación deberá ser «'para siempre».

11. Seleccione **Actualizar** para actualizar el Diagrama de retención y confirmar las instrucciones de colocación.
12. Seleccione **Siguiente**.

    Aparece el paso 3 (definir comportamiento de procesamiento).

13. Seleccione la opción de protección de datos que se va a utilizar cuando se ingieren objetos y seleccione **Guardar**.

Cree una política de ILM

Cree una política de ILM: Descripción general

Al crear una política de ILM, para comenzar, debe seleccionar y organizar las reglas de ILM. A continuación, se comprueba el comportamiento de la directiva propuesta simulándola de objetos ingeridos previamente. Cuando esté satisfecho de que la directiva propuesta funcione según lo previsto, puede activarla para crear la directiva activa.

> Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Consideraciones que tener en cuenta para crear una política de ILM

- Utilice la política integrada del sistema, la directiva de copias base 2, sólo en sistemas de prueba. La regla hacer 2 copias de esta política utiliza el pool 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.
- Al diseñar una nueva política, tenga en cuenta todos los diferentes tipos de objetos que se podrían procesar en el grid. Asegúrese de que la política incluye reglas para coincidir y colocar estos objetos según sea necesario.
- Mantenga la política de ILM de la forma más sencilla posible. Esto evita situaciones potencialmente peligrosas en las que los datos de objetos no se protegen como se deben realizar cambios en el sistema StorageGRID a lo largo del tiempo.
- Asegúrese de que las reglas de la política están en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior. Por ejemplo, si la primera regla de una política coincide con un objeto, dicha regla no será evaluada por

ninguna otra regla.

- La última regla de todas las políticas de ILM es la regla predeterminada de ILM, que no puede usar ningún filtro. Si un objeto no ha sido coincidente con otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se retiene.
- Antes de activar una nueva política, revise los cambios que realice la política en la ubicación de objetos existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Cree una política de ILM propuesta

Puede crear una política de ILM propuesta desde cero o clonar la política activa actual si desea empezar con el mismo conjunto de reglas.

> Si se habilitó el ajuste global de bloqueo de objetos S3, utilice este procedimiento en su lugar: Cree una política de ILM después de habilitar el bloqueo de objetos de S3.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha creado las reglas de ILM que desea añadir a la política propuesta. Según sea necesario, puede guardar una directiva propuesta, crear reglas adicionales y, a continuación, editar la directiva propuesta para agregar las nuevas reglas.
- Ya tienes Se ha creado una regla de ILM predeterminada para la directiva que no contiene ningún filtro.
- Opcionalmente, ha visto el vídeo: "Vídeo: Políticas de ILM de StorageGRID"

Acerca de esta tarea

Algunos de los motivos típicos para crear una política de ILM propuesta son:

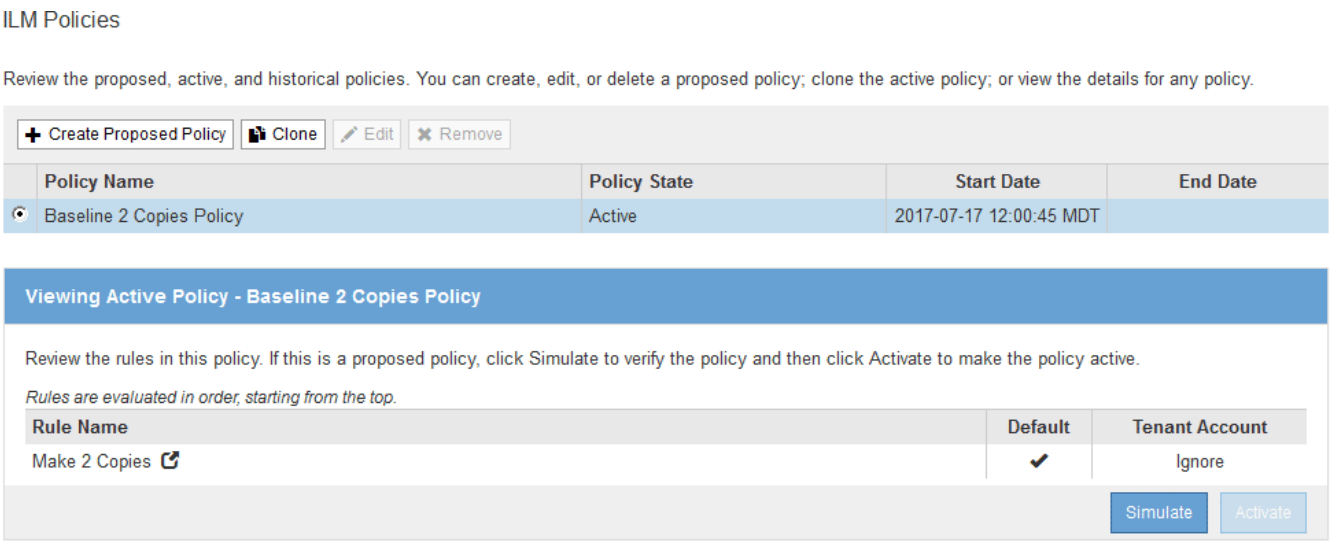
- Ha añadido un sitio nuevo y debe utilizar nuevas reglas de ILM para colocar objetos en dicho sitio.
- Se está decomisionando un sitio y es necesario eliminar todas las reglas que hacen referencia al sitio.
- Se ha agregado un nuevo inquilino que tiene requisitos especiales de protección de datos.
- Comenzó a utilizar un pool de almacenamiento en el cloud.

Utilice la política integrada del sistema, la directiva de copias base 2, sólo en sistemas de prueba. La regla hacer 2 copias de esta política utiliza el pool 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.

Pasos

1. Seleccione **ILM** > **políticas**.

   Aparece la página ILM Policies. En esta página puede revisar la lista de políticas propuestas, activas e históricas; crear, editar, o elimine una política propuesta; clone la política activa o vea los detalles de cualquier política.

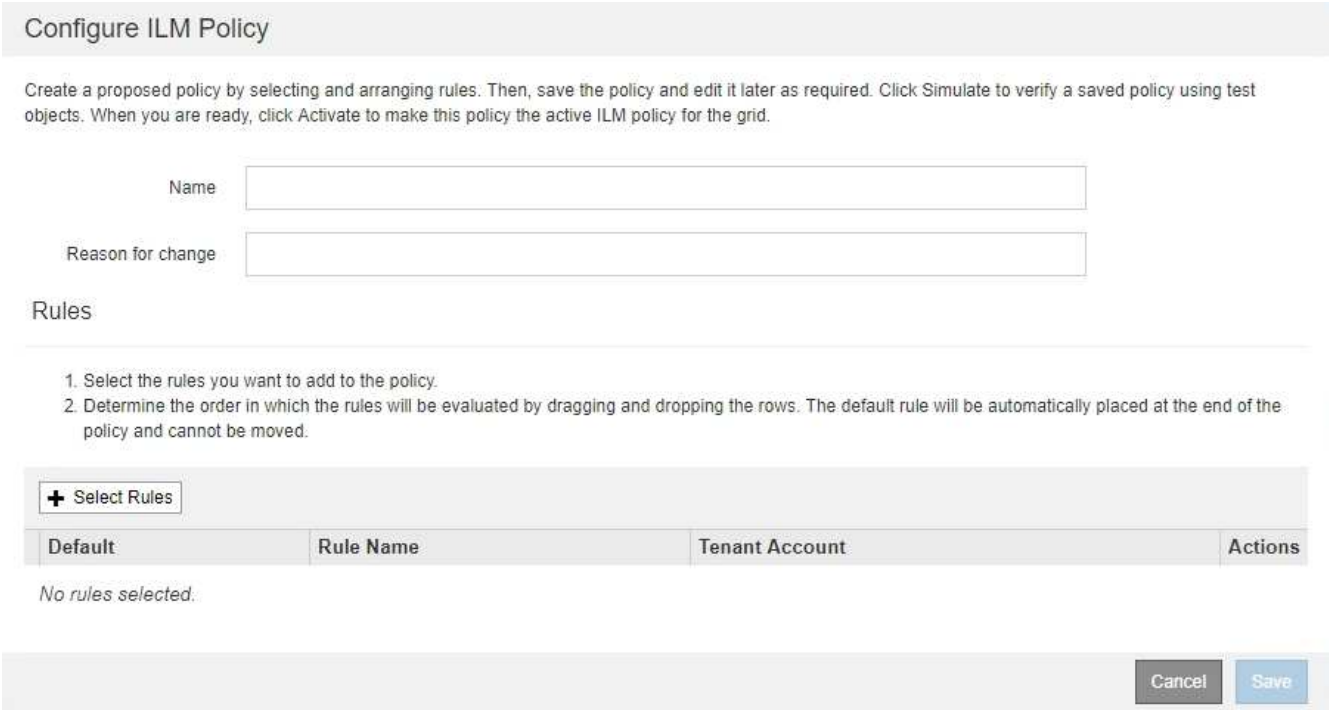


2. Determine cómo desea crear la política de ILM propuesta.

Opción	Pasos
Cree una nueva directiva propuesta que no tenga reglas ya seleccionadas	a. Si actualmente existe una política ILM propuesta, seleccione esa política y seleccione **Quitar**. No puede crear una nueva directiva propuesta si ya existe una propuesta. b. Seleccione **Crear directiva propuesta**.
Crear una directiva propuesta basada en la política activa	a. Si actualmente existe una política ILM propuesta, seleccione esa política y seleccione **Quitar**. No puede clonar la política activa si ya existe una política propuesta. b. Seleccione la directiva activa de la tabla. c. Seleccione **Clonar**.
Edite la directiva propuesta existente	a. Seleccione la directiva propuesta en la tabla. b. Seleccione **Editar**.

Se muestra el cuadro de diálogo Configurar política de ILM.

Si va a crear una nueva directiva propuesta, todos los campos estarán en blanco y no se seleccionará ninguna regla.



Si va a clonar la directiva activa, el campo **Nombre** muestra el nombre de la directiva activa, adjunto por un número de versión ("'v2'" en el ejemplo). Las reglas utilizadas en la directiva activa se seleccionan y se muestran en su orden actual.

3. Introduzca un nombre único para la directiva propuesta en el campo **Nombre**.

   Debe introducir al menos 1 y no más de 64 caracteres. Si clona la política activa, puede utilizar el nombre actual con el número de versión añadido o puede introducir un nuevo nombre.

4. Introduzca el motivo por el que está creando una nueva directiva propuesta en el campo **motivo del cambio**.

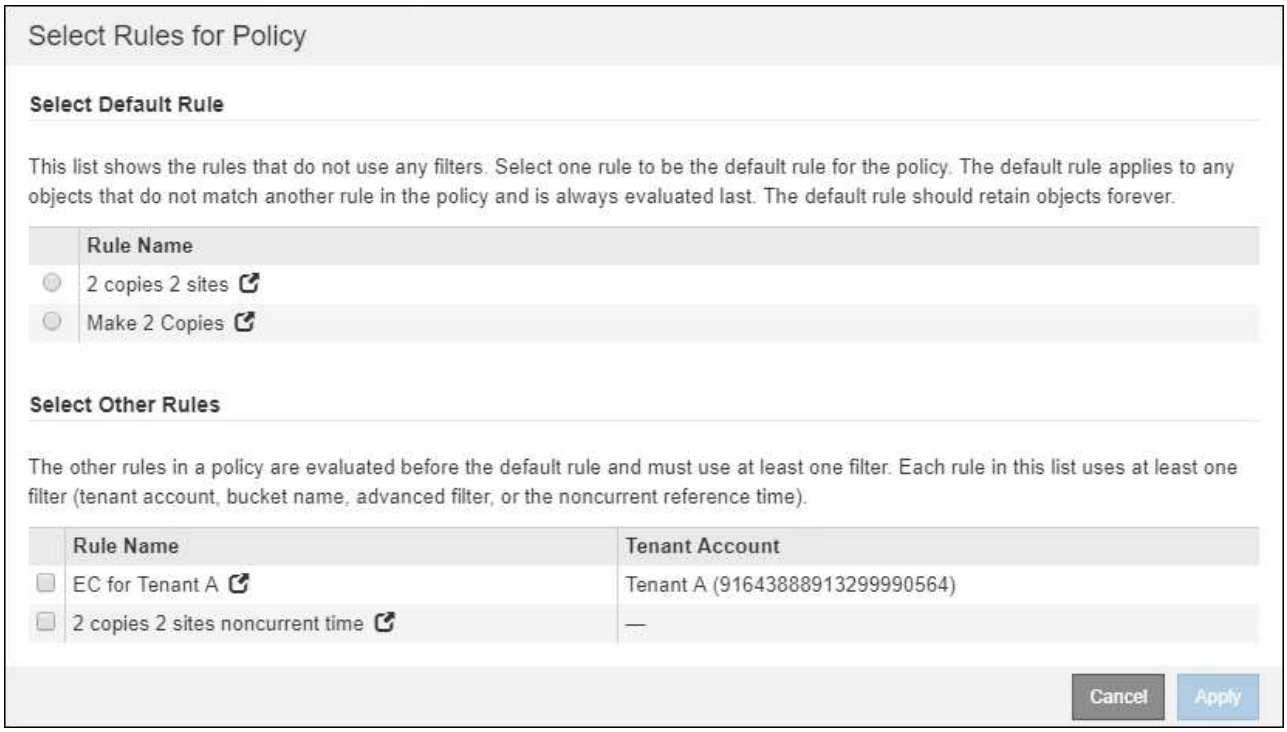
   Debe introducir al menos 1 y no más de 128 caracteres.

5. Para agregar reglas a la directiva, seleccione **Seleccionar reglas**.

   Aparece el cuadro de diálogo Seleccionar reglas para la directiva, con todas las reglas definidas en la lista. Si está clonando una política:

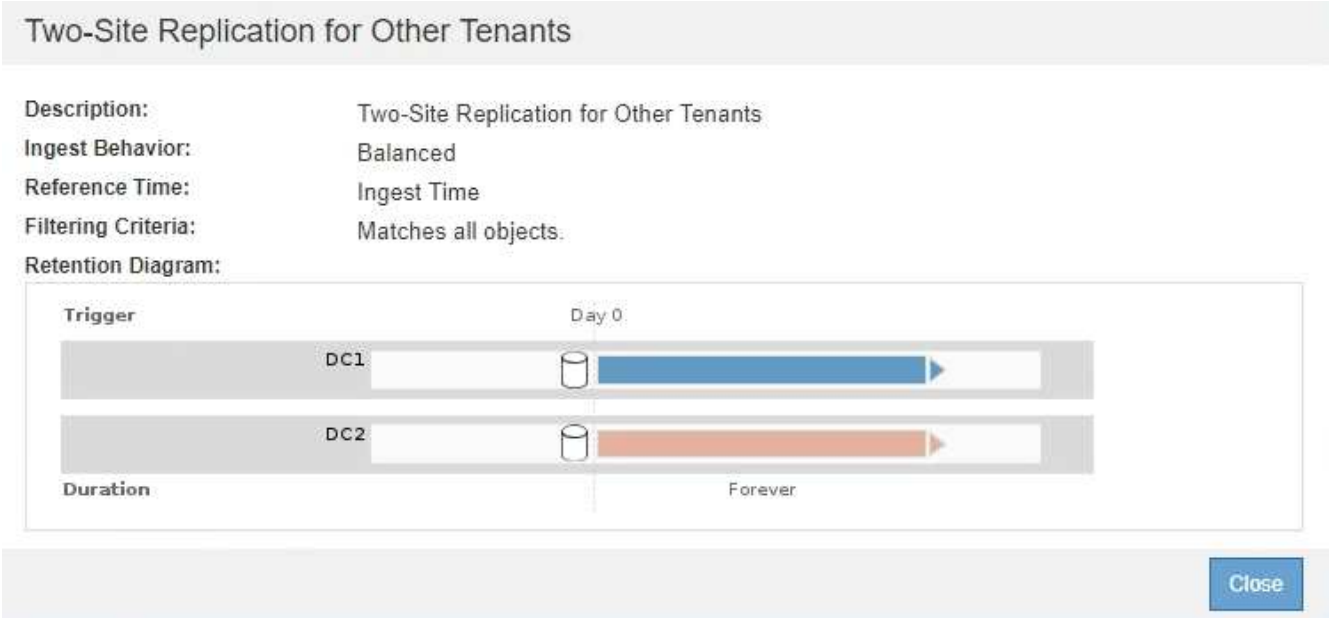
   - Se seleccionan las reglas que utiliza la política que se está clonando.
   - Si la política que está clonando usa reglas sin filtros que no sean la regla predeterminada, se le solicitará que elimine todas las reglas, excepto una de ellas.

- Si la regla predeterminada utiliza un filtro o la hora de referencia no corriente, se le solicitará que seleccione una nueva regla predeterminada.
- Si la regla predeterminada no era la última regla, un botón le permite mover la regla al final de la nueva directiva.



6. Seleccione un nombre de regla o el icono más detalles para ver la configuración de esa regla.

   Este ejemplo muestra los detalles de una regla de ILM que realiza dos copias replicadas en dos sitios.



7. En la sección **Seleccionar regla predeterminada**, seleccione una regla predeterminada para la directiva propuesta.

   La regla predeterminada se aplica a cualquier objeto que no coincida con otra regla de la política. La regla

predeterminada no puede utilizar ningún filtro y siempre se evalúa en último lugar.

> Si no aparece ninguna regla en la sección Select Default Rule, debe salir de la página de la política de ILM y. Cree una regla de ILM predeterminada.

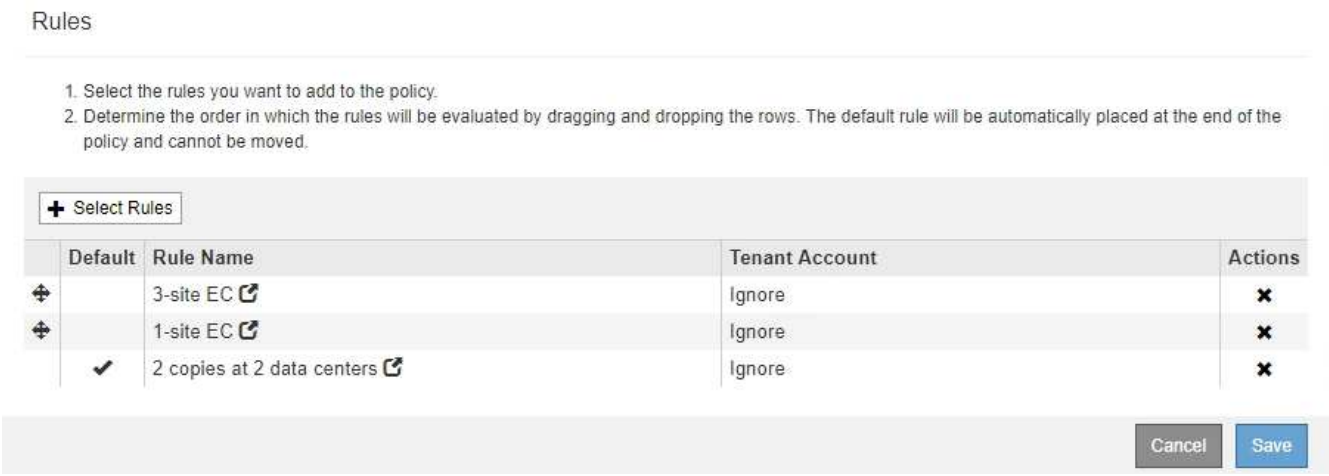
> No utilice la regla convertir 2 copias en stock como regla predeterminada para una directiva. La regla make 2 copies utiliza un único pool de almacenamiento, todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen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

8. En la sección **Seleccionar otras reglas**, seleccione cualquier otra regla que desee incluir en la directiva.

   Las demás reglas se evalúan antes de la regla predeterminada y deben utilizar al menos un filtro (cuenta de inquilino, nombre de bloque, filtro avanzado o tiempo de referencia no corriente).

9. Cuando haya terminado de seleccionar reglas, seleccione **aplicar**.

   Se muestran las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima.



> Aparece una advertencia si la regla predeterminada no conserva objetos para siempre. Al activar esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurra las instrucciones de colocación de la regla predeterminada (a menos que un ciclo de vida de bloque mantenga los objetos durante más tiempo).

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

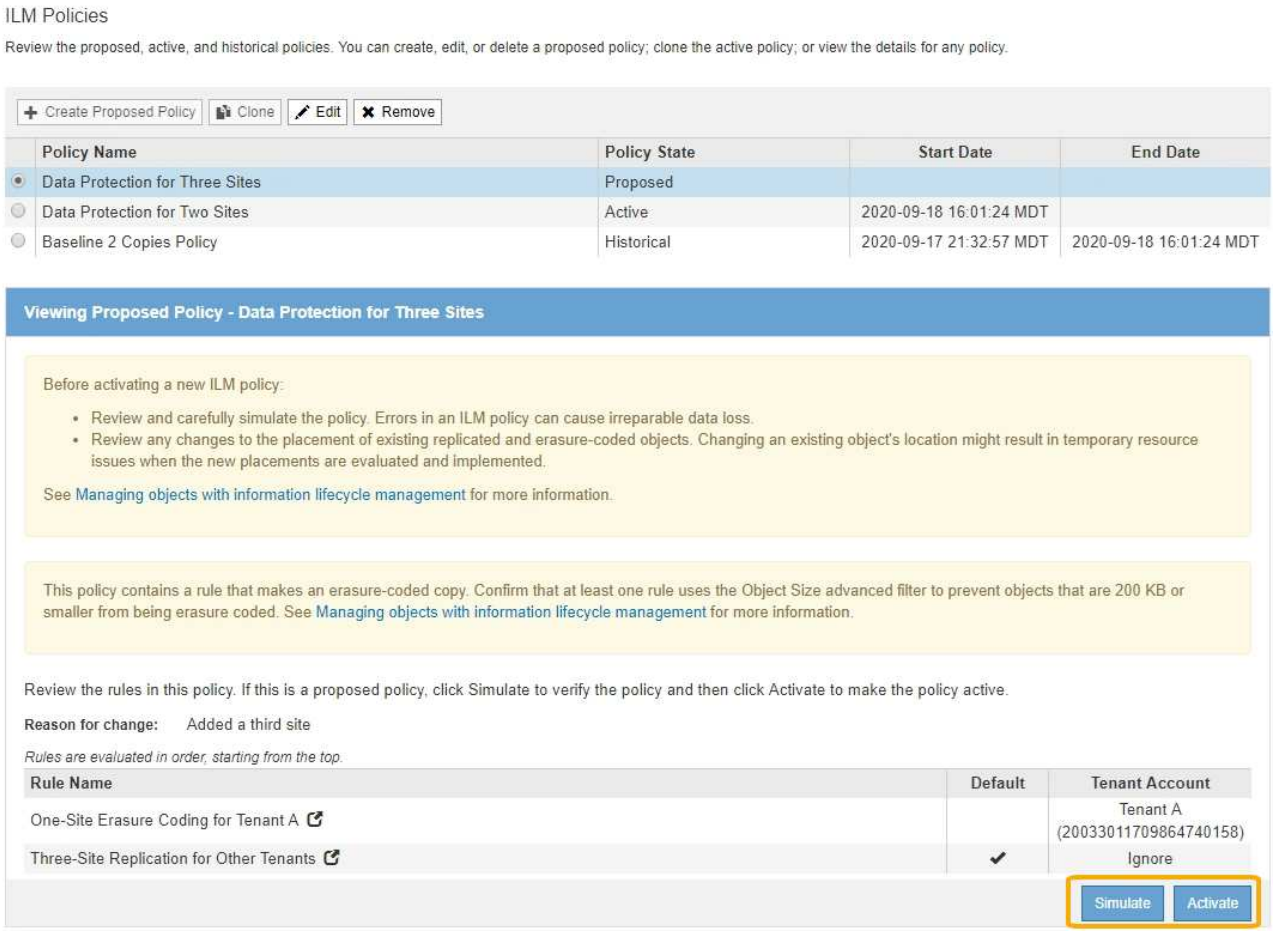
    No se puede mover la regla predeterminada.

> Debe confirmar que las reglas de ILM se encuentran en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior.

11. Según sea necesario, seleccione el icono de eliminación ✖ Para eliminar cualquier regla que no desee en la directiva o seleccione **Seleccionar reglas** para agregar más reglas.
12. Cuando haya terminado, seleccione **Guardar**.

    La página ILM Policies se actualiza:

    - La política que ha guardado se muestra como propuesta. Las políticas propuestas no tienen fechas de inicio y finalización.
    - Los botones **Simulate** y **Activate** están activados.



13. Vaya a. Simule una política de gestión de la vida útil.

Información relacionada

- Qué es una política de ILM
- Gestione objetos con S3 Object Lock

Cree una política de ILM después de habilitar el bloqueo de objetos de S3

Si la configuración global de bloqueo de objetos S3 está habilitada, los pasos para crear una política son ligeramente diferentes. Debe asegurarse de que la política de ILM

cumpla con los requisitos de los bloques con S3 Object Lock habilitado.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- La configuración global de bloqueo de objetos S3 ya está habilitada para el sistema StorageGRID.

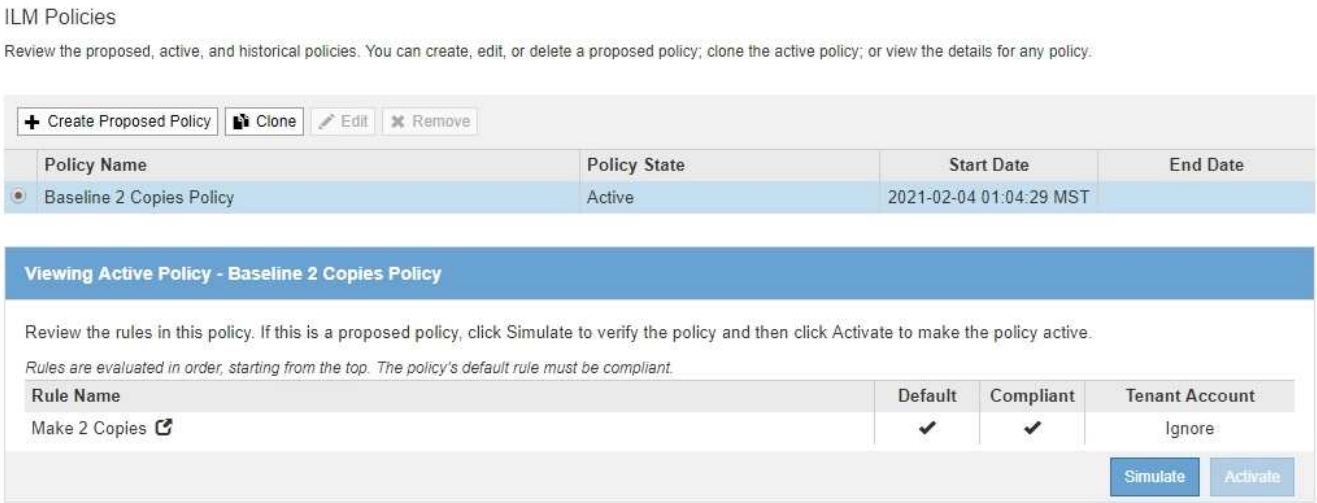
> Si la opción de bloqueo de objetos global de S3 no se ha habilitado, utilice las instrucciones generales para Creación de una política de ILM propuesta.

- Ha creado las reglas de ILM que cumplen y no cumplen con las normativas que desea agregar a la política propuesta. Según sea necesario, puede guardar una directiva propuesta, crear reglas adicionales y, a continuación, editar la directiva propuesta para agregar las nuevas reglas. ConsulteEjemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3.
- Ya tienes Se ha creado una regla de ILM predeterminada para la directiva que cumple con las normativas.
- Opcionalmente, ha visto el vídeo: "Vídeo: Políticas de ILM de StorageGRID"

Pasos

1. Seleccione **ILM** > **políticas**.

   Aparece la página ILM Policies. Si la configuración de bloqueo de objetos global de S3 está habilitada, la página ILM Policies indica qué reglas de ILM son compatibles.



2. Introduzca un nombre único para la directiva propuesta en el campo **Nombre**.

   Debe introducir al menos 1 y no más de 64 caracteres.

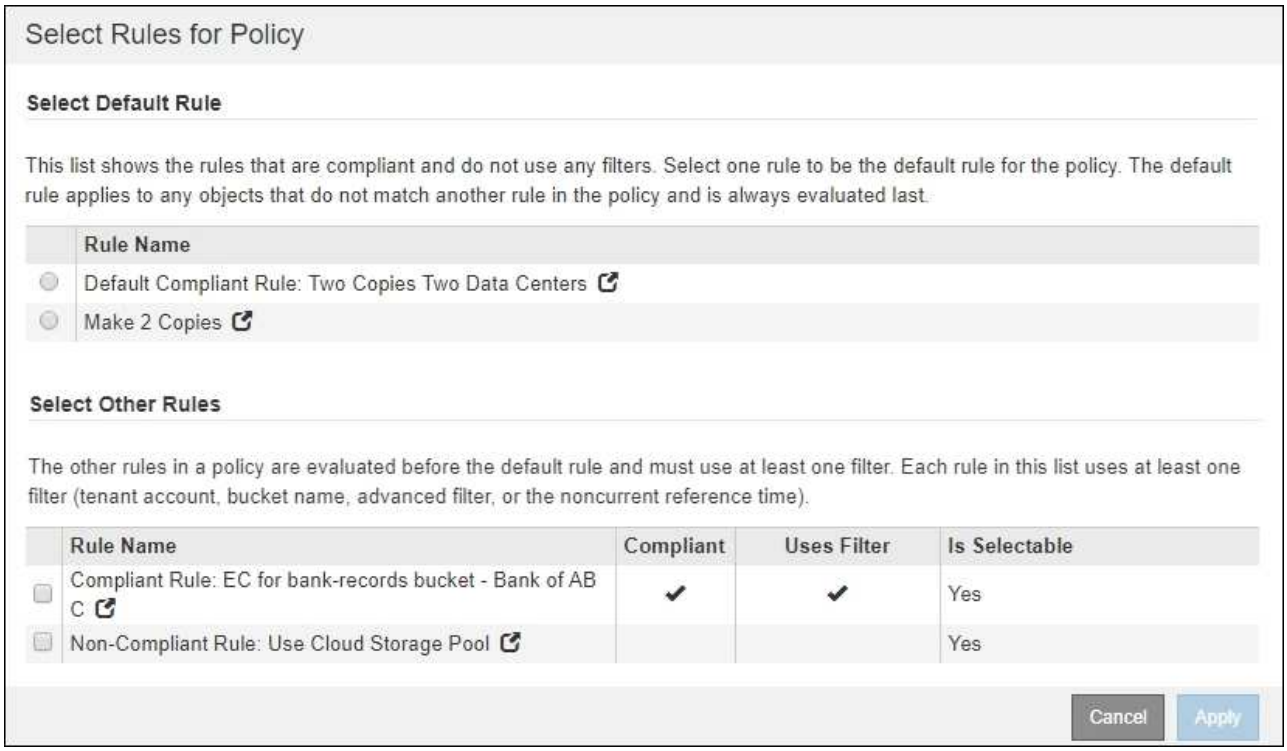
3. Introduzca el motivo por el que está creando una nueva directiva propuesta en el campo **motivo del cambio**.

   Debe introducir al menos 1 y no más de 128 caracteres.

4. Para agregar reglas a la directiva, seleccione **Seleccionar reglas**.

   Aparece el cuadro de diálogo Seleccionar reglas para la directiva, con todas las reglas definidas en la lista.

   - La sección Seleccionar regla predeterminada enumera las reglas que pueden ser predeterminadas para una directiva compatible. Incluye reglas compatibles que no utilizan filtros ni el tiempo de referencia no corriente.
   - La sección Seleccionar otras reglas enumera las demás reglas compatibles y no compatibles que se pueden seleccionar para esta directiva.



5. Seleccione un nombre de regla o el icono más detalles para ver la configuración de esa regla.
6. En la sección **Seleccionar regla predeterminada**, seleccione una regla predeterminada para la directiva propuesta.

   En la tabla de esta sección sólo se enumeran las reglas que cumplen y no utilizan ningún filtro.

   > Si no aparece ninguna regla en la sección Select Default Rule, debe salir de la página de la política de ILM y. Cree una regla de ILM predeterminada eso es conforme.

   > No utilice la regla convertir 2 copias en stock como regla predeterminada para una directiva. La regla make 2 copies utiliza un único pool 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.

7. En la sección **Seleccionar otras reglas**, seleccione cualquier otra regla que desee incluir en la directiva.

   a. Si necesita una regla «predeterminada» distinta para los objetos de bloques S3 que no cumplen las normativas, seleccione opcionalmente una regla no conforme a la normativa que no utilice un filtro.

      Por ejemplo, se recomienda usar un pool de almacenamiento en cloud o un nodo de archivado para almacenar objetos en bloques que no tienen el bloqueo de objetos de S3 habilitado.

      > Sólo puede seleccionar una regla no compatible que no utilice un filtro. Tan pronto como seleccione una regla, la columna **is Selectable** muestra **no** para cualquier otra regla no compatible sin filtros.

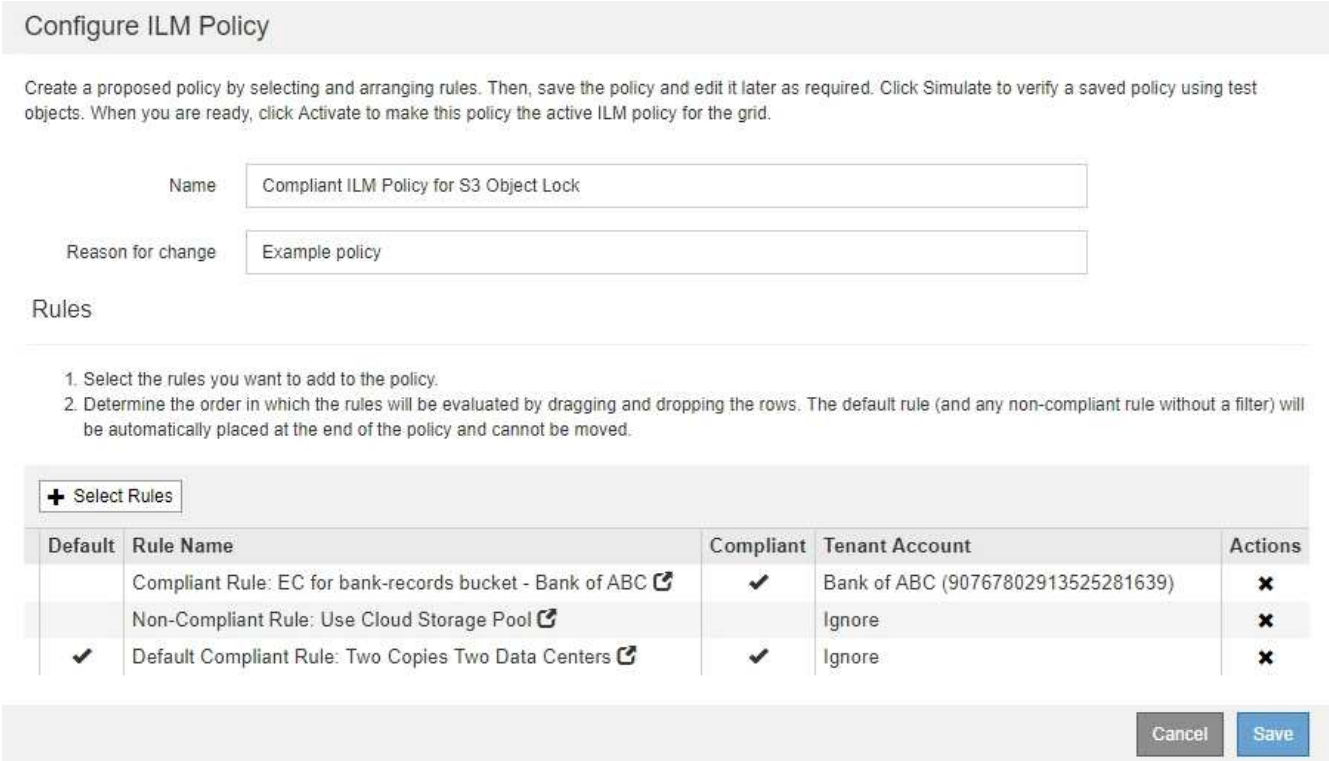
   a. Seleccione cualquier otra regla compatible o no compatible que desee utilizar en la directiva.

      Las otras reglas deben utilizar al menos un filtro (cuenta de inquilino, nombre de bloque o filtro avanzado, como el tamaño del objeto).

8. Cuando haya terminado de seleccionar las reglas, seleccione **aplicar**.

   Se muestran las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima. Si también ha seleccionado una regla de «default» no conforme, esa regla se añade como la regla de segundo a último en la política.

   En este ejemplo, la última regla, 2 copias 2 centros de datos, es la regla predeterminada: Es compatible y no tiene filtros. La segunda regla, Cloud Storage Pool, también no tiene filtros pero no es conforme.



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

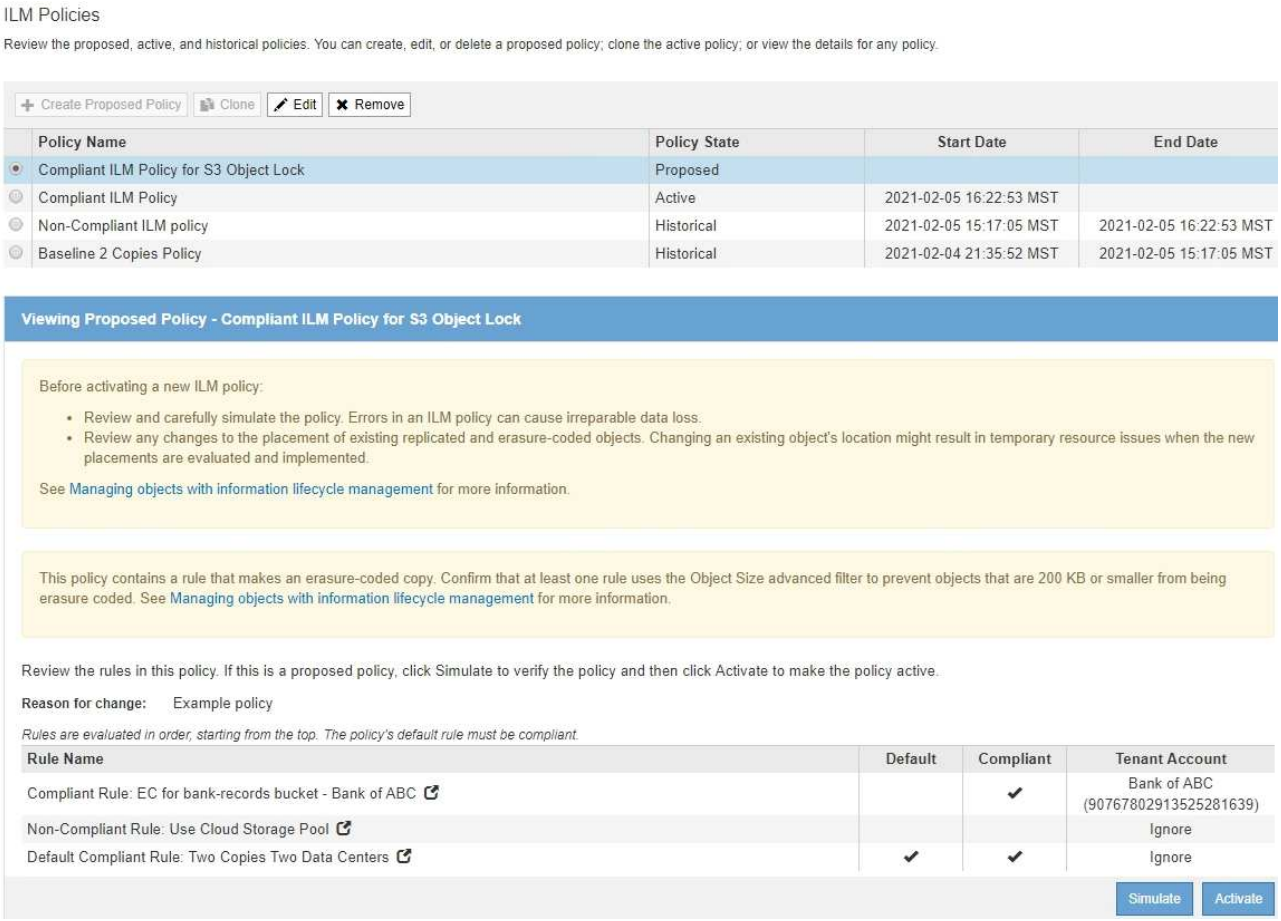
   No se puede mover la regla predeterminada ni la regla de «incumplimiento».

   > Debe confirmar que las reglas de ILM se encuentran en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior.

10. Según sea necesario, seleccione el icono de eliminación ✖ Para eliminar cualquier regla que no desee en la directiva, o **Seleccionar reglas** para agregar más reglas.
11. Cuando haya terminado, seleccione **Guardar**.

    La página ILM Policies se actualiza:

    - La política que ha guardado se muestra como propuesta. Las políticas propuestas no tienen fechas de inicio y finalización.
    - Los botones **Simulate** y **Activate** están activados.



12. Vaya a. Simule una política de gestión de la vida útil.

Simule una política de gestión de la vida útil

Debe simular una directiva propuesta en objetos de prueba antes de activar la directiva y aplicarla a los datos de producción. La ventana de simulación proporciona un entorno independiente que es seguro para las políticas de prueba antes de que se activen y apliquen a los datos en el entorno de producción.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Conoce el bucket/object-key o el contenedor/nombre de objeto de Swift para cada objeto que desea probar y ya ha ingerido esos objetos.

Acerca de esta tarea

Debe seleccionar cuidadosamente los objetos que desea que pruebe la directiva propuesta. Para simular una política completamente, debe probar al menos un objeto para cada filtro en cada regla.

Por ejemplo, si una política incluye una regla para que coincida con los objetos del bloque A y otra regla para que coincidan con los objetos del bloque B, debe seleccionar al menos un objeto del bloque A y un objeto del bloque B para probar la política a fondo. También debe seleccionar al menos un objeto de otro bloque para probar la regla predeterminada.

Al simular una directiva, se aplican las siguientes consideraciones:

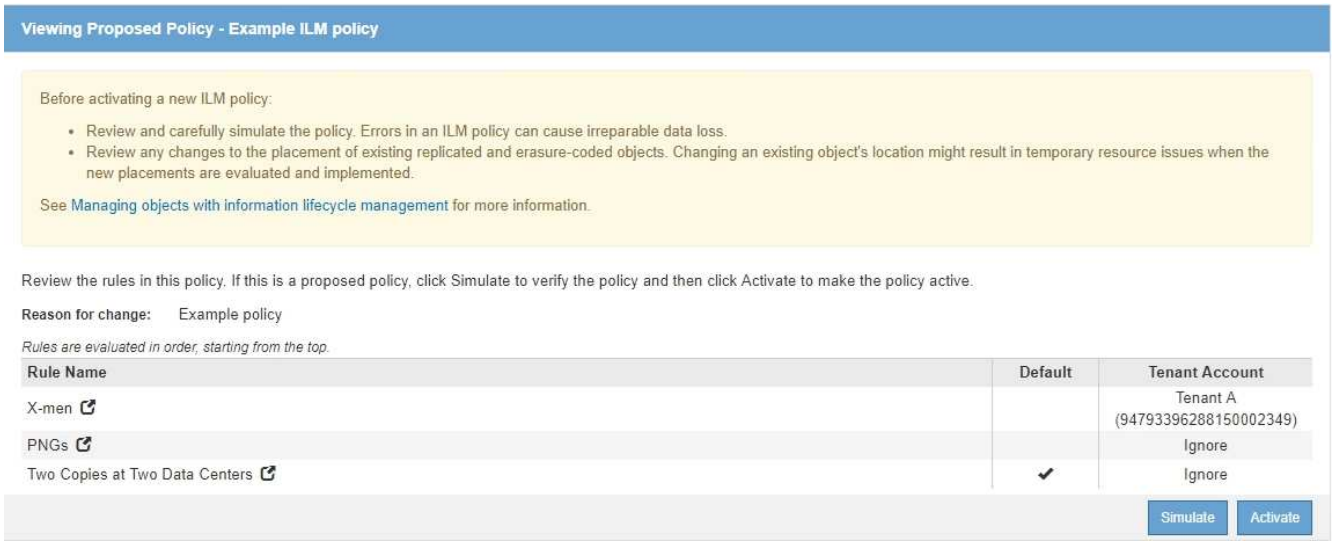
- Después de realizar cambios en una directiva, guarde la directiva propuesta. A continuación, simule el comportamiento de la directiva propuesta guardada.
- Cuando se simula una política, las reglas de ILM en la política filtran los objetos de prueba, de modo que se puede ver qué regla se aplicó a cada objeto. Sin embargo, no se crean copias de objeto y no se coloca ningún objeto. Al ejecutar una simulación no se modifican los datos, las reglas ni la política de ningún modo.
- La página Simulation conserva los objetos probados hasta que se cierra, se aleja o se actualiza la página políticas de ILM.
- Simulation devuelve el nombre de la regla coincidente. Para determinar qué pool de almacenamiento o perfil de código de borrado está activo, puede ver el diagrama de retención seleccionando el nombre de la regla o el icono más detalles .
- Si está habilitada la versión de S3, la política solo se simula con respecto a la versión actual del objeto.

Pasos

1. Seleccione y organice las reglas y guarde la política propuesta.

   La directiva de este ejemplo tiene tres reglas:

Nombre de regla	Filtro	Tipo de copias	Retención
Hombres-X.	• Inquilinoa • Metadatos del usuario (series=x-men)	2 copias en dos centros de datos	2 años
PNs	La clave termina con .png	2 copias en dos centros de datos	5 años
Dos copias dos centros de datos	*Ninguno*	2 copias en dos centros de datos	Para siempre



2. Use un cliente S3 o Swift o el Consola de S3 de experimental, Que está disponible en el Administrador de

arrendatarios para cada arrendatario, procese los objetos necesarios para probar cada regla.

3. Seleccione **simular**.

   Aparecerá el cuadro de diálogo Directiva de gestión de la vida útil de Simulation.

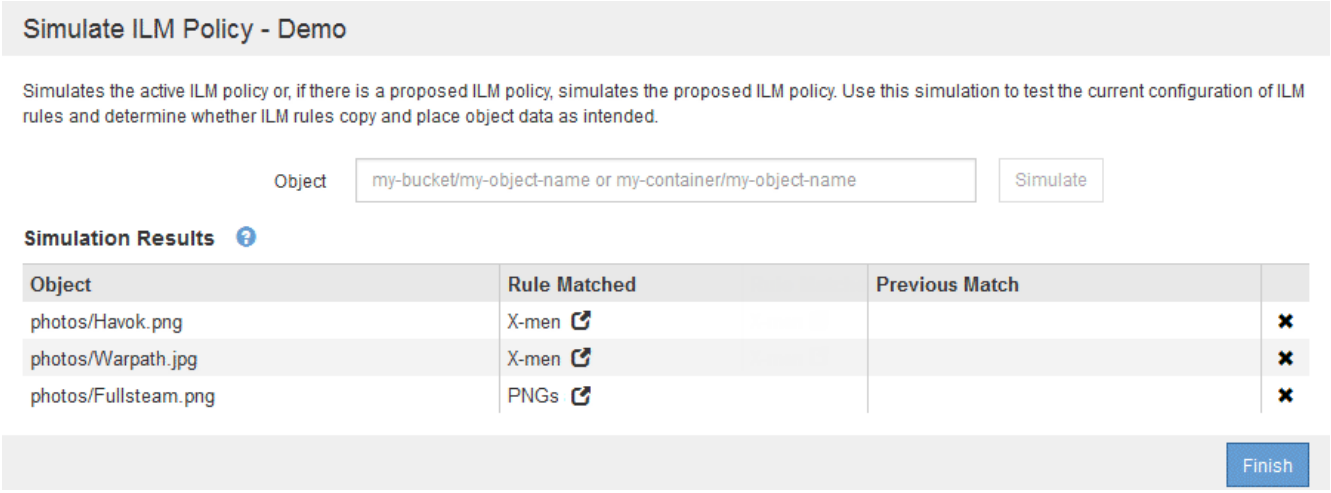
4. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

   Aparece un mensaje si especifica un objeto que no se ha ingerido.

5. En **resultados de Simulation**, confirme que cada objeto estaba coincidente con la regla correcta.

   En el ejemplo, la `Havok.png` y.. `Warpath.jpg` Los objetos estaban correctamente emparejados con la regla X-men. La `Fullsteam.png` objeto, que no incluye `series=x-men` Los metadatos del usuario no se corresponden con la regla X-men, pero se emparejaron correctamente con la regla PNG. La regla predeterminada no se ha utilizado porque los tres objetos coinciden con otras reglas.

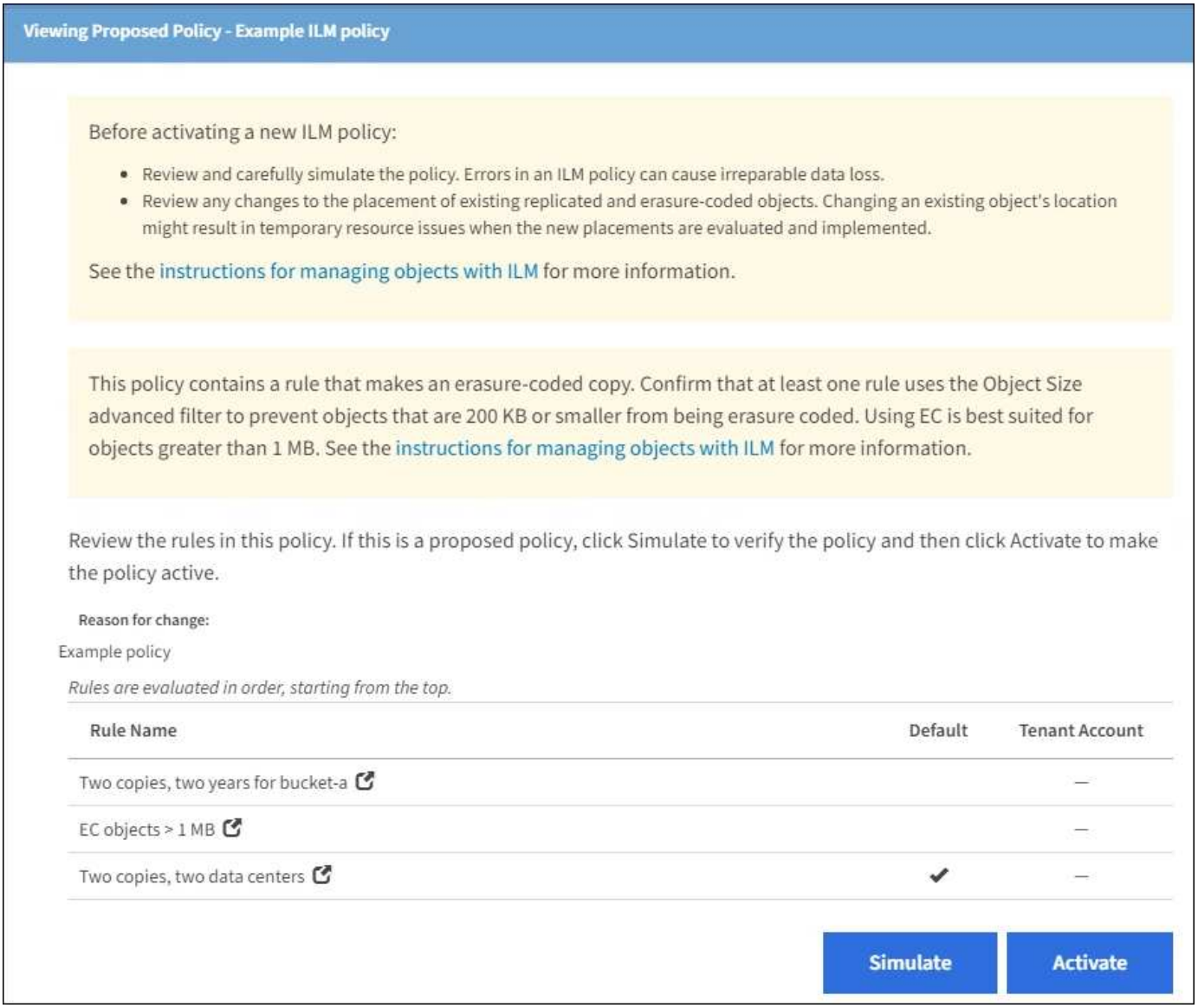
   

Ejemplo 1: Verifique las reglas al simular una política de ILM propuesta

En este ejemplo se muestra cómo comprobar las reglas al simular una directiva propuesta.

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

- La primera regla, **dos copias, dos años para el segmento a**, se aplica sólo a los objetos en el bloque a.
- La segunda regla, **objetos EC > 1 MB**, se aplica a todos los cubos pero filtra a los objetos superiores a 1 MB.
- La tercera regla, **dos copias, dos centros de datos**, es la regla por defecto. No incluye ningún filtro ni utiliza el tiempo de referencia no corriente.



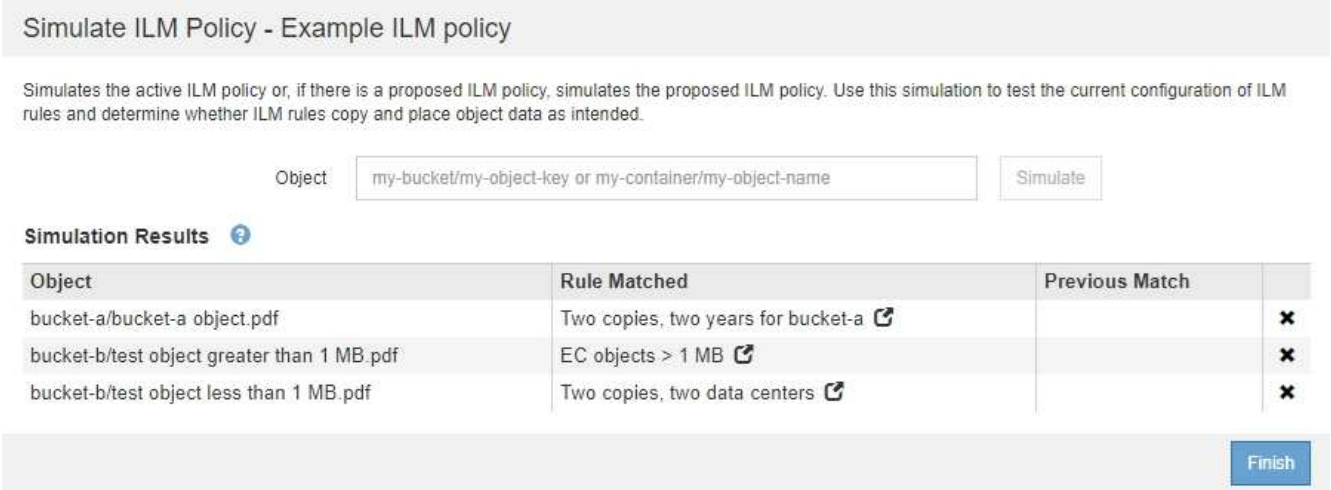
Pasos

1. Después de agregar las reglas y guardar la directiva, seleccione **simular**.

   Se muestra el cuadro de diálogo Simulate ILM Policy.

2. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

   Aparecen los resultados de Simulation, mostrando qué regla de la directiva coincide con cada objeto probado.



3. Confirme que cada objeto se ha coincidido con la regla correcta.

   En este ejemplo:

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

   b. `bucket-b/test object greater than 1 MB.pdf` está en `bucket-b`, así que no coincide con la primera regla. En lugar de ello, la segunda regla coincide correctamente, que filtra los objetos de más de 1 MB.

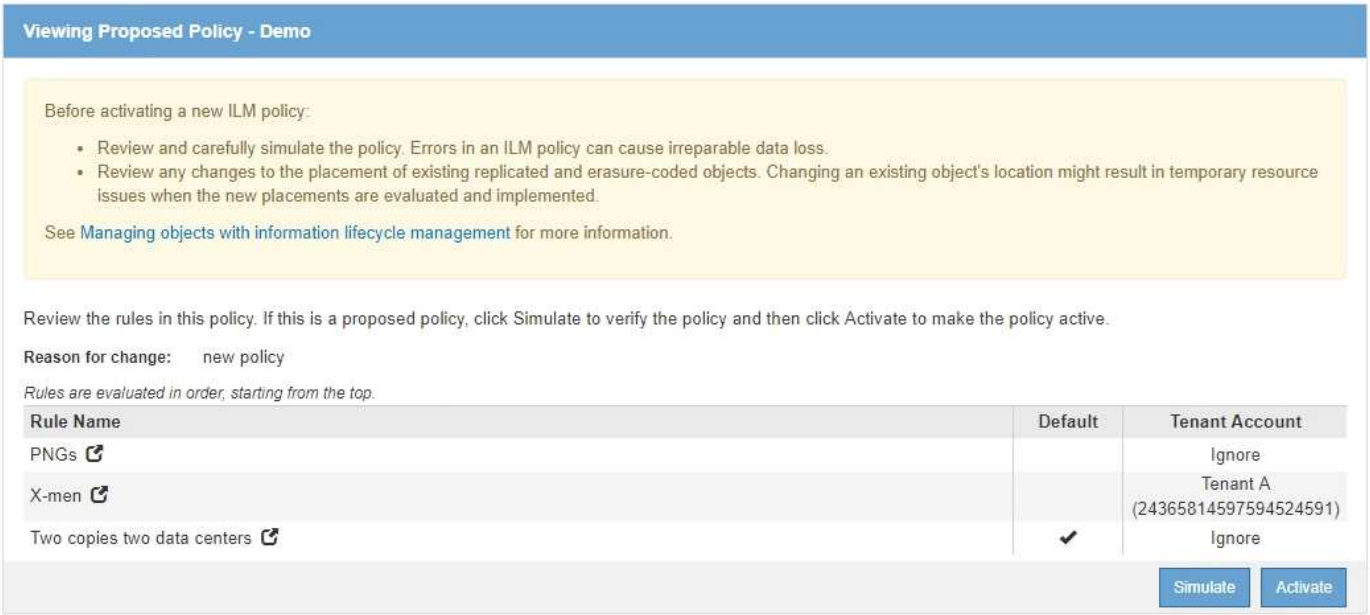
   c. `bucket-b/test object less than 1 MB.pdf` no coincide con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye ningún filtro.

Ejemplo 2: Reordenación de reglas al simular una política de ILM propuesta

En este ejemplo se muestra cómo puede reordenar las reglas para cambiar los resultados al simular una directiva.

En este ejemplo, se está simulando la política **Demo**. Esta política, que está destinada a encontrar objetos que tienen metadatos de usuario de series=x-men, incluye tres reglas de la siguiente manera:

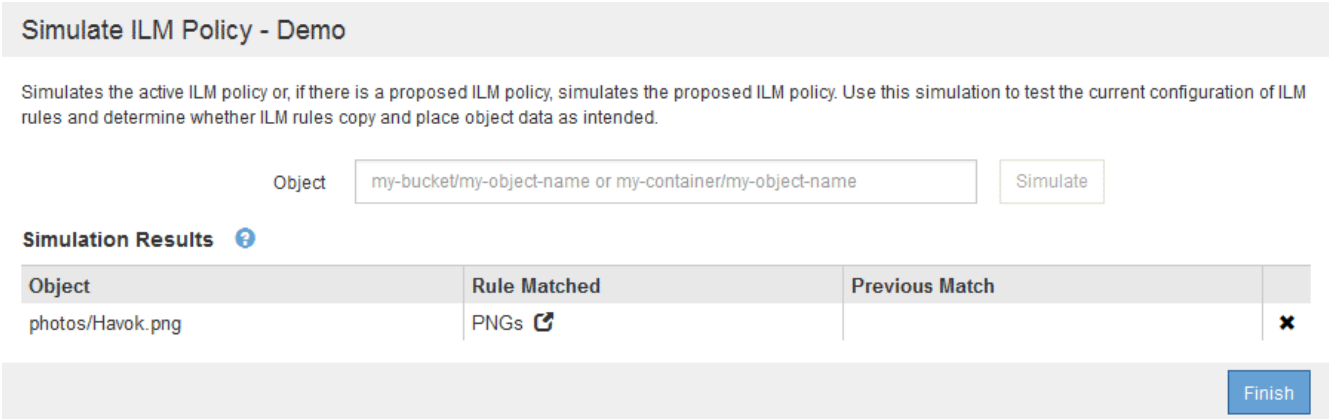
- La primera regla, **PNgs**, filtra los nombres de clave que terminan en `.png`.
- La segunda regla, **X-men**, se aplica sólo a los objetos para el arrendatario A y filtros para `series=x-men` metadatos del usuario.
- La última regla, **dos copias dos centros de datos**, es la regla predeterminada,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



Pasos

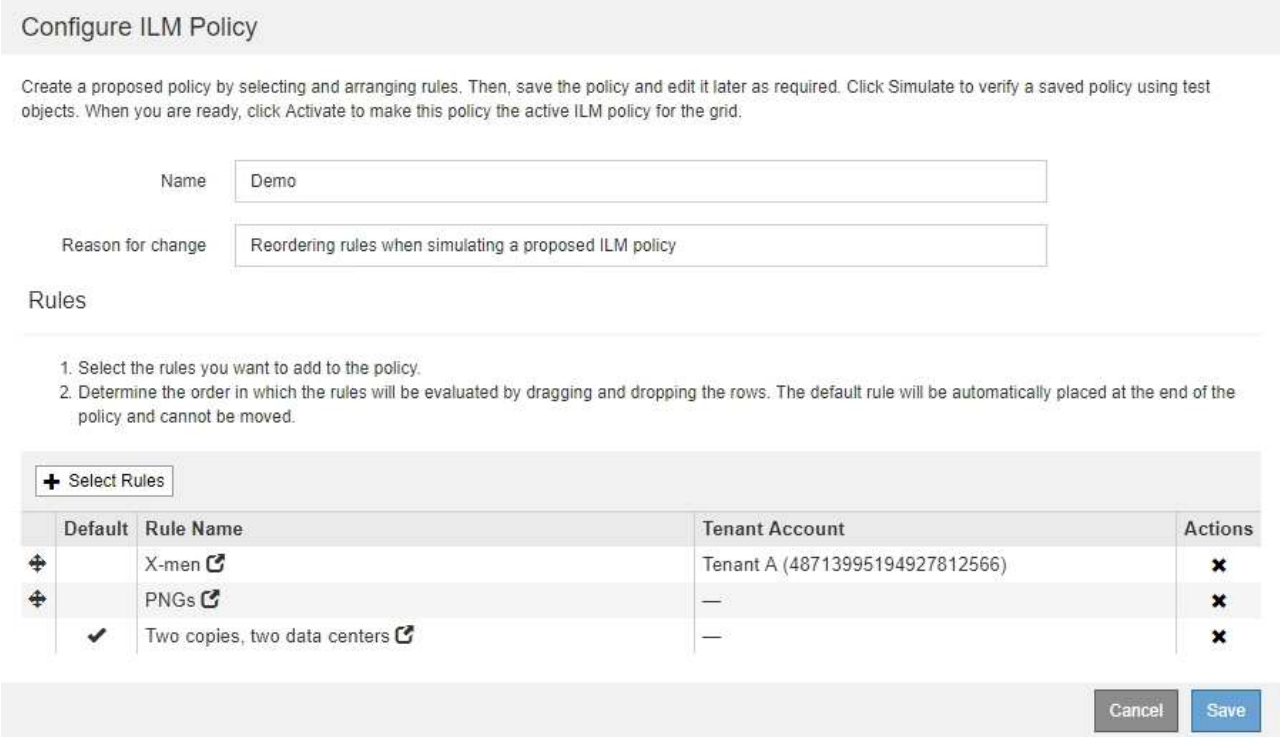
1. Después de agregar las reglas y guardar la directiva, seleccione **simular**.
2. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

   Aparecen los resultados de Simulation, mostrando que `Havok.png` El objeto coincide con la regla **PNgs**.



   Sin embargo, la regla que el `Havok.png` El objeto fue ideado para probar la regla **X-men**.

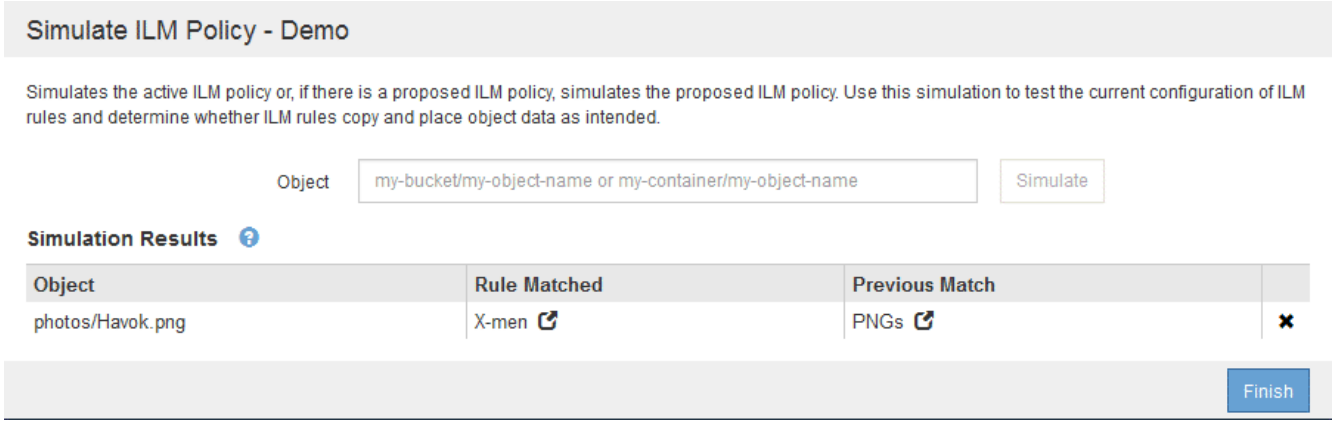
3. Para resolver el problema, vuelva a ordenar las reglas.
   a. Seleccione **Finalizar** para cerrar la página simular política de ILM.
   b. Seleccione **Editar** para editar la directiva.
   c. Arrastre la regla **X-men** hasta la parte superior de la lista.



d. Seleccione **Guardar**.

4. Seleccione **simular**.

Los objetos probados anteriormente se vuelven a evaluar con la directiva actualizada y se muestran los nuevos resultados de simulación. En el ejemplo, la columna Regla conciliada muestra que `Havok.png` Ahora Object coincide con la regla de metadatos X-men, según lo esperado. La columna coincidencia anterior muestra que la regla PNG coincide con el objeto de la simulación anterior.



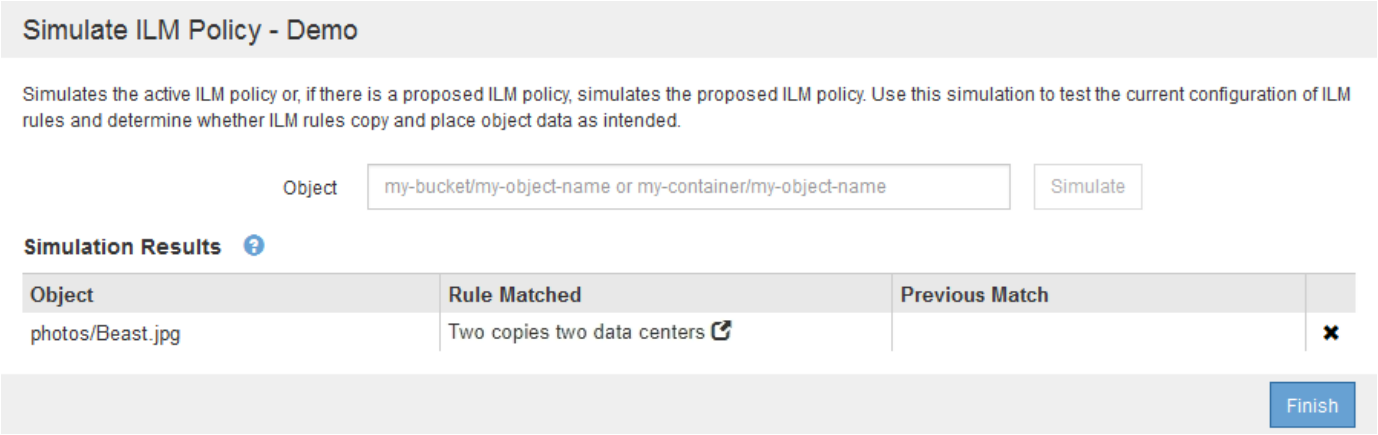
> Si permanece en la página Configure Policies, puede volver a simular una política después de realizar cambios sin tener que volver a introducir los nombres de los objetos de prueba.

Ejemplo 3: Corrección de una regla al simular una política de ILM propuesta

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

En este ejemplo, se está simulando la política **Demo**. Esta política está destinada a encontrar objetos que tienen `series=x-men` metadatos del usuario. Sin embargo, se produjeron resultados inesperados al simular

esta política con la `Beast.jpg` objeto. En lugar de coincidir con la regla de metadatos de X-men, el objeto coincide con la regla predeterminada, dos copias de dos centros de datos.

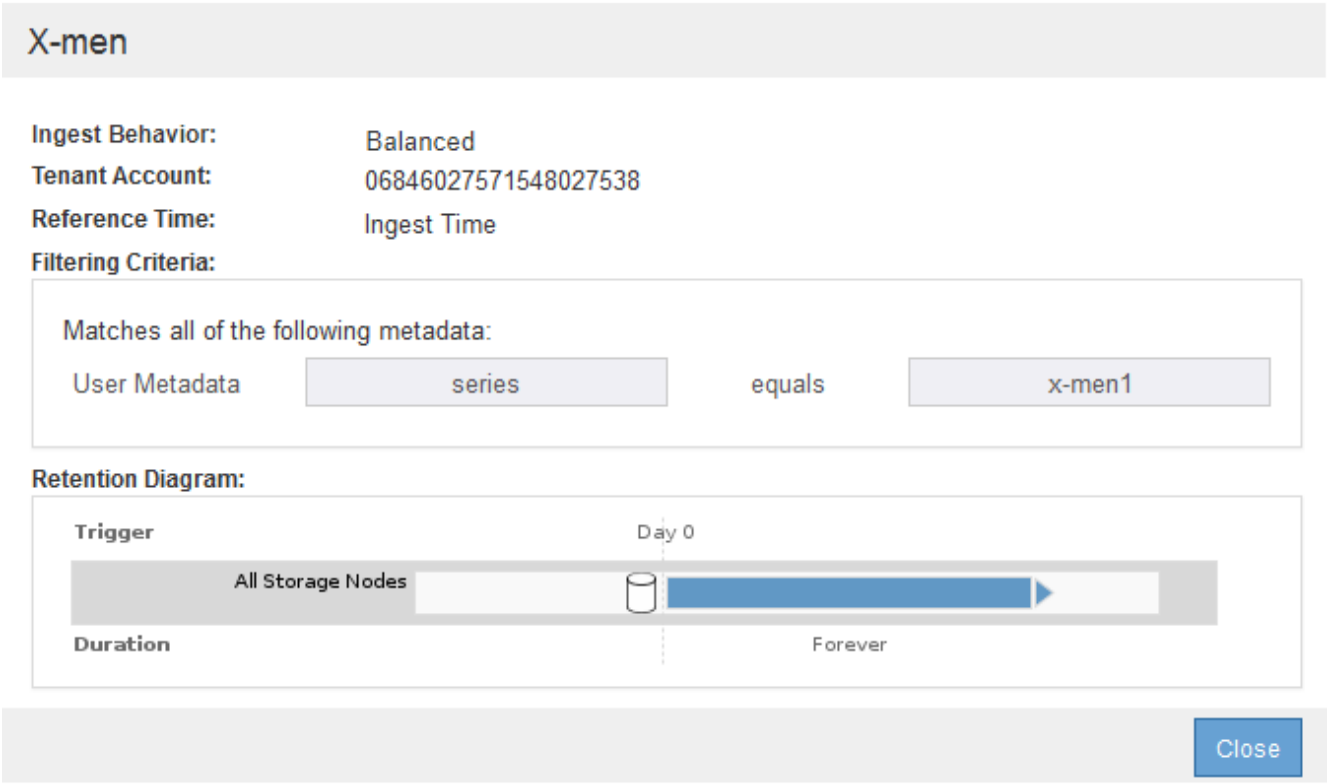


Cuando un objeto de prueba no coincide con la regla esperada de la directiva, debe examinar cada regla de la directiva y corregir cualquier error.

Pasos

1. Para cada regla de la política, consulte la configuración de reglas seleccionando el nombre de la regla o el icono más detalles en cualquier cuadro de diálogo en el que se muestre la regla.
2. Revise la cuenta de arrendatario de la regla, el tiempo de referencia y los criterios de filtrado.

   En este ejemplo, los metadatos de la regla X-men incluyen un error. El valor de los metadatos se introdujo como «'x-men1'» en lugar de «'x-men'».



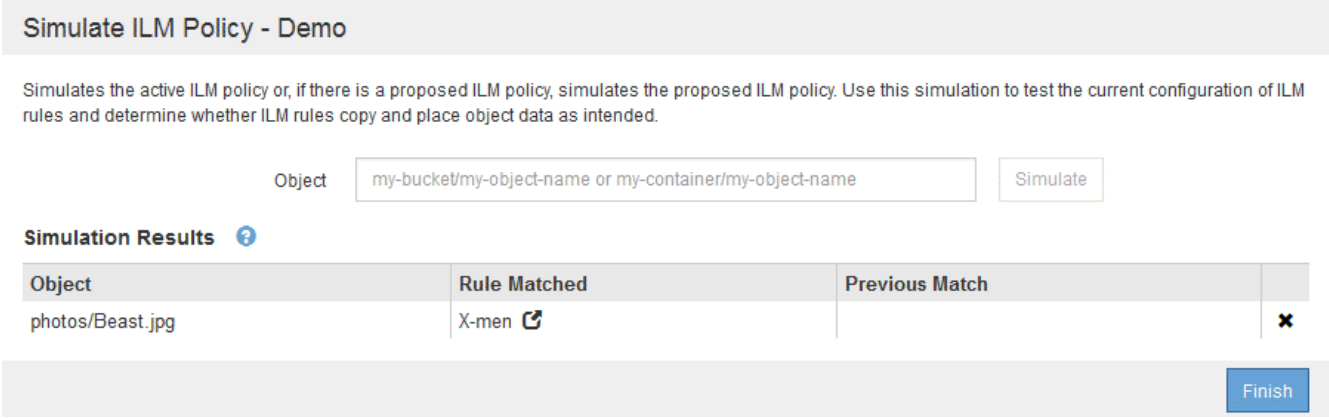
3. Para resolver el error, corrija la regla de la siguiente manera:
   - Si la regla forma parte de la política propuesta, puede clonar la regla o quitar la regla de la política y editarla.
   - Si la regla forma parte de la política activa, debe clonar esa regla. No puede editar ni eliminar una regla de la directiva activa.

Opción	Descripción
Clone la regla	i. Seleccione **ILM** > **Reglas**. ii. Seleccione la regla incorrecta y seleccione **Clonar**. iii. Cambie la información incorrecta y seleccione **Guardar**. iv. Seleccione **ILM** > **políticas**. v. Seleccione la directiva propuesta y seleccione **Editar**. vi. Seleccione **Seleccionar reglas**. vii. Active la casilla de verificación de la nueva regla, desactive la casilla de verificación de la regla original y seleccione **aplicar**. viii. Seleccione **Guardar**.
Edite la regla	i. Seleccione la directiva propuesta y seleccione **Editar**. ii. Seleccione el icono de eliminar ✖ Para eliminar la regla incorrecta y seleccione **Guardar**. iii. Seleccione **ILM** > **Reglas**. iv. Seleccione la regla incorrecta y seleccione **Editar**. v. Cambie la información incorrecta y seleccione **Guardar**. vi. Seleccione **ILM** > **políticas**. vii. Seleccione la directiva propuesta y seleccione **Editar**. viii. Seleccione la regla corregida, seleccione **aplicar** y seleccione **Guardar**.

4. Vuelva a ejecutar la simulación.

> Dado que aleja de la página ILM Policies para editar la regla, los objetos que introdujo anteriormente para la simulación ya no se muestran. Debe volver a introducir los nombres de los objetos.

En este ejemplo, la regla X-men corregida ahora coincide con `Beast.jpg` objeto basado en `series=x-men` los metadatos del usuario, según lo esperado.



Active la política de ILM

Después de añadir reglas de ILM a una política de ILM propuesta, simular la política y confirmar que se comporta como esperaba, está listo para activar la política propuesta.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha guardado y simulado la política de ILM propuesta.

> Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable. Revise y simule cuidadosamente la directiva antes de activarla para confirmar que funcionará según lo previsto.

> Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Acerca de esta tarea

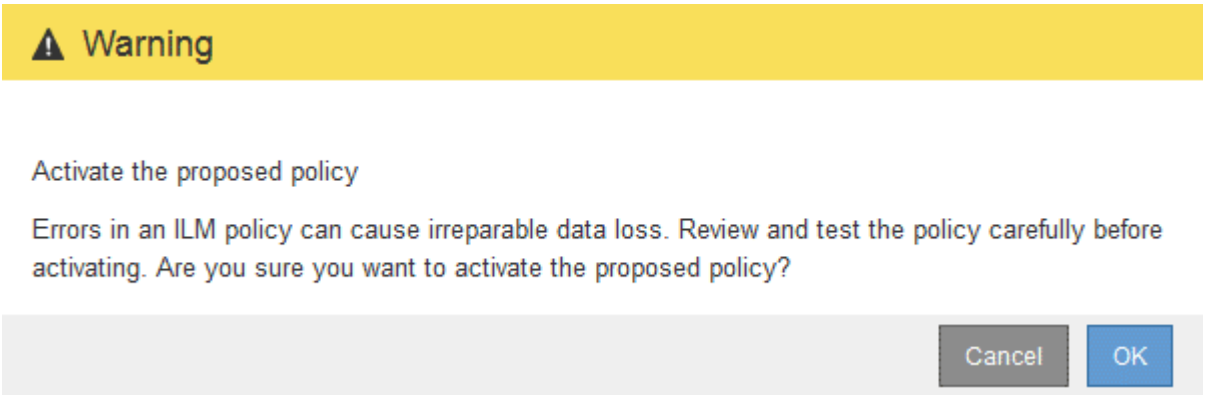
Cuando activa una política de ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva directiva activa no surta efecto hasta que todos los nodos de grid estén disponibles para recibir la nueva directiva. En algunos casos, el sistema espera a implementar una nueva directiva activa para garantizar que los objetos de la cuadrícula no se eliminen accidentalmente.

- Si realiza cambios en las políticas que aumentan la redundancia o la durabilidad de los datos, estos 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, dicha política se implementará de forma inmediata porque aumenta la redundancia de datos.
- Si realiza cambios en las políticas que podrían reducir la redundancia o la durabilidad de los datos, dichos cambios no se implementarán hasta que todos los nodos de grid estén disponibles. Por ejemplo, si activa una nueva directiva que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva directiva se marcará como "'activo'", pero no entrará en vigor hasta que todos los nodos estén en línea y disponibles.

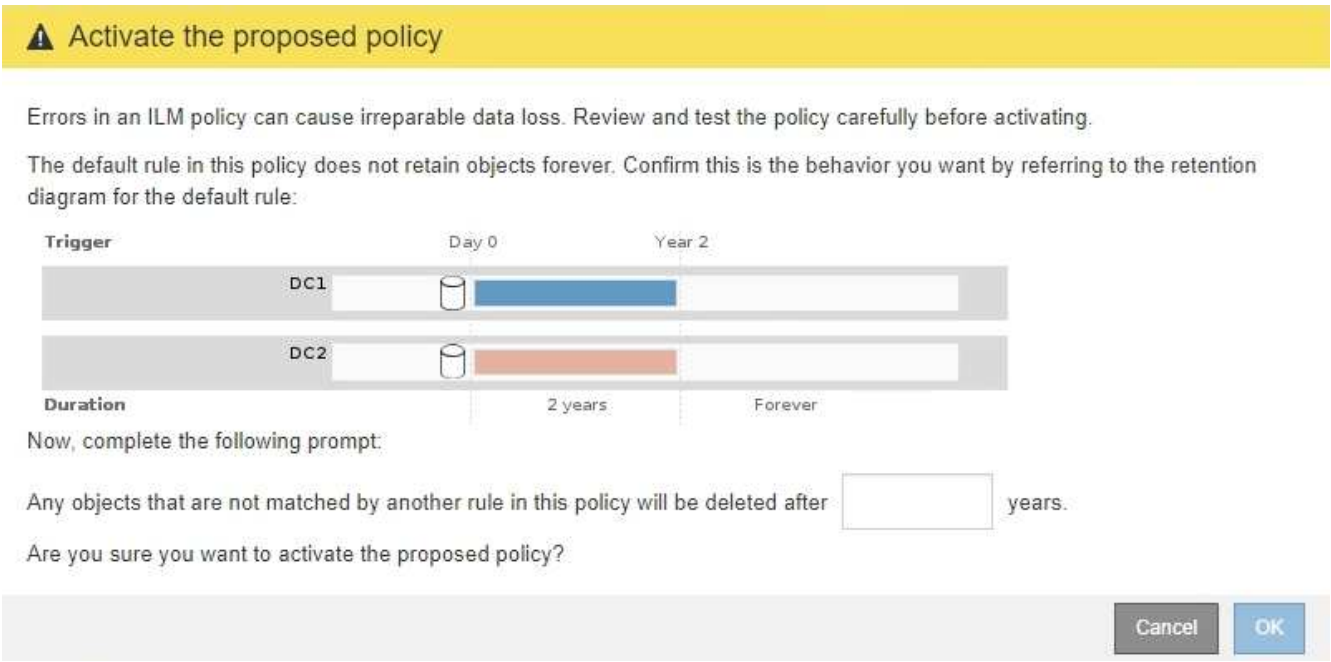
Pasos

1. Cuando esté listo para activar una directiva propuesta, seleccione la directiva en la página políticas de ILM y seleccione **Activar**.

   Aparecerá un mensaje de advertencia en el que se le pedirá que confirme que desea activar la directiva propuesta.



   Aparece un mensaje en el mensaje de advertencia si la regla predeterminada de la directiva no conserva objetos para siempre. En este ejemplo, el diagrama de retención muestra que la regla predeterminada eliminará objetos después de 2 años. Debe escribir **2** en el cuadro de texto para reconocer que cualquier objeto que no coincida con otra regla de la política se eliminará de StorageGRID después de 2 años.



2. Seleccione **OK**.

Resultado

Cuando se activa una nueva política de ILM:

- La política se muestra con un estado de política activo en la tabla de la página ILM Policies. La entrada Fecha de inicio indica la fecha y la hora en que se activó la directiva.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy | Clone | Edit | Remove

	Policy Name	Policy State	Start Date	End Date
◉	New Policy	Active	2017-07-20 18:49:53 MDT	
○	Baseline 2 Copies Policy	Historical	2017-07-19 21:24:30 MDT	2017-07-20 18:49:53 MDT

- La directiva anteriormente activa se muestra con un estado de directiva histórico. Las entradas Fecha de inicio y Fecha de finalización indican cuándo se ha activado la directiva y cuándo ha dejado de estar en vigor.

Información relacionada

Ejemplo 6: Cambiar una política de ILM

Comprobar una política de ILM con la búsqueda de metadatos de objetos

Después de activar una política de ILM, debe procesar objetos de prueba representativos en el sistema StorageGRID. A continuación, debe realizar una búsqueda de metadatos de objetos para confirmar que las copias se están creando como intencionadas y se encuentran en las ubicaciones correctas.

Lo que necesitará

- Tiene un identificador de objeto, que puede ser uno de los siguientes:
  - **UUID**: Identificador único universal del objeto. Introduzca el UUID en toda la mayúscula.
  - **CBID**: Identificador único del objeto dentro de StorageGRID. Es posible obtener el CBID de un objeto del registro de auditoría. Introduzca el CBID en todas las mayúsculas.
  - **Bloque de S3 y clave de objeto**: Cuando un objeto se ingiere a través de la interfaz S3, la aplicación cliente utiliza una combinación de bucket y clave de objeto para almacenar e identificar el objeto. Si el bloque de S3 tiene versiones y desea buscar una versión específica de un objeto S3 mediante el bloque y la clave de objeto, tendrá el **ID de versión**.
  - **Nombre de objeto y contenedor Swift**: Cuando un objeto se ingiere a través de la interfaz Swift, la aplicación cliente utiliza una combinación de nombre de objeto y contenedor para almacenar e identificar el objeto.

Pasos

1. Procese el objeto.
2. Seleccione **ILM** > **Búsqueda de metadatos de objetos**.
3. Escriba el identificador del objeto en el campo **Identificador**. Es posible introducir un UUID, CBID, bucket/object-key de S3 o nombre de objeto/contenedor de Swift.
4. De manera opcional, introduzca un ID de versión para el objeto (solo S3).

5. Seleccione **Buscar**.

   Se muestran los resultados de la búsqueda de metadatos de los objetos. Esta página incluye los siguientes tipos de información:

   - Metadatos del sistema, incluidos el ID de objeto (UUID), el nombre del objeto, el nombre del contenedor, el ID o el nombre de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez, y la fecha y hora en que se modificó por última vez el objeto.
   - Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
   - Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
   - Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
   - Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
   - Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
   - Para objetos segmentados y objetos multipartes, una lista de segmentos de objetos que incluyen identificadores de segmentos y tamaños de datos. Para objetos con más de 100 segmentos, sólo se muestran los primeros 100 segmentos.
   - Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen los metadatos internos del sistema que no se garantiza que continúen del lanzamiento al lanzamiento.

     En el ejemplo siguiente se muestran los resultados de búsqueda de metadatos de objetos para un objeto de prueba S3 almacenado como dos copias replicadas.

System Metadata

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

Replicated Copies

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

Raw Metadata


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


6. Confirme que el objeto se almacena en la ubicación o las ubicaciones correctas y que es el tipo de copia correcto.

> Si la opción Auditoría está activada, también puede supervisar el registro de auditoría del mensaje ORLM Object Rules met. El mensaje de auditoría de ORLM puede proporcionarle más información sobre el estado del proceso de evaluación de ILM, pero no puede proporcionarle información sobre la corrección de la ubicación de los datos del objeto ni sobre la integridad de la política de ILM. Debe evaluar esto usted mismo. Para obtener más información, consulte Revisar los registros de auditoría.

Información relacionada

- Use S3
- Use Swift

Trabaje con las reglas de ILM y las políticas de ILM

Una vez creadas las reglas de ILM y una política de ILM, puede seguir trabajando con ellas, modificando su configuración a medida que cambian sus requisitos de almacenamiento.

Lo que necesitará

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

Elimine una regla de ILM

Para que la lista de reglas de ILM actuales pueda ser manejable, elimine las reglas de ILM que no pueda usar.

No puede eliminar una regla de ILM si actualmente se encuentra en uso en la política activa o en la política propuesta. Si necesita eliminar una regla de ILM que utilice una política, primero debe realizar estos pasos:

1. Clone la política activa o edite la política propuesta.
2. Quite la regla de ILM de la política.
3. Guarde, simule y active la nueva directiva para asegurarse de que los objetos están protegidos como se espera.

Pasos

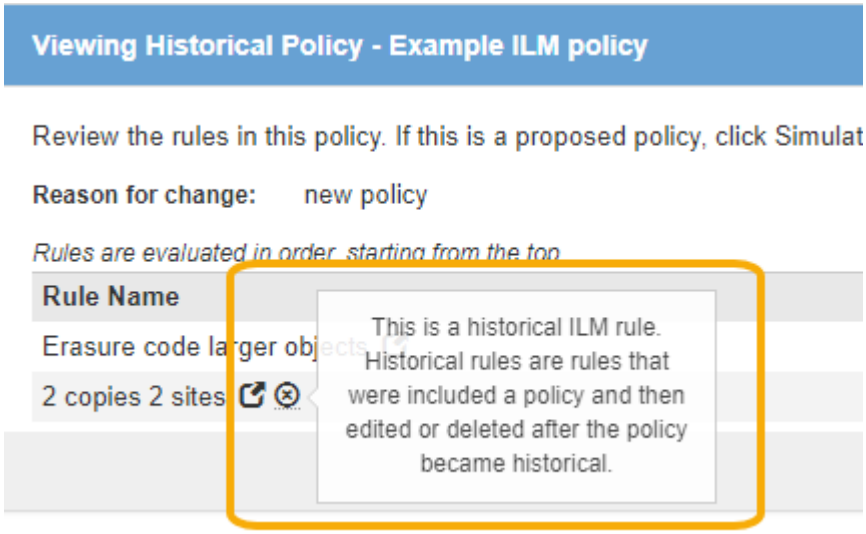
1. Seleccione **ILM** > **Reglas**.
2. Revise la entrada de tabla de la regla que desea quitar.

   Confirme que la regla no se utiliza en la política de ILM activa o en la política de ILM propuesta.

3. Si la regla que desea eliminar no está en uso, seleccione el botón de opción y seleccione **Quitar**.
4. Seleccione **Aceptar** para confirmar que desea eliminar la regla ILM.

   La regla de ILM se elimina.

Si elimina una regla que se utiliza en una política histórica, a. ⊗ aparece un icono para la regla cuando se visualiza la política, lo que indica que la regla se ha convertido en una regla histórica.



Editar una regla de ILM

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

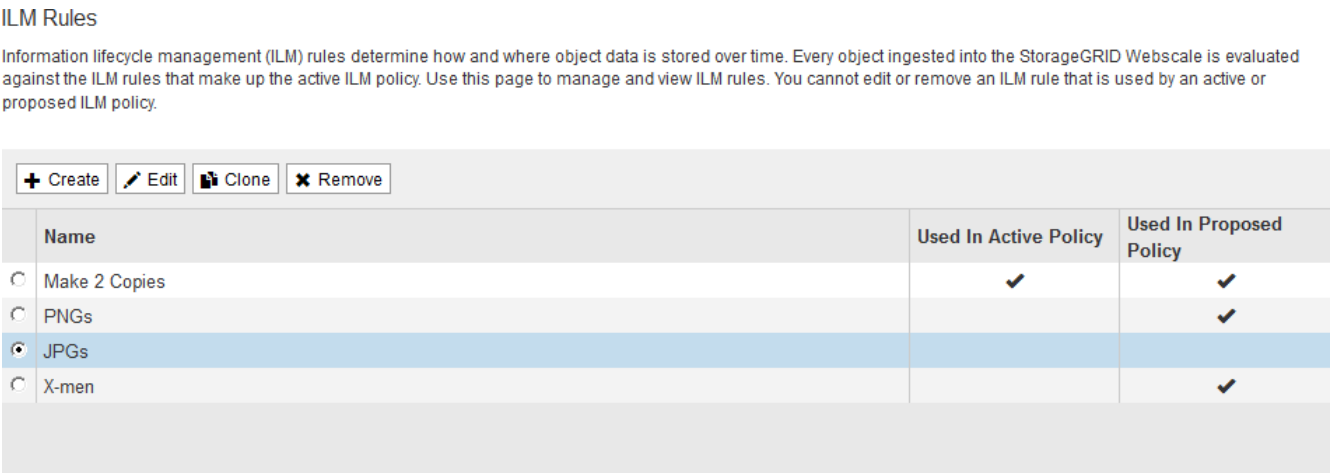
No se puede editar una regla si se está utilizando en la política de ILM propuesta o en la política de ILM activa. En su lugar, puede clonar estas reglas y hacer los cambios necesarios en la copia clonada. Tampoco puede editar la regla de gestión del ciclo de vida de la información (hacer 2 copias) o las reglas de gestión del ciclo de vida de la información creadas antes de la versión 10.3 de StorageGRID.

> Antes de agregar una regla editada a la política de ILM activa, tenga en cuenta que un cambio en las instrucciones de ubicación de un objeto puede provocar un aumento de la carga en el sistema.

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules. Esta página muestra todas las reglas disponibles e indica qué reglas se están utilizando en la directiva activa o en la directiva propuesta.



2. Seleccione una regla que no se esté utilizando y seleccione **Editar**.

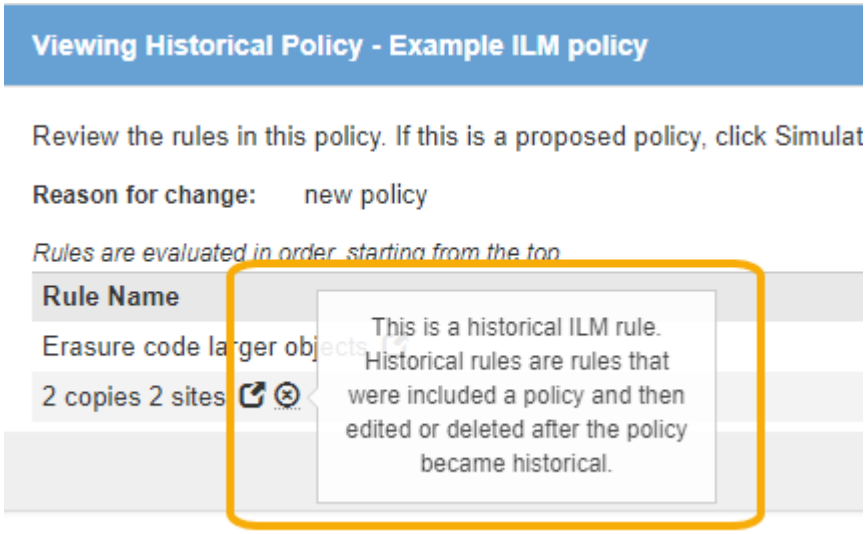
   Se abrirá el asistente Editar regla de ILM.

3. Complete las páginas del asistente Edit ILM Rule, siguiendo los pasos de Creación de una regla de ILM y.. uso de filtros avanzados, según sea necesario.

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

4. Seleccione **Guardar**.

Si edita una regla que se utiliza en una política histórica, una ⊗ aparece un icono para la regla cuando se visualiza la política, lo que indica que la regla se ha convertido en una regla histórica.



Clonar una regla de ILM

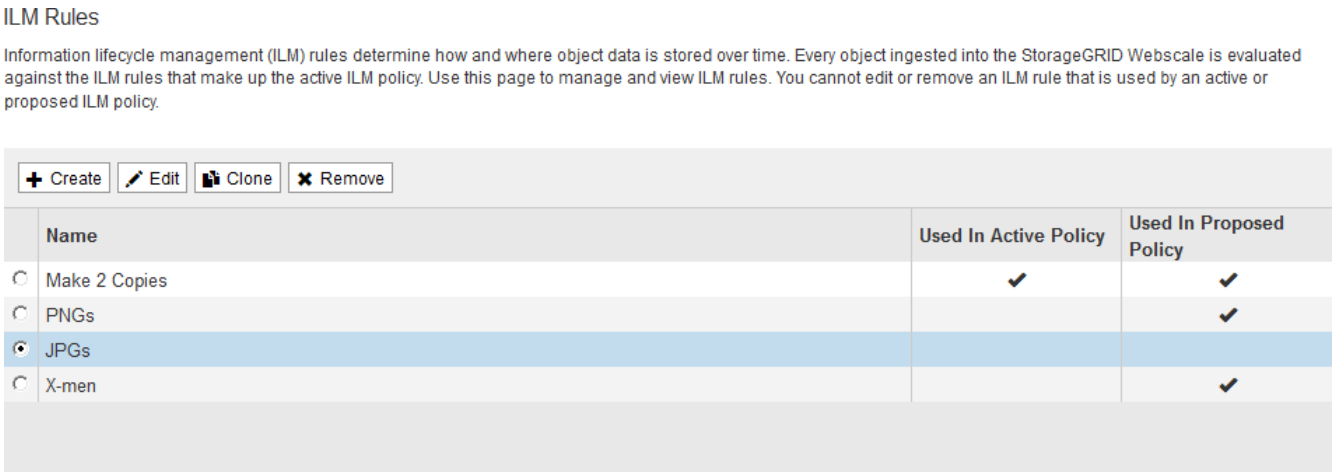
No se puede editar una regla si se está utilizando en la política de ILM propuesta o en la política de ILM activa. En su lugar, puede clonar una regla y hacer los cambios necesarios en la copia clonada. A continuación, si es necesario, puede eliminar la regla original de la directiva propuesta y sustituirla por la versión modificada. No puede clonar una regla de ILM si se creó con StorageGRID versión 10.2 o anterior.

Antes de añadir una regla clonada a la política de ILM activa, tenga en cuenta que un cambio en las instrucciones de ubicación de un objeto puede provocar un aumento de la carga en el sistema.

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules.



2. Seleccione la regla ILM que desea clonar y seleccione **Clonar**.

   Se abrirá el asistente Crear regla de ILM.

3. Actualice la regla clonada siguiendo los pasos para editar una regla de ILM y usando filtros avanzados.

   Al clonar una regla de ILM, debe introducir un nombre nuevo.

4. Seleccione **Guardar**.

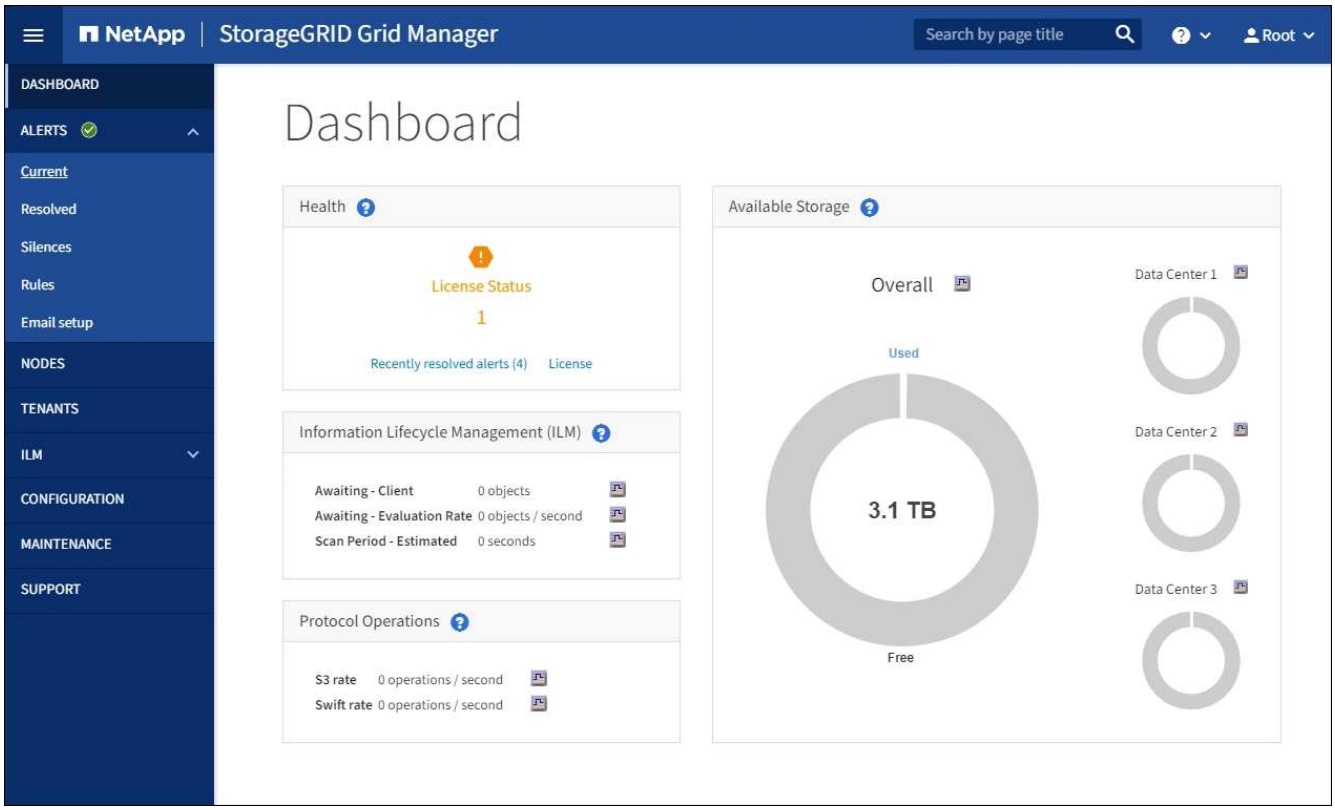
   Se crea la nueva regla de ILM.

Ver la cola de actividades de la política de ILM

Puede ver el número de objetos que hay en la cola que se van a evaluar en comparación con la política de ILM en cualquier momento. Puede ser conveniente supervisar la cola de procesamiento de ILM para determinar el rendimiento del sistema. Una cola grande puede indicar que el sistema no puede seguir el ritmo de la tasa de ingesta, la carga de las aplicaciones cliente es demasiado alta o que existe alguna condición anormal.

Pasos

1. Seleccione **Panel**.



2. Supervise la sección Information Lifecycle Management (ILM).

   Puede seleccionar el signo de interrogación para ver una descripción de los elementos de esta sección.

Utilice la bloqueo de objetos de S3 con ILM

Gestione objetos con S3 Object Lock

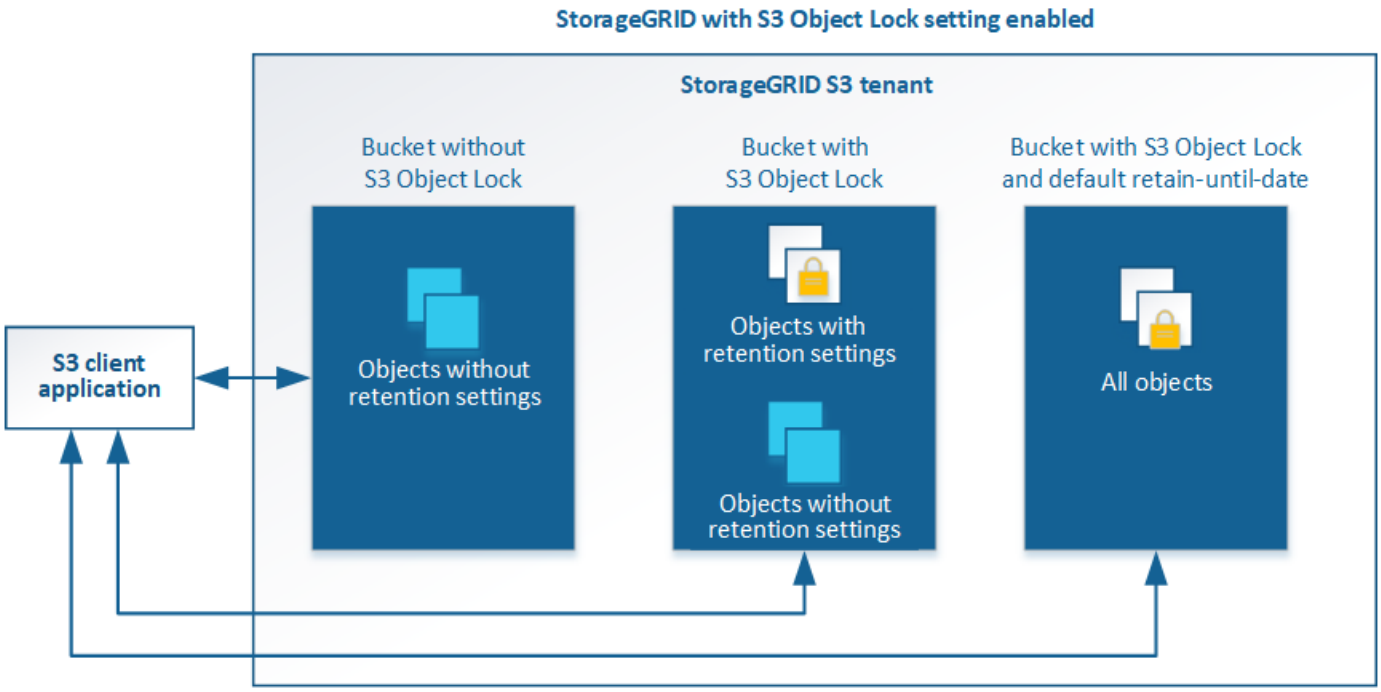
Como administrador de grid, puede habilitar S3 Object Lock para el sistema

StorageGRID e implementar una política de ILM compatible para ayudar a garantizar que los objetos de bloques S3 específicos no se eliminen ni se sobrescriban por un periodo de tiempo determinado.

¿Qué es el bloqueo de objetos de S3?

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

Tal y como se muestra en la figura, cuando se habilita la opción global de bloqueo de objetos de S3 para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear bloques con o sin la función de bloqueo de objetos de S3 habilitada. Si un bloque tiene habilitada la función S3 Object Lock, las aplicaciones cliente S3 pueden especificar, opcionalmente, la configuración de retención para cualquier versión del objeto en ese bloque. Una versión de objeto debe tener la configuración de retención especificada para estar protegida por S3 Object Lock. Además, cada bloque con el bloqueo de objetos S3 habilitado puede tener, de manera opcional, un modo de retención y un período de retención predeterminados, lo que se aplica si se agregan objetos al bloque sin su propia configuración de retención.



La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Si un bloque tiene habilitado el bloqueo de objetos S3, la aplicación cliente S3 puede especificar, de manera opcional, la siguiente configuración de retención a nivel de objeto al crear o actualizar un objeto:

- **Retener-hasta-fecha**: Si la fecha retener-hasta-fecha de una versión de objeto es en el futuro, el objeto puede ser recuperado, pero no puede ser modificado o eliminado. Según sea necesario, se puede aumentar la fecha de retención hasta de un objeto, pero esta fecha no se puede disminuir.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece

en su lugar hasta que se elimina explícitamente. La retención legal es independiente de la retención hasta la fecha.

Para obtener detalles sobre la configuración de retención de objetos, vaya a. Utilice el bloqueo de objetos de S3.

Para obtener más información acerca de la configuración de retención de bloque predeterminada, vaya a. Use la retención de bloque predeterminada de Object Lock de S3.

Comparación del bloqueo de objetos de S3 con el cumplimiento de normativas heredado

El bloqueo de objetos de S3 sustituye la función de cumplimiento de normativas que estaba disponible en versiones anteriores de StorageGRID. Debido a que la función de bloqueo de objetos S3 cumple los requisitos de Amazon S3, deja obsoleto la función propia de cumplimiento de StorageGRID, que ahora se conoce como "'Legacy Compliance".

Si anteriormente habilitó la configuración de cumplimiento global, la opción global de bloqueo de objetos S3 se habilitó automáticamente. Los usuarios inquilinos ya no pueden crear nuevos bloques con el servicio de cumplimiento de normativas; sin embargo, según sea necesario, los usuarios inquilinos pueden seguir usando y gestionando cualquier parte existente compatible, lo que incluye realizar las siguientes tareas:

- Incorporación de objetos nuevos en un bloque existente con cumplimiento de normativas heredado habilitado.
- Aumento del período de retención de un bloque existente que tiene activada la normativa heredada.
- Cambio de la configuración de eliminación automática para un bloque existente que tiene activada la conformidad heredada.
- Colocar una retención legal en un bloque existente que tenga activada la conformidad heredada.
- Levantar una retención legal.

Consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5" si desea obtener instrucciones.

Si ha utilizado la función de cumplimiento de normativas heredada en una versión anterior de StorageGRID, consulte la siguiente tabla para saber cómo se compara con la función de bloqueo de objetos S3 de StorageGRID.

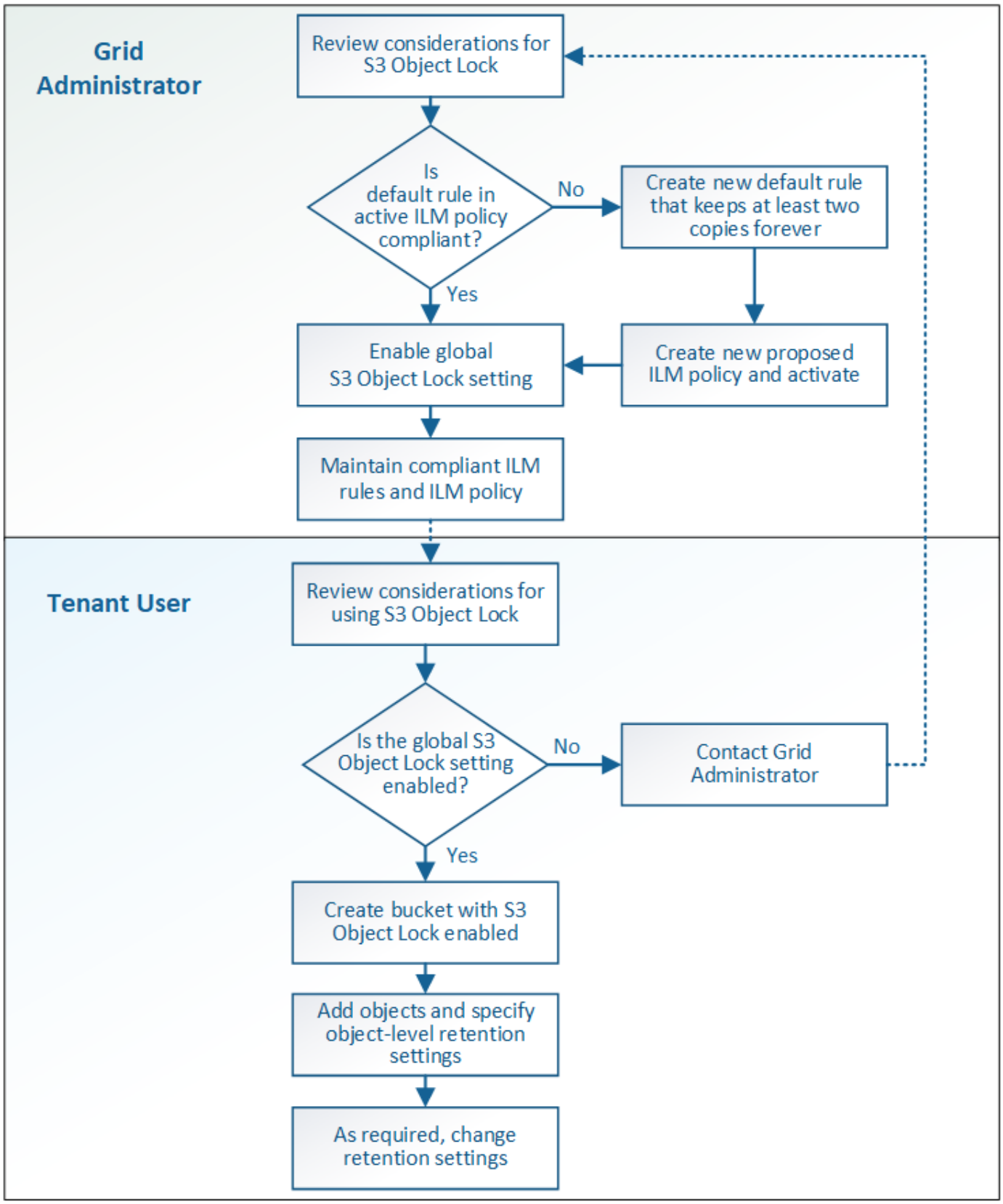
	Bloqueo de objetos de S3 (nuevo)	Cumplimiento (heredado)
¿Cómo se habilita la función a nivel global?	En Grid Manager, seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.	Ya no es compatible. **Nota:** Si ha activado la configuración de cumplimiento global con una versión anterior de StorageGRID, la configuración de bloqueo de objetos S3 está activada en StorageGRID 11.6. Puede seguir utilizando StorageGRID para gestionar la configuración de los bloques compatibles existentes; sin embargo, no puede crear nuevos bloques compatibles.
¿Cómo se habilita la función para un bloque?	Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo bloque con el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST de S3.	Los usuarios ya no pueden crear nuevos bloques con el cumplimiento habilitado; sin embargo, pueden continuar agregando objetos nuevos a bloques compatibles existentes.
¿Se admite el control de versiones de bloques?	Sí. El versionado de bloques se requiere y se habilita automáticamente si se habilita S3 Object Lock para el bloque.	No La función de cumplimiento heredado no permite el control de versiones de bloques.
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención hasta cada versión de objeto.	Los usuarios deben establecer un período de retención para todo el segmento. El período de retención se aplica a todos los objetos del bloque.
¿Puede un bloque tener la configuración predeterminada para la retención y la retención legal?	Sí. Los bloques StorageGRID que tienen el bloqueo de objetos S3 habilitado pueden tener un período de retención predeterminado que se aplica a las versiones de objetos que no tienen su propia configuración de retención especificada durante el procesamiento.	Sí
¿Se puede cambiar el período de retención?	La fecha de retención hasta la versión de un objeto se puede aumentar pero nunca disminuir.	El período de retención del cucharón se puede aumentar pero nunca disminuir.

	Bloqueo de objetos de S3 (nuevo)	Cumplimiento (heredado)
¿Dónde se controla la conservación legal?	Los usuarios pueden poner una retención legal o levantar una retención legal para cualquier versión de objeto en el cubo.	Se coloca una retención legal en el cubo y afecta a todos los objetos del cucharón.
¿Cuándo se pueden eliminar los objetos?	Una versión de objeto se puede eliminar después de alcanzar la fecha de retención hasta la fecha, suponiendo que el objeto no esté en espera legal.	Un objeto se puede eliminar después de que caduque el período de retención, suponiendo que el segmento no esté en retención legal. Los objetos se pueden eliminar de forma automática o manual.
¿Se admite la configuración del ciclo de vida de bloques?	Sí	No

Flujo de trabajo para bloqueo de objetos de S3

Como administrador de grid, debe coordinar estrechamente con los usuarios inquilinos a fin de asegurarse de que los objetos estén protegidos de forma que cumplan sus requisitos de retención.

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar el bloqueo de objetos de S3. Estos pasos los realiza el administrador de grid y los usuarios inquilinos.



Tareas del administrador de grid

Tal y como se muestra en el diagrama de flujo de trabajo, un administrador de grid debe ejecutar dos tareas de alto nivel para que los usuarios de inquilinos S3 puedan usar el bloqueo de objetos S3:

1. Cree al menos una regla de ILM que cumpla las normativas y convierta esa regla en la regla predeterminada en la política de ILM activa.
2. Habilite el valor global de Object Lock para todo el sistema StorageGRID.

Tareas del usuario inquilino

Una vez habilitada la configuración global de bloqueo de objetos S3, los inquilinos pueden realizar estas tareas:

1. Cree bloques con el bloqueo de objetos de S3 habilitado.
2. Especifique la configuración de retención predeterminada para el bloque, que se aplica a los objetos agregados al bloque que no especifican sus propias configuraciones de retención.
3. Agregue objetos a esos bloques y especifique los períodos de retención a nivel de objeto y la configuración de retención legal.
4. Según sea necesario, actualice un período de retención o cambie la configuración de retención legal de un objeto individual.

Información relacionada

- Usar una cuenta de inquilino
- Use S3
- Use la retención de bloque predeterminada de Object Lock de S3

Requisitos para el bloqueo de objetos de S3

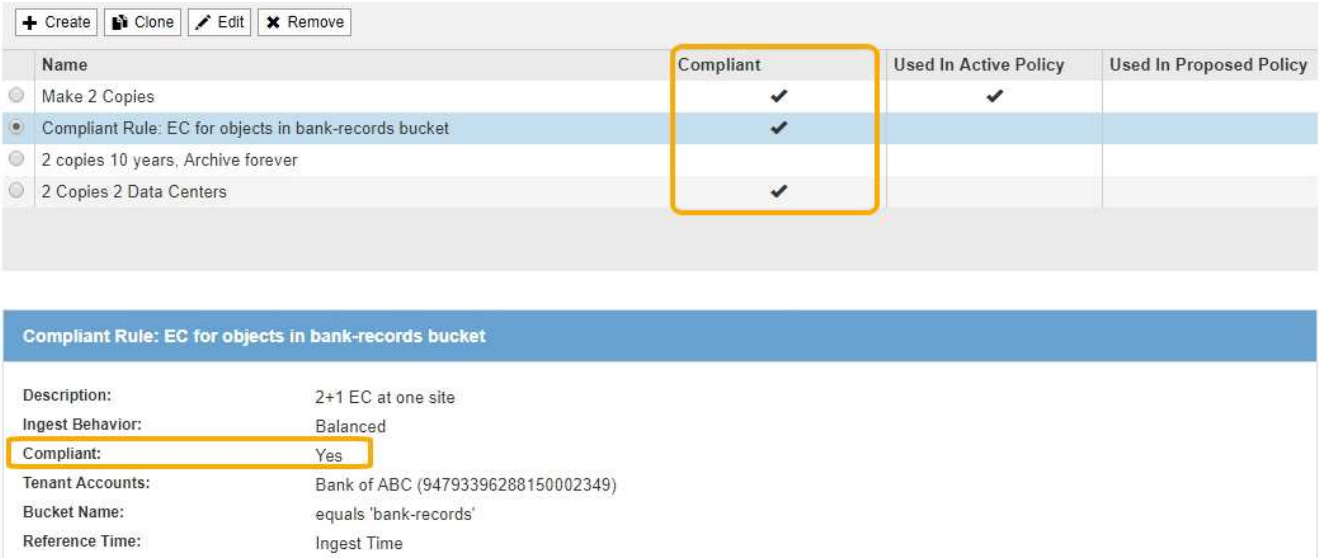
Debe revisar los requisitos para habilitar la configuración global de bloqueo de objetos de S3, los requisitos para crear reglas de ILM y políticas de ILM conformes con la normativa, y las restricciones que StorageGRID coloca en bloques y objetos que usan el bloqueo de objetos S3.

Requisitos para usar el valor global de bloqueo de objetos S3

- Debe habilitar la configuración global de Object Lock mediante el administrador de grid o la API de gestión de grid antes de que cualquier inquilino de S3 pueda crear un bucket con el bloqueo de objetos S3 habilitado.
- Al habilitar el ajuste global de Object Lock, todas las cuentas de inquilinos S3 pueden crear bloques con el bloqueo de objetos S3 habilitado.
- Después de habilitar la configuración global de bloqueo de objetos S3, no se puede deshabilitar esa opción.
- No puede habilitar el bloqueo de objetos global de S3 a menos que la regla predeterminada de la política de ILM activa sea *conforme a* (es decir, la regla predeterminada debe cumplir con los requisitos de los bloques con el bloqueo de objetos S3 habilitado).
- Cuando la configuración de bloqueo de objetos global de S3 está habilitada, no se puede crear una nueva política de ILM propuesta ni activar una política de ILM propuesta existente, a menos que la regla predeterminada de la política sea conforme con la normativa. Una vez habilitada la configuración global de bloqueo de objetos de S3, las páginas de reglas de ILM y políticas de ILM indican qué reglas de ILM son compatibles.

  En el siguiente ejemplo, la página de reglas de ILM enumera tres reglas que cumplen con los bloques con

el bloqueo de objetos S3 habilitado.

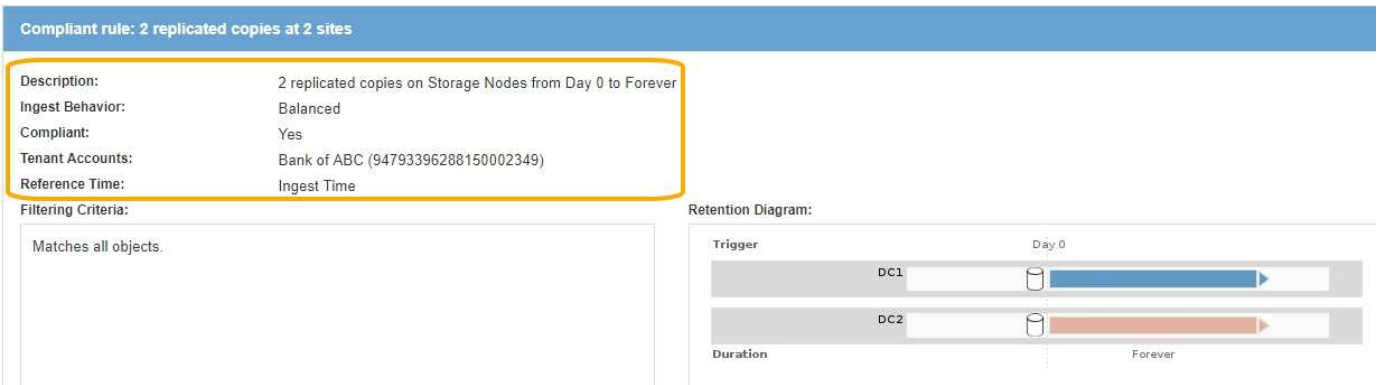


Requisitos para las reglas de ILM que cumplen con las normativas

Si desea habilitar la configuración global de bloqueo de objetos S3, debe asegurarse de que la regla predeterminada de la política de ILM activa sea compatible. Una regla conforme a las normativas satisface los requisitos de ambos bloques con el bloqueo de objetos S3 habilitado y de cualquier bloque existente con el cumplimiento de normativas heredado habilitado:

- Debe crear al menos dos copias de objetos replicados o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante todo el tiempo que dure cada línea en las instrucciones de colocación.
- Las copias de objetos no se pueden guardar en un pool de almacenamiento en cloud.
- Las copias de objetos no se pueden guardar en los nodos de archivado.
- Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando **tiempo de procesamiento** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación deberá ser «'para siempre».

Por ejemplo, esta regla satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado. Almacena dos copias de objetos replicados del tiempo de procesamiento (día 0) al estado «'eternamente». Los objetos se almacenarán en nodos de almacenamiento en dos centros de datos.



Requisitos para políticas de ILM activas y propuestas

Cuando se habilita la configuración global de bloqueo de objetos S3, las políticas de ILM activas y propuestas pueden incluir reglas tanto conformes a la normativa como no.

- La regla predeterminada de la política de ILM activa o propuesta debe ser conforme.
- Las reglas no compatibles solo se aplican a los objetos en bloques que no tienen habilitada el bloqueo de objetos S3 o que no tienen habilitada la función de cumplimiento heredada.
- Las reglas que cumplen las normativas se pueden aplicar a los objetos de cualquier bloque; no es necesario habilitar el bloqueo de objetos S3 o la conformidad heredada para el bloque.

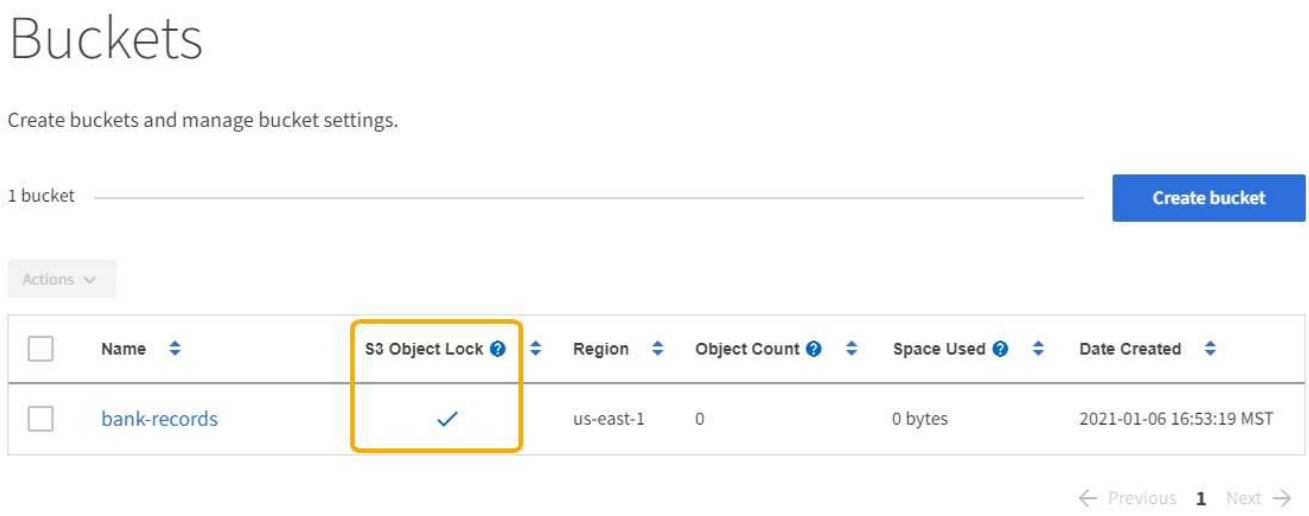
Una política de ILM compatible puede incluir estas tres reglas:

1. Se trata de una regla que crea copias de los objetos con código de borrado en un bloque específico con el bloqueo de objetos S3 habilitado. Las copias EC se almacenan en nodos de almacenamiento del día 0 al permanente.
2. Una regla no compatible que crea dos copias de objetos replicadas en los nodos de almacenamiento durante un año y, a continuación, mueve una copia de objetos a los nodos de archivado y almacena esa copia para siempre. Esta regla solo se aplica a bloques que no tienen habilitado el bloqueo de objetos S3 o el cumplimiento heredado, ya que solo almacena una copia de objeto para siempre y utiliza nodos de archivado.
3. Una regla predeterminada que cumple con las normativas crea dos copias de objetos replicados en los nodos de almacenamiento del día 0 al permanente. Esta regla se aplica a cualquier objeto de cualquier segmento que no haya sido filtrado por las dos primeras reglas.

Requisitos para bloques con bloqueo de objetos de S3 habilitado

- Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede usar el administrador de inquilinos, la API de gestión de inquilinos o la API REST de S3 para crear bloques con el bloqueo de objetos S3 habilitado.

  Este ejemplo del Administrador de inquilinos muestra un bloque con el bloqueo de objetos S3 habilitado.



- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No es posible habilitar el bloqueo de objetos de S3 para un bloque existente.
- Se requiere el versionado de bloques con S3 Object Lock. Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque.

- Después de crear un bloque con el bloqueo de objetos S3 habilitado, no se puede deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones de ese bloque.
- Si lo desea, puede configurar la retención predeterminada para un bloque. Cuando se carga una versión de objeto, la retención predeterminada se aplica a la versión del objeto. Puede anular el valor predeterminado de bloque especificando un modo de retención y retener hasta la fecha en la solicitud para cargar una versión de objeto.
- Se admite la configuración del ciclo de vida de bloques para los bloques del ciclo de vida de objetos S3.
- La replicación de CloudMirror no es compatible para bloques con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en bloques con S3 Object Lock habilitado

- Para proteger una versión de objeto, la aplicación cliente S3 debe configurar la retención predeterminada de bloques o especificar la configuración de retención en cada solicitud de carga.
- Puede aumentar la fecha de retención hasta una versión de objeto, pero nunca puede disminuir este valor.
- Si recibe una notificación de una acción legal pendiente o una investigación normativa, puede conservar la información relevante colocando una retención legal en una versión del objeto. Cuando una versión de objeto se encuentra bajo una retención legal, ese objeto no se puede eliminar de StorageGRID, aunque haya alcanzado su fecha de retención. Tan pronto como se levante la retención legal, la versión del objeto se puede eliminar si se ha alcanzado la fecha de retención.
- El bloqueo de objetos de S3 requiere el uso de bloques con versiones. La configuración de retención se aplica a versiones individuales de objetos. Una versión de objeto puede tener una configuración de retención hasta fecha y una retención legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta fecha o de retención legal para un objeto, sólo se protege la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en bloques con S3 Object Lock habilitado

Cada objeto que se guarda en un bloque con el bloqueo de objetos S3 habilitado atraviesa tres etapas:

1. **Procesamiento de objetos**
   - Cuando se añade una versión de objeto a un bloque con S3 Object Lock habilitado, la aplicación cliente S3 puede usar la configuración de retención de bloque predeterminada o especificar, opcionalmente, la configuración de retención para el objeto (retenga hasta la fecha, la conservación legal o ambos). A continuación, StorageGRID genera metadatos para ese objeto, que incluye un identificador de objeto (UUID) único y la fecha y la hora de procesamiento.
   - Después de procesar una versión de objeto con configuración de retención, sus datos y los metadatos definidos por el usuario de S3 no se pueden modificar.
   - StorageGRID almacena los metadatos del objeto de forma independiente de los datos del objeto. Mantiene tres copias de todos los metadatos de objetos en cada sitio.
2. **Retención de objetos**
   - StorageGRID almacena varias copias del objeto. El número y el tipo exactos de copias y las ubicaciones del almacenamiento se determinan según las reglas conformes de la política de ILM activa.
3. **Eliminación de objetos**
   - Un objeto se puede eliminar cuando se alcanza su fecha de retención.
   - No se puede eliminar un objeto que se encuentra bajo una retención legal.

Información relacionada

- Usar una cuenta de inquilino
- Use S3
- Comparación del bloqueo de objetos de S3 con el cumplimiento de normativas heredado
- Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3
- Revisar los registros de auditoría
- Use la retención de bloque predeterminada de Object Lock de S3.

Habilite el bloqueo de objetos de S3 globalmente

Si una cuenta de inquilino de S3 tiene que cumplir con los requisitos de normativa al guardar datos de objetos, debe habilitar el bloqueo de objetos de S3 para todo el sistema StorageGRID. Al habilitar el ajuste global de bloqueo de objetos de S3, cualquier usuario inquilino de S3 puede crear y gestionar bloques y objetos con S3 Object Lock.

Lo que necesitará

- Tiene el permiso acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Ha revisado el flujo de trabajo de bloqueo de objetos de S3 y debe comprender estas consideraciones.
- La regla predeterminada de la política de ILM activa es compatible.
  - Cree una regla de ILM predeterminada
  - Cree una política de ILM

Acerca de esta tarea

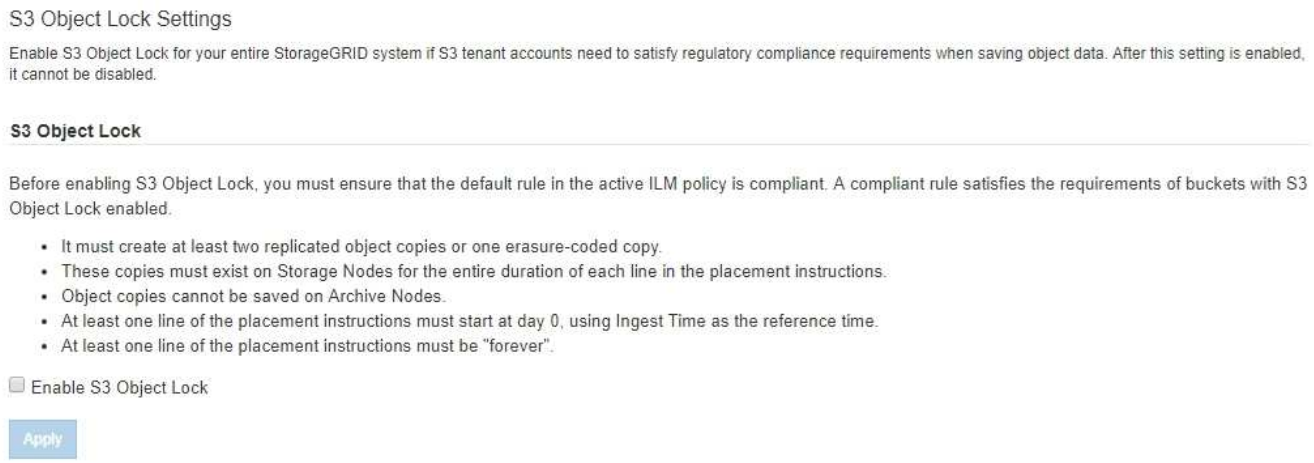
Un administrador de grid debe habilitar la configuración global de bloqueo de objetos S3 para permitir a los usuarios inquilinos crear nuevos bloques con el bloqueo de objetos S3 habilitado. Una vez que este ajuste está activado, no se puede desactivar.

> Si habilitó la opción de cumplimiento global mediante una versión anterior de StorageGRID, la opción de bloqueo de objetos S3 se habilita en StorageGRID 11.6. Puede seguir utilizando StorageGRID para gestionar la configuración de los bloques compatibles existentes; sin embargo, no puede crear nuevos bloques compatibles. Consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

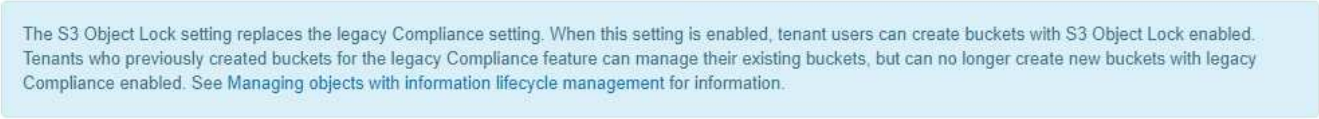
Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.

   Se muestra la página S3 Object Lock Settings.



Si ha habilitado la configuración de cumplimiento global con una versión anterior de StorageGRID, la página incluye la siguiente nota:



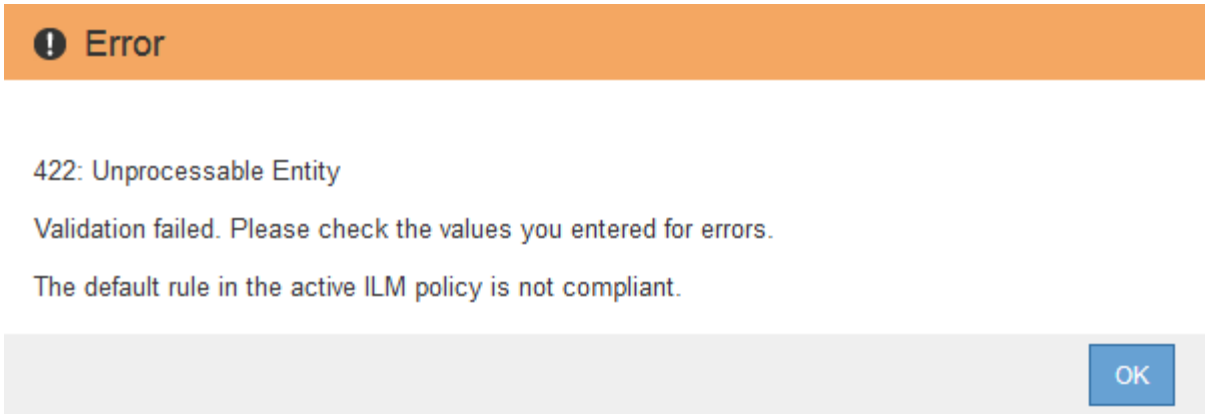
2. Seleccione **Activar el bloqueo de objetos S3**.
3. Seleccione **aplicar**.

   Aparece un cuadro de diálogo de confirmación que le recuerda que no puede deshabilitar el bloqueo de objetos S3 después de estar activado.

4. Si está seguro de que desea activar de forma permanente el bloqueo de objetos S3 para todo el sistema, seleccione **Aceptar**.

   Al seleccionar **Aceptar**:

   - Si la regla predeterminada de la política de ILM activa es compatible, el bloqueo de objetos S3 ahora está habilitado para toda la cuadrícula y no puede deshabilitarse.
   - Si la regla predeterminada no es compatible, aparece un error que indica que debe crear y activar una nueva política de ILM que incluya una regla de cumplimiento como regla predeterminada. Seleccione **Aceptar**, cree una nueva directiva propuesta, simule y actívela.



Después de terminar

Después de habilitar la configuración global de bloqueo de objetos S3, es posible que deba hacerlo cree una regla predeterminada eso es compatible y. Cree una política de ILM eso es conforme. Una vez activada la configuración, la política de ILM puede incluir de manera opcional una regla predeterminada que cumpla las normativas y una regla predeterminada que no sea compatible. Por ejemplo, puede que desee usar una regla no conforme a la normativa que no tenga filtros para los objetos de los bloques que no tengan habilitado el bloqueo de objetos S3.

Información relacionada

- Compare el bloqueo de objetos de S3 con el cumplimiento de normativas heredado

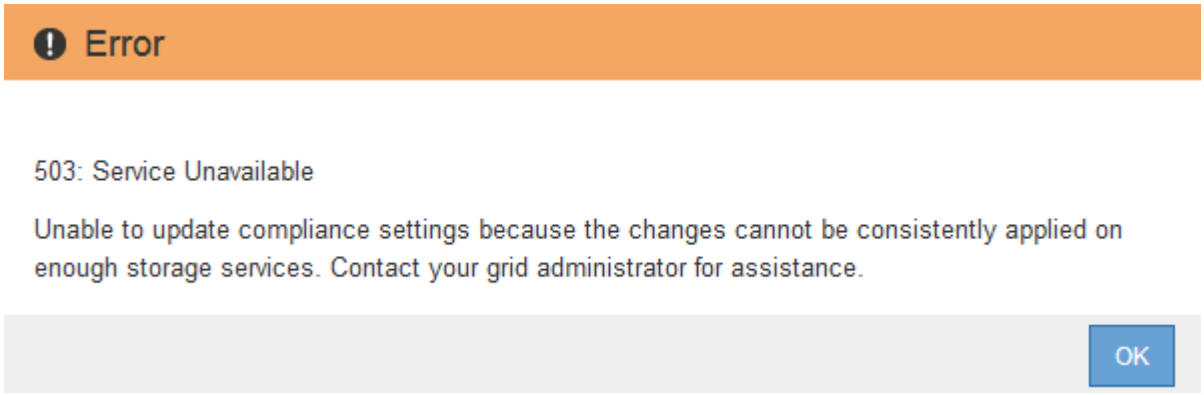
Resuelva los errores de coherencia al actualizar la configuración de bloqueo de objetos de S3 o cumplimiento heredado

Si un sitio de centro de datos o varios nodos de almacenamiento de un sitio no están disponibles, es posible que deba ayudar a los usuarios inquilinos S3 a aplicar los cambios en la configuración del bloqueo de objetos S3 o del cumplimiento heredado.

Los usuarios inquilinos que tienen bloques con S3 Object Lock (o Legacy Compliance) habilitado pueden cambiar ciertas opciones. Por ejemplo, es posible que un usuario arrendatario que utilice el bloqueo de objetos S3 deba poner una versión de objeto en retención legal.

Cuando un usuario tenant actualiza la configuración de un bloque de S3 o una versión de objeto, StorageGRID intenta actualizar inmediatamente los metadatos del objeto o el bloque en el grid. Si el sistema no puede actualizar los metadatos debido a que un sitio de centro de datos o varios nodos de almacenamiento no están disponibles, se muestra un mensaje de error. Específicamente:

- Los usuarios de tenant Manager ven el siguiente mensaje de error:



- Los usuarios de la API de gestión de inquilinos y los usuarios de la API S3 reciben un código de respuesta de `503 Service Unavailable` con texto de mensaje similar.

Para resolver este error, siga estos pasos:

1. Se debe intentar que todos los nodos o sitios de almacenamiento estén disponibles de nuevo Lo antes posible..
2. Si no puede dejar suficientes nodos de almacenamiento en cada sitio disponible, póngase en contacto con el soporte técnico, que puede ayudarle a recuperar nodos y asegurarse de que los cambios se apliquen de manera coherente en la cuadrícula.
3. Una vez resuelto el problema subyacente, recuerde al usuario inquilino que vuelva a intentar cambiar sus cambios de configuración.

Información relacionada

- Usar una cuenta de inquilino
- Use S3
- Recuperación y mantenimiento

Ejemplo de reglas y políticas de ILM

Ejemplo 1: Reglas de ILM y políticas para el almacenamiento de objetos

Es posible usar las siguientes reglas y políticas de ejemplo como punto de inicio al definir una política de ILM para cumplir con los requisitos de retención y protección de objetos.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Regla 1 de ILM, por ejemplo 1: Copiar datos de objetos en dos centros de datos

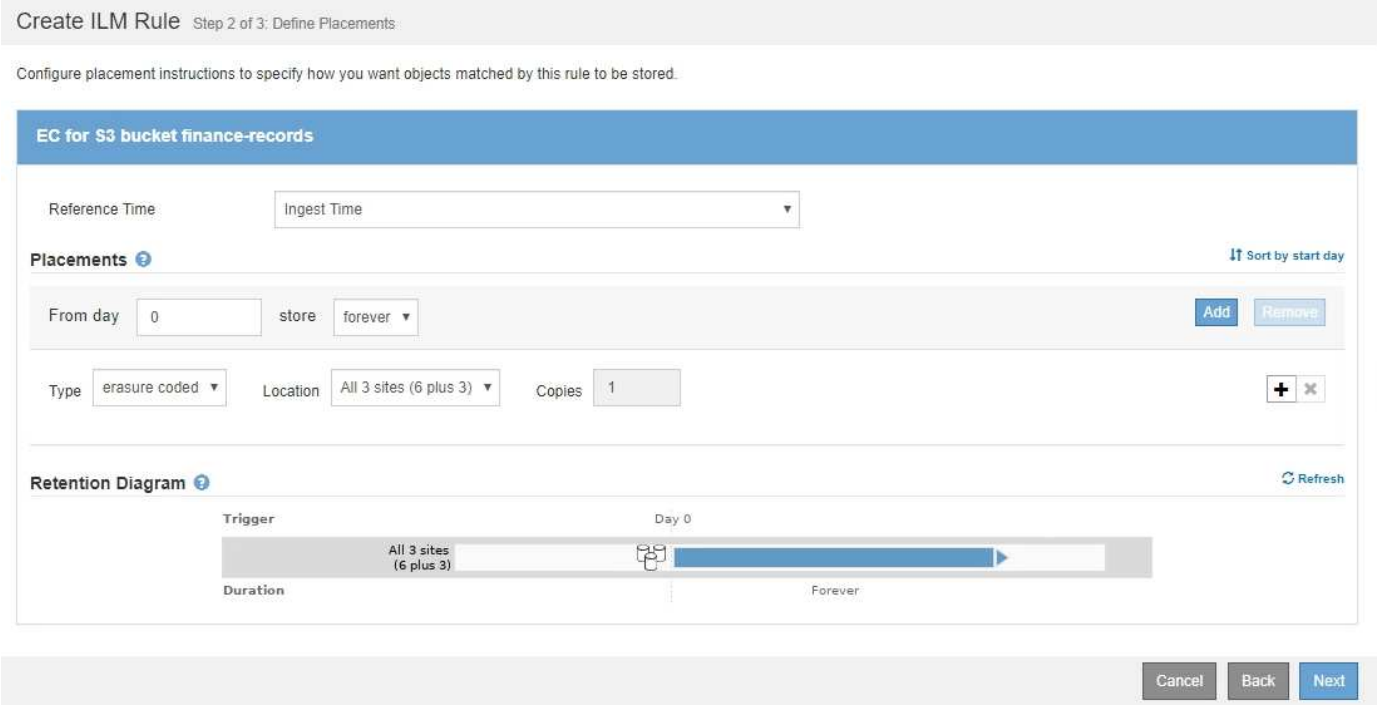
Esta regla de ILM de ejemplo copia los datos de objetos en dos pools de almacenamiento en dos centros de datos.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos pools de almacenamiento, cada uno en centros de datos diferentes, llamados Storage Pool DC1 y Storage Pool DC2.
Nombre de regla	Dos copias dos centros de datos
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	El día 0, mantenga dos copias replicadas para siempre: Una en el DC1 del pool de almacenamiento y otra en el DC2 del pool de almacenamiento.

Regla 2 de ILM por ejemplo 1: Perfil de código de borrado con coincidencia de bloques

Esta regla de ILM de ejemplo utiliza un perfil de código de borrado y un bloque de S3 para determinar dónde y cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Perfil de código de borrado	• Un único pool de almacenamiento en tres centros de datos (los 3 sitios) • Utilice un esquema de codificación de borrado de 6+3
Nombre de regla	EC para registros financieros de bloques de S3
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	Para los objetos del bloque de S3 denominados registros financieros, cree una copia con código de borrado en el pool especificado por el perfil de código de borrado. Guarde esta copia para siempre.



Política de ILM, por ejemplo 1

El sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas; sin embargo, en la práctica, la mayoría de las políticas de ILM son simples.

Una política de ILM típica de una topología de varios sitios puede incluir reglas de ILM como las siguientes:

- Durante la ingesta, use la codificación de borrado 6+3 para almacenar todos los objetos que pertenecen al bloque de S3 denominado `finance-records` en tres centros de datos.
- Si un objeto no coincide con la primera regla de ILM, utilice la regla de ILM predeterminada de la política, dos copias de dos centros de datos, para almacenar una copia de ese objeto en dos centros de datos,

DC1 y DC2.

Ejemplo 2: Reglas de ILM y política para el filtrado de tamaño de objetos de EC

Puede usar las siguientes reglas y políticas de ejemplo como puntos de inicio para definir una política de ILM que filtra por tamaño de objeto para cumplir los requisitos de EC recomendados.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Regla de ILM 1 por ejemplo 2: Utilice EC para objetos de más de 1 MB

Este ejemplo codifica los objetos de borrado de regla ILM que tienen más de 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

Definición de regla	Valor de ejemplo
Nombre de regla	Sólo objetos de EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtrado avanzado para el tamaño del objeto	Tamaño de objeto (MB) mayor que 1
Colocación del contenido	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones

Regla de ILM 2 por ejemplo 2: Dos copias replicadas

Esta regla de ILM de ejemplo crea dos copias replicadas y no filtra por el tamaño del objeto. Esta regla es la regla predeterminada para la directiva. Dado que la primera regla filtra todos los objetos mayores de 1 MB, esta regla sólo se aplica a objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de regla	Dos copias replicadas
Tiempo de referencia	Tiempo de ingesta
Filtrado avanzado para el tamaño del objeto	Ninguno
Colocación del contenido	Cree dos copias replicadas y guárdelas en dos centros de datos, DC1 y DC2

Política de ILM, por ejemplo 2: Usar EC para objetos de más de 1 MB

Este ejemplo de política de ILM incluye dos reglas ILM:

- La primera regla de borrado codifica todos los objetos que sean mayores de 1 MB.
- La segunda regla de ILM (predeterminada) crea dos copias replicadas. Dado que los objetos mayores de 1 MB se han filtrado mediante la regla 1, la regla 2 sólo se aplica a objetos de 1 MB o menos.

Ejemplo 3: Reglas de ILM y política para mejorar la protección de los archivos de imagen

Puede utilizar las siguientes reglas y políticas de ejemplo a fin de garantizar que las imágenes mayores de 1 MB estén codificadas para el borrado y que haya dos copias de imágenes más pequeñas.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

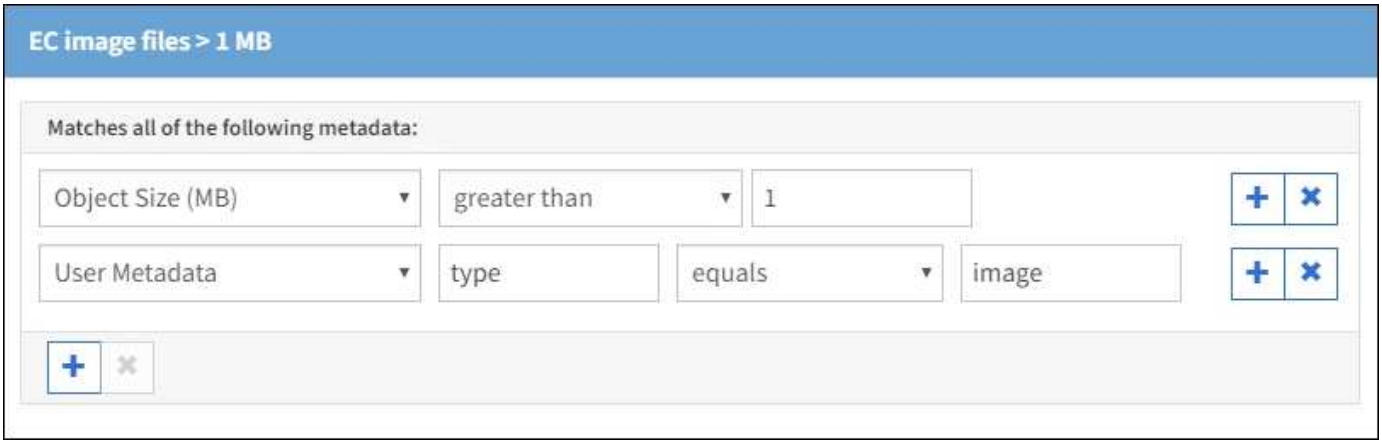
Regla ILM 1 por ejemplo 3: Utilice EC para archivos de imagen superiores a 1 MB

En esta regla de ILM de ejemplo se utiliza un filtrado avanzado para borrar el código de todos los archivos de imagen superiores a 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

Definición de regla	Valor de ejemplo
Nombre de regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingesta

Definición de regla	Valor de ejemplo
Filtrado avanzado para el tamaño del objeto	Tamaño de objeto (MB) mayor que 1.0
Filtrado avanzado para metadatos de usuario	El tipo de metadatos de usuario es igual a la imagen
Colocación del contenido	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones



Dado que esta regla se configura como la primera regla de la política, la instrucción de colocación de codificación de borrado sólo se aplica a las imágenes que son superiores a 1 MB.

Regla ILM 2 por ejemplo 3: Cree 2 copias replicadas para todos los archivos de imagen restantes

En este ejemplo, la regla ILM utiliza un filtrado avanzado para especificar que se repliquen los archivos de imagen más pequeños. Dado que la primera regla de la directiva ya coincide con los archivos de imagen superiores a 1 MB, esta regla se aplica a los archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de regla	2 copias para archivos de imagen
Tiempo de referencia	Tiempo de ingesta
Filtrado avanzado para metadatos de usuario	El tipo de metadatos de usuario equivale a los archivos de imagen
Colocación del contenido	Cree 2 copias replicadas en dos pools de almacenamiento

Política de ILM, por ejemplo 3: Mejor protección para los archivos de imagen

Este ejemplo de política de ILM incluye tres reglas:

- La primera regla de borrado codifica todos los archivos de imagen mayores de 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 de imagen).

Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3

Si tiene un bloque de S3 con el control de versiones activado, puede gestionar las versiones de objetos no actuales incluyendo reglas en su política de ILM que utilicen **tiempo no corriente** como tiempo de referencia.

Como se muestra en este ejemplo, puede controlar la cantidad de almacenamiento que utilizan los objetos con versiones utilizando instrucciones de colocación diferentes para las versiones de objetos no actuales.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

> Si crea políticas de ILM para gestionar versiones de objetos no actuales, tenga en cuenta que debe conocer el UUID o el CBID de la versión del objeto para simular la política. Para buscar el UUID y el CBID de un objeto, utilice Búsqueda de metadatos de objetos mientras el objeto sigue estando actualizado. Consulte Comprobar una política de ILM con la búsqueda de metadatos de objetos.

Información relacionada

- Cómo se eliminan los objetos

Regla 1 de ILM, por ejemplo 4: Guarde tres copias durante 10 años

Esta regla de ILM de ejemplo almacena una copia de cada objeto en tres centros de datos durante 10 años.

Esta regla se aplica a todos los objetos, con o sin versiones.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Tres pools de almacenamiento, cada uno en centros de datos diferentes, denominados DC1, DC2 y DC3.
Nombre de regla	Tres copias diez años
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	En el día 0, guarde tres copias replicadas durante 10 años (3,652 días), una en CD1, una en DC2 y una en CD3. Al final de 10 años, elimine todas las copias del objeto.

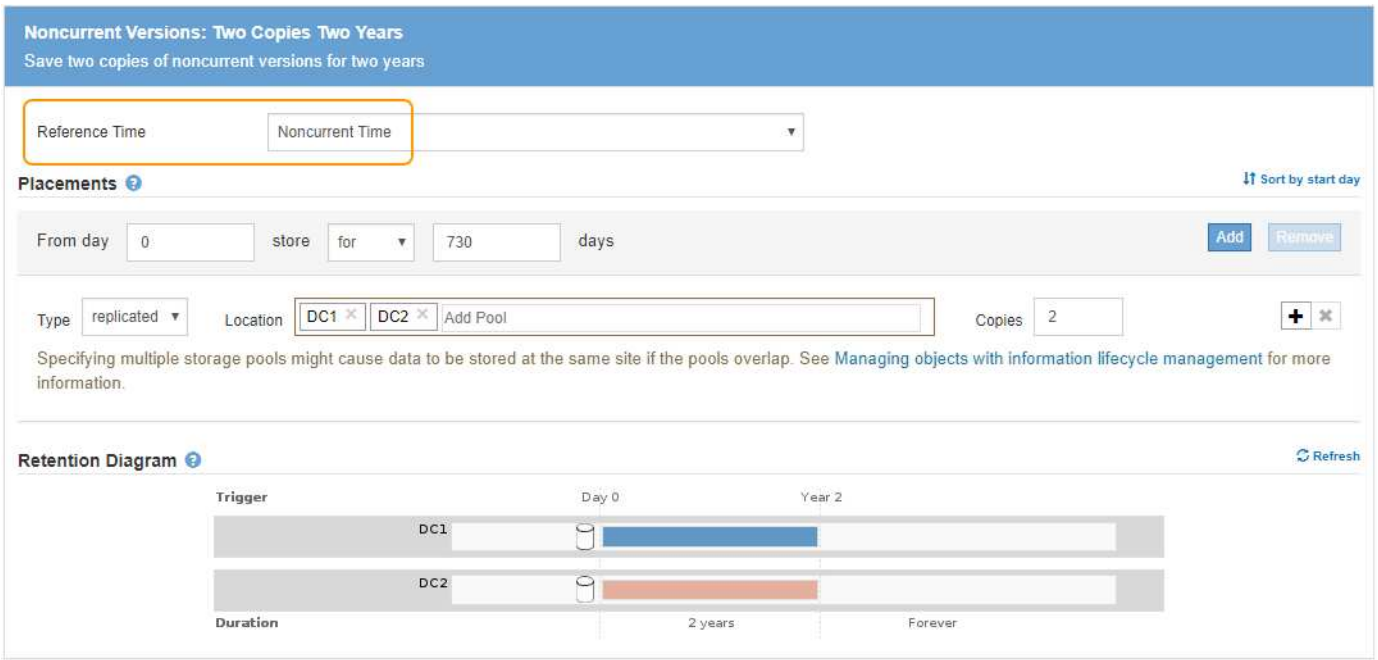
Regla de ILM 2 por ejemplo 4: Guarde dos copias de las versiones no corrientes durante 2 años

Esta regla de ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto con versiones de S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debe crear otra regla para filtrar las versiones no actuales. Esta regla utiliza la opción **tiempo no corriente** para tiempo de referencia.

En este ejemplo, sólo se almacenan dos copias de las versiones no corrientes, y esas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos pools de almacenamiento, cada uno en centros de datos diferentes, denominados DC1 y DC2.
Nombre de regla	Versiones no corrientes: Dos copias dos años
Tiempo de referencia	Hora no actual
Colocación del contenido	El día 0 en relación con la hora no corriente (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 de objeto no corrientes durante 2 años (730 días), una en DC1 y otra en DC2. Al final de 2 años, elimine las versiones no actuales.



Política de ILM, por ejemplo 4: Objetos con versiones de S3

Si desea administrar versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilizan **Hora no corriente** como Hora de referencia deben aparecer en la directiva ILM antes de las reglas que se aplican a la versión actual del objeto.

Una política de ILM para objetos con versiones de S3 puede incluir reglas de ILM como las siguientes:

- Mantenga las versiones antiguas (no actuales) de cada objeto durante 2 años, a partir del día en que la versión se volvió no actual.

> Las reglas de tiempo no corrientes deben aparecer en la directiva antes de las reglas que se aplican a la versión de objeto actual. De lo contrario, las versiones de objeto no actuales nunca serán coincidentes con la regla de tiempo no corriente.

- Cuando se procesa, cree tres copias replicadas y almacene una copia en cada uno de los tres centros de datos. Guarde copias de la versión actual del objeto durante 10 años.

Al simular la directiva de ejemplo, se esperaría que los objetos de prueba se evaluaran de la siguiente manera:

- Cualquier versión de objeto no actual se haría coincidir con la primera regla. Si una versión de objeto no actual tiene más de 2 años, ILM lo elimina de forma permanente (todas las copias de la versión no actual se eliminan de la cuadrícula).

> Para simular versiones de objeto no actuales, debe utilizar el UUID o CBID de esa versión. Mientras el objeto sigue siendo actual, puede utilizar Búsqueda de metadatos de objetos para buscar su UUID y CBID.

- 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 DELETE como la versión actual del objeto, y hace que la versión anterior del objeto '"no actual"'. La próxima vez que se realice la evaluación de ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en DC3 se purga y las dos copias en DC1 y DC2 se almacenan durante dos años más.

Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto

Puede usar un filtro de ubicación y el comportamiento de ingesta estricto de 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 preocupaciones regulatorias. Otros objetos, incluidos todos los objetos de otras cuentas de inquilino, pueden almacenarse 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. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Información relacionada

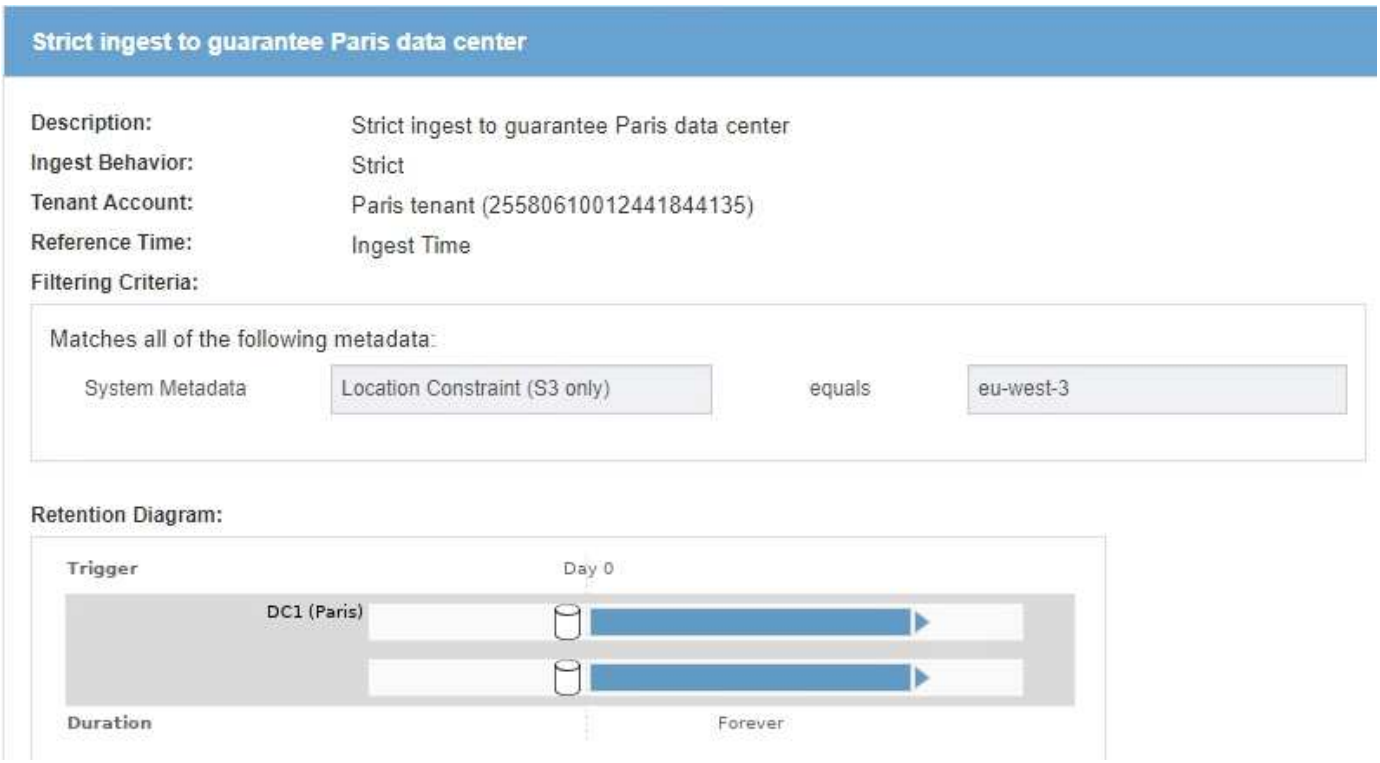
- Opciones de protección de datos para consumo
- Paso 3 de 3: Definir el comportamiento de la ingesta

Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

Esta regla de ILM de ejemplo usa el comportamiento de ingesta estricto para garantizar que los objetos que ha ahorrado un inquilino basado en París en cubos S3 con la región establecida en la región eu-West-3 (París) nunca se almacenen en el centro de datos de EE. UU.

Esta regla se aplica a objetos que pertenecen al arrendatario de París y que tienen la región de cubo S3 establecida en eu-West-3 (París).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Inquilino de París
Filtrado avanzado	La limitación de ubicación es igual a la ue-oeste-3
Pools de almacenamiento	CD1 (París)
Nombre de regla	Ingesta estricta para garantizar el centro de datos París
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	El día 0, conservar para siempre dos copias replicadas en DC1 (París)
Comportamiento de ingesta	Estricto. Utilice siempre las colocaciones de esta regla durante el procesamiento. 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 de otros objetos

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta equilibrada para proporcionar una eficiencia de ILM óptima para cualquier objeto que no sea coincidente con la primera regla. Se almacenarán dos copias de todos los objetos compatibles con esta regla: Una en el centro de datos estadounidense y una en el centro de datos de París. Si la regla no se puede satisfacer inmediatamente, las copias provisionales se almacenan en cualquier ubicación disponible.

Esta regla se aplica a objetos que pertenecen a cualquier arrendatario y a cualquier región.

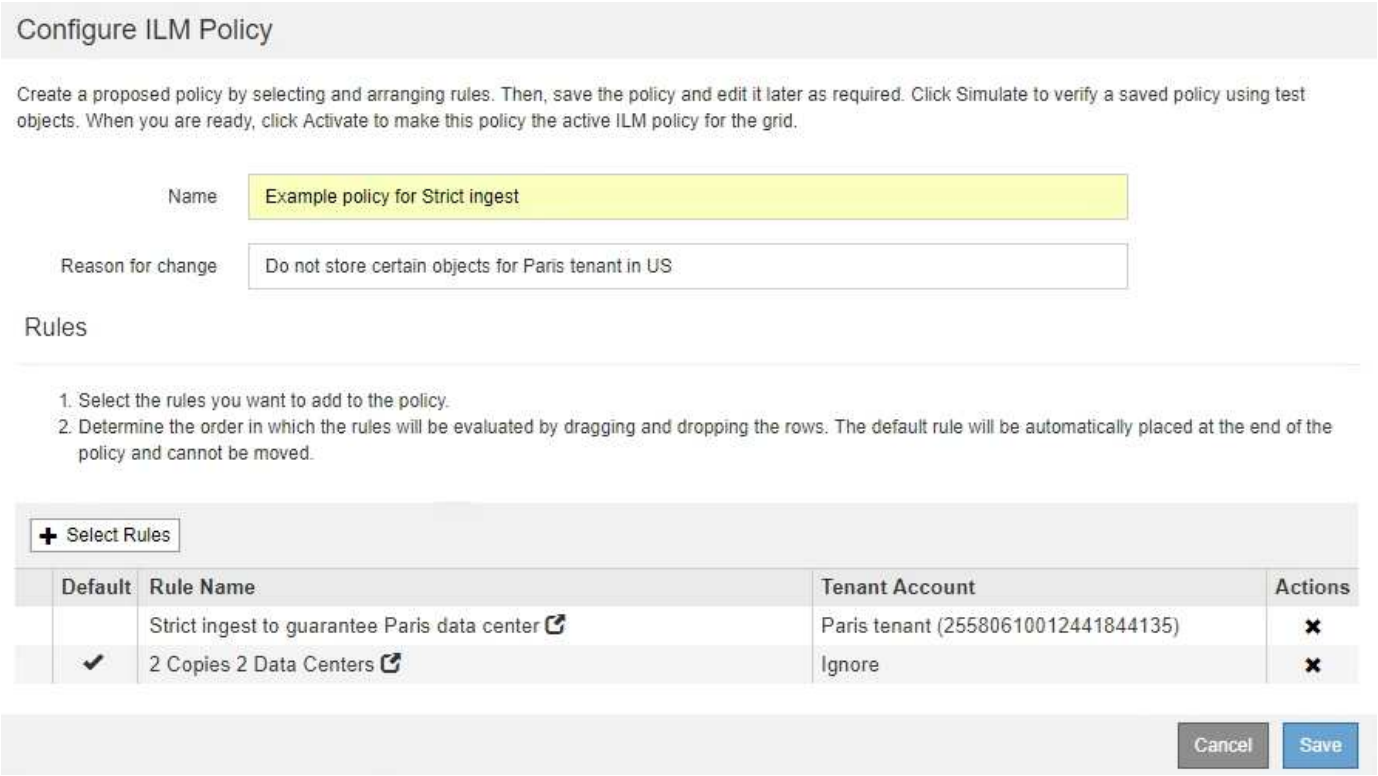
Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtrado avanzado	*No especificado*
Pools de almacenamiento	DC1 (París) y DC2 (EE. UU.)
Nombre de regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	Desde el día 0, mantenga dos copias replicadas 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 colocación de la regla, si es posible. De lo contrario, las copias provisionales se realizan en cualquier lugar disponible.

Política de ILM, por ejemplo 5: Combinar comportamientos de consumo

La política de ILM de ejemplo incluye dos reglas que tienen comportamientos de consumo diferentes.

Una política de ILM que usa dos comportamientos de consumo diferentes puede incluir reglas de ILM como las siguientes:

- Almacene objetos que pertenecen al inquilino de París y que tienen la región de cubo de S3 establecida en eu-West-3 (París) solo en el centro de datos de París. No se procese correctamente si el centro de datos de París no está disponible.
- Almacenar todos los demás objetos (incluidos los que pertenecen al inquilino de París, pero que tienen una región de bloques diferente) tanto en el centro de datos de EE. UU. Como en el de París. Haga copias provisionales en cualquier ubicación disponible si no se puede cumplir la instrucción de colocación.



Al simular la directiva de ejemplo, espera que los objetos de prueba se evalúen de la siguiente forma:

- Cualquier objeto que pertenezca al inquilino de París y que tenga la región de bloque de S3 establecida en eu-West-3 se ajusta a la primera regla y se almacena en el centro de datos de París. Como la primera regla usa un procesamiento estricto, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los nodos de almacenamiento del centro de datos de París no están disponibles, la ingesta falla.
- Todos los demás objetos se comparan con la segunda regla, incluidos los objetos que pertenecen al inquilino de París y que no tienen la región de cubo S3 establecida en eu-West-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, como la segunda regla utiliza procesamiento equilibrado, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Ejemplo 6: Cambiar una política de ILM

Es posible que deba crear y activar una nueva política de ILM si sus necesidades de protección de datos cambian o si añade nuevos sitios.

Antes de cambiar una política, debe comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente al rendimiento general de un sistema StorageGRID.

En este ejemplo, se ha añadido un nuevo sitio StorageGRID en una ampliación y se debe revisar la política activa de ILM para almacenar datos en el nuevo sitio.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

¿Cómo afecta el rendimiento el cambio de una política de ILM

Al activar una nueva política de ILM, el rendimiento de su sistema StorageGRID puede verse afectado temporalmente, especialmente si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se muevan a nuevas ubicaciones.

> Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Entre los tipos de cambios en la política de ILM que pueden afectar temporalmente el rendimiento de la StorageGRID se encuentran los siguientes:

- Aplicar un perfil de codificación de borrado diferente a los objetos existentes codificados con borrado.

  > StorageGRID considera que cada perfil de código de borrado es único y no reutiliza fragmentos de código de borrado cuando se utiliza un perfil nuevo.

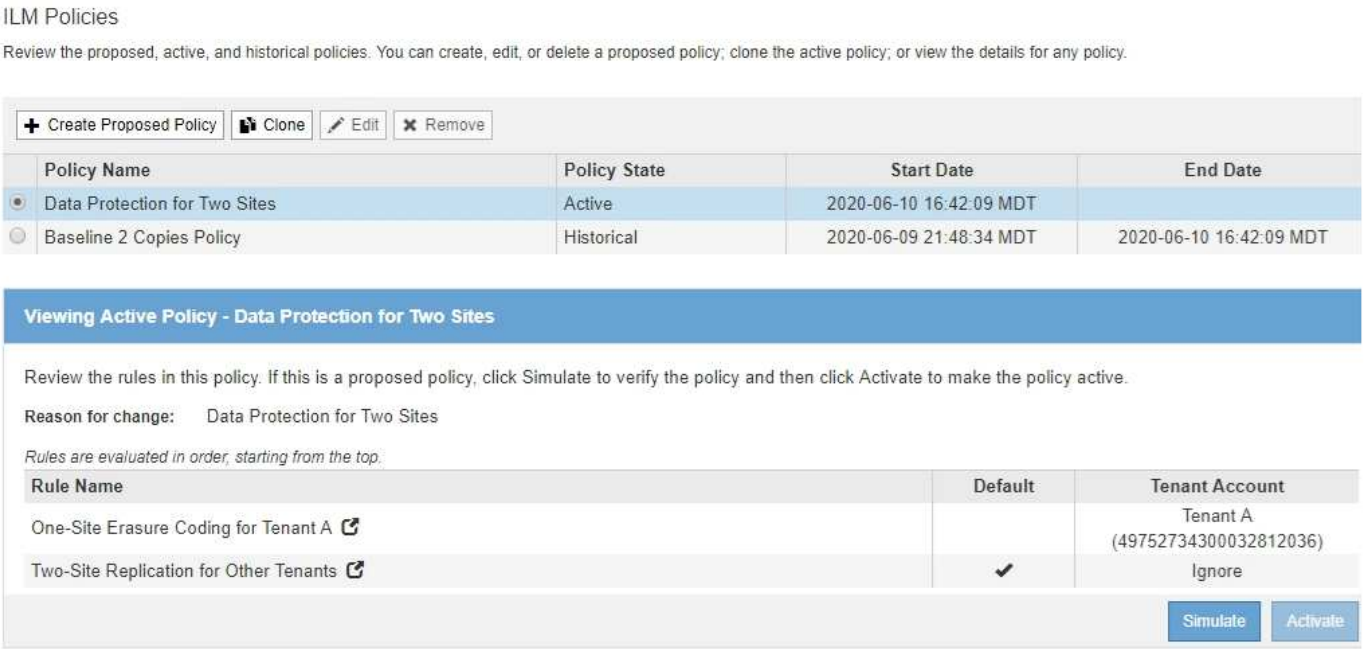
- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos de código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover un gran número de objetos hacia o desde un pool de almacenamiento en cloud, o desde un sitio remoto.

Información relacionada

Cree una política de ILM

Política de ILM activa, por ejemplo 6: Protección de datos en dos sitios

En este ejemplo, la activa política de ILM se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas de ILM.



En esta política de ILM, los objetos del inquilino A están protegidos con codificación de borrado 2+1 en un único sitio, mientras que los objetos que pertenecen al resto de usuarios se protegen en dos sitios mediante replicación de copia.

> La primera regla de este ejemplo utiliza un filtro avanzado para garantizar que la codificación de borrado no se utilice para objetos pequeños. Cualquiera de los objetos del arrendatario A que sean menores de 1 MB estará protegido por la segunda regla, que utiliza la replicación.

Regla 1: Codificación de borrado de un sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de regla	Codificación de borrado de un sitio para el inquilino A
Cuenta de inquilino	Inquilinoa
Pool de almacenamiento	Centro de datos 1
Colocación del contenido	Codificación de borrado 2+1 en el centro de datos 1 del día 0 al para siempre

Regla 2: Replicación de dos sitios para otros inquilinos

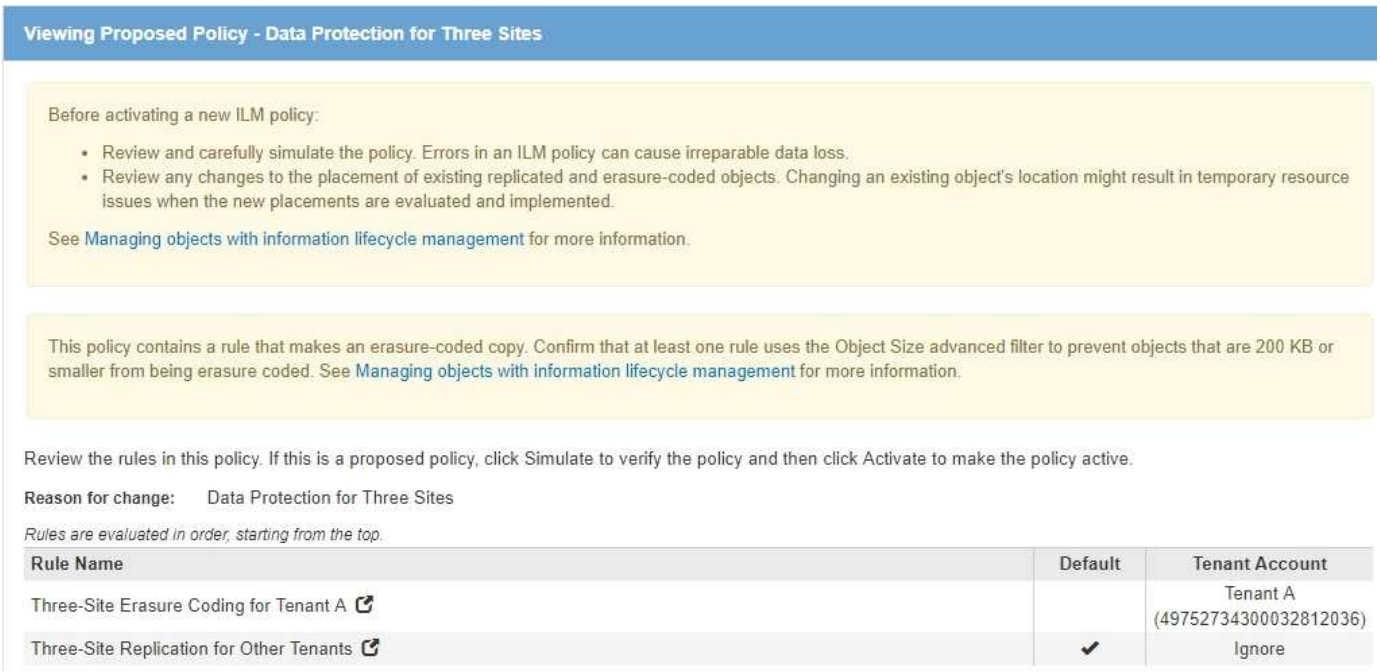
Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de dos sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Data Center 1 y Data Center 2

Definición de regla	Valor de ejemplo
Colocación del contenido	Dos copias replicadas del día 0 para siempre: Una copia en el centro de datos 1 y una copia en el centro de datos 2.

Propuesta de política de ILM, por ejemplo 6: Protección de datos en tres sitios

En este ejemplo, se está actualizando la política de ILM para un sistema StorageGRID de tres sitios.

Tras realizar una ampliación para añadir el nuevo sitio, el administrador de grid creó dos nuevos pools de almacenamiento: Un pool de almacenamiento para Data Center 3 y un pool de almacenamiento que contiene los tres sitios (no es lo mismo que el pool de almacenamiento predeterminado de todos los nodos de almacenamiento). Posteriormente, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM propuesta, diseñada para proteger datos en los tres sitios.



Cuando se activa esta nueva política de ILM, los objetos que pertenecen al inquilino A se protegerán mediante codificación de borrado 2+1 en tres sitios, mientras que los objetos que pertenecen a otros clientes (y objetos más pequeños que pertenecen al inquilino A) se protegerán en tres sitios usando replicación de 3 copias.

Regla 1: Codificación de borrado a tres ubicaciones para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de regla	Codificación de borrado de tres sitios para el inquilino A
Cuenta de inquilino	Inquilinoa
Pool de almacenamiento	Los 3 centros de datos (incluye el centro de datos 1, el centro de datos 2 y el centro de datos 3)

Definición de regla	Valor de ejemplo
Colocación del contenido	Codificación de borrado 2+1 en los 3 centros de datos del día 0 para siempre

Regla 2: Replicación de tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Data Center 1, Data Center 2 y Data Center 3
Colocación del contenido	Tres copias replicadas del día 0 para siempre: Una copia en el centro de datos 1, una copia en el centro de datos 2 y una copia en el centro de datos 3.

Activar la política de ILM propuesta por ejemplo 6

Al activar una nueva política de ILM propuesta, es posible que los objetos existentes se muevan a nuevas ubicaciones o que se puedan crear copias de objetos nuevas para los objetos existentes, según las instrucciones de colocación de cualquier regla nueva o actualizada.

Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable. Revise y simule cuidadosamente la directiva antes de activarla para confirmar que funcionará según lo previsto.

Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Lo que ocurre al cambiar las instrucciones de codificación de borrado

En la política de ILM activa actualmente para este ejemplo, los objetos del inquilino A están protegidos mediante codificación de borrado 2+1 en el centro de datos 1. En la nueva política de ILM propuesta, los objetos del inquilino A se protegerán mediante codificación de borrado 2+1 en los centros de datos 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Los objetos nuevos procesados por el inquilino A se dividen en dos fragmentos de datos y se añade un fragmento de paridad. A continuación, cada uno de los tres fragmentos se almacena en un centro de datos diferente.
- Los objetos existentes que pertenecen al inquilino A se reevalúan durante el proceso de análisis de ILM en curso. Dado que las instrucciones de colocación de ILM usan un nuevo perfil de código de borrado, se crean y distribuyen fragmentos totalmente nuevos codificados por borrado a los tres centros de datos.

Los fragmentos 2+1 existentes en el centro de datos 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza fragmentos de código de borrado cuando se utiliza un perfil nuevo.

Qué ocurre cuando cambian las instrucciones de replicación

En la política de ILM activa actualmente para este ejemplo, los objetos que pertenecen a otros inquilinos se protegen con dos copias replicadas en los pools de almacenamiento en los centros de datos 1 y 2. En la nueva política de ILM propuesta, los objetos que pertenecen a otros clientes se protegerán mediante tres copias replicadas de los pools de almacenamiento en los centros de datos 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Cuando un inquilino distinto De inquilino procesa un objeto nuevo, StorageGRID crea tres copias y guarda una copia en cada centro de datos.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Debido a que las copias de objetos existentes en el centro de datos 1 y en el centro de datos 2 siguen satisfaciendo los requisitos de replicación de la nueva regla de ILM, StorageGRID solo tiene que crear una nueva copia del objeto para el centro de datos 3.

Impacto en el rendimiento de la activación de esta política

Si se activa la política de ILM propuesta en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles más altos que los niveles normales de los recursos de grid para crear nuevos fragmentos con código de borrado para los objetos existentes De inquilino A y las nuevas copias replicadas en el centro de datos 3 para los objetos existentes de otros clientes.

Como resultado del cambio en la política de ILM, es posible que las solicitudes de lectura y escritura del cliente experimenten temporalmente más latencias normales. Las latencias volverán a los niveles normales una vez que se implementen por completo las instrucciones de colocación en el grid.

Para evitar problemas de recursos al activar una nueva política de ILM, puede usar el filtro avanzado de tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta como mayor o igual que el tiempo aproximado en el que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.

Si necesita ralentizar o aumentar la velocidad a la que se procesan los objetos después de un cambio de la política de ILM, póngase en contacto con el soporte técnico.

Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3

Puede usar el bloque de S3, las reglas de ILM y la política de ILM en este ejemplo como un punto de partida para definir una política de ILM para cumplir con los requisitos de retención y protección de objetos para los objetos en bloques con el bloqueo de objetos S3 habilitado.

Si ha utilizado la función de cumplimiento de normativas anterior en versiones de StorageGRID anteriores, también puede utilizar este ejemplo para ayudar a gestionar los bloques existentes que tengan habilitada la función de cumplimiento de normativas heredadas.

Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

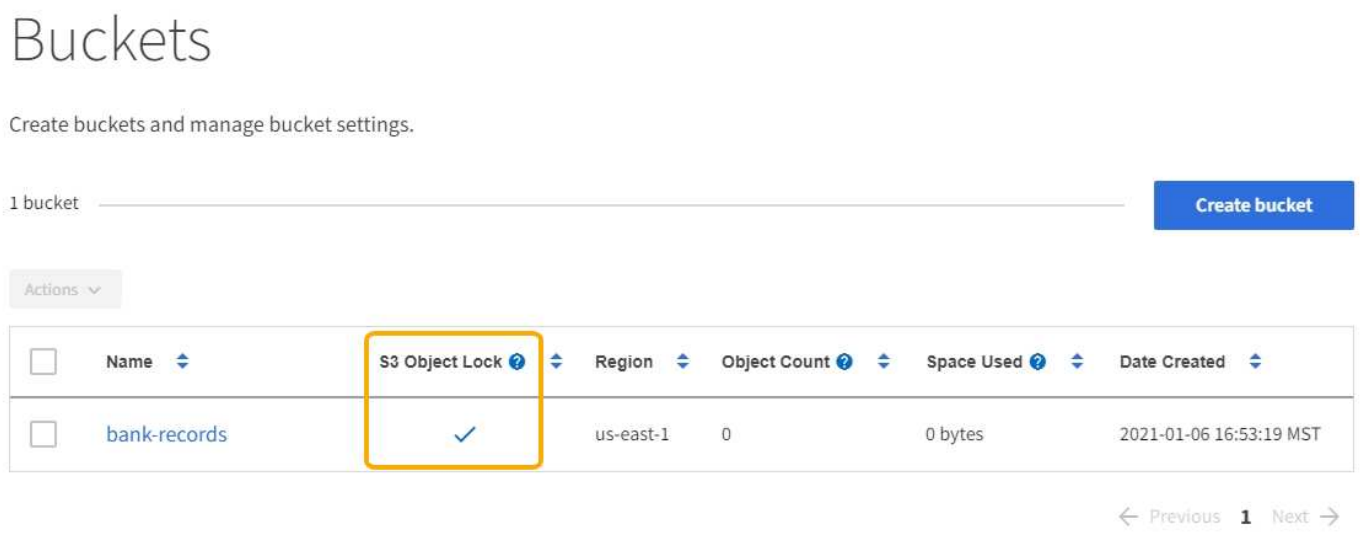
Información relacionada

- Gestione objetos con S3 Object Lock
- Cree una política de ILM

Ejemplo de bloque y objetos para S3 Object Lock

En este ejemplo, una cuenta de inquilino de S3 llamada Bank of ABC ha utilizado el administrador de inquilinos para crear un bloque con el bloqueo de objetos S3 habilitado para almacenar registros bancarios críticos.

Definición de bloque	Valor de ejemplo
Nombre de cuenta de inquilino	Banco de ABC
Nombre del bloque	registros bancarios
Región de bloque	us-east-1 (predeterminado)



Cada objeto y versión de objeto que se agrega al bloque de registros bancarios utilizará los siguientes valores para `retain-until-date` y.. `legal hold` configuración.

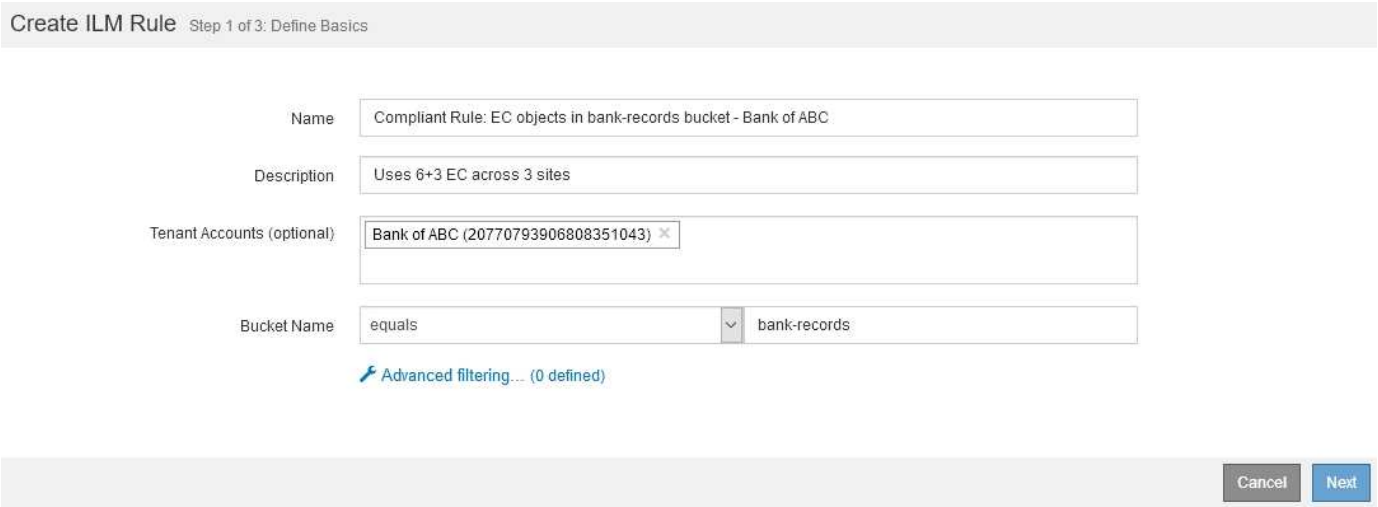
Configuración para cada objeto	Valor de ejemplo
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 de diciembre de 2030) Cada versión de objeto tiene su propia `retain-until-date` ajuste. Este ajuste se puede aumentar, pero no disminuir.

Configuración para cada objeto	Valor de ejemplo
`legal hold`	`"OFF"` (No en vigor) Se puede colocar o levantar una retención legal en cualquier versión del 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 el `retain-until-date` se ha alcanzado.

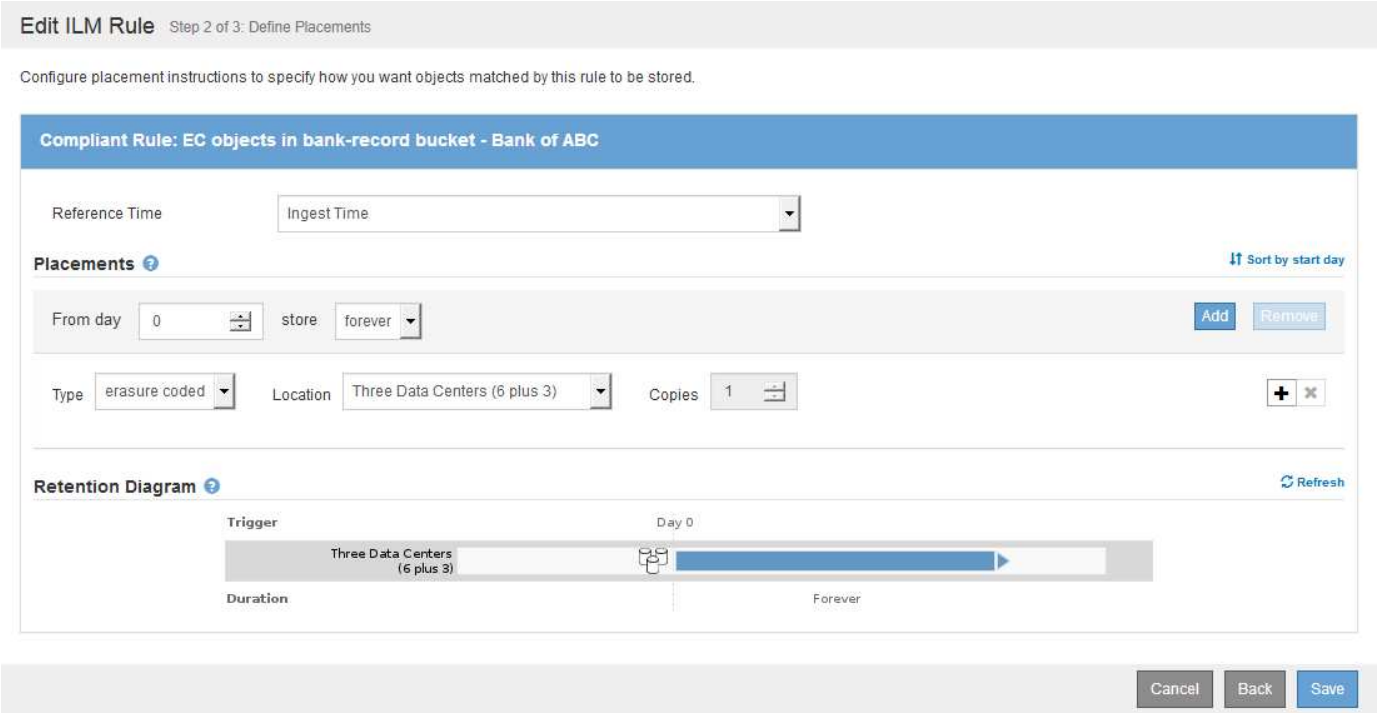
Ejemplo de regla de ILM 1 para el bloqueo de objetos S3: Perfil de código de borrado con coincidencia de bloques

Esta regla de ILM de ejemplo se aplica solo a la cuenta de inquilino de S3 llamada Bank of ABC. Coincide con cualquier objeto de `bank-records` Bucket y, a continuación, utiliza la codificación de borrado para almacenar el objeto en nodos de almacenamiento en tres sitios de centro de datos mediante un perfil de código de borrado 6+3. Esta regla satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado: Se conserva una copia codificada con borrado en los nodos de almacenamiento desde el día 0 hasta siempre utilizando el tiempo de ingesta como hora de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla conforme: Objetos de EC en bloque de registros bancarios - Banco de ABC
Cuenta de inquilino	Banco de ABC
Nombre del bloque	`bank-records`
Filtrado avanzado	Tamaño de objeto (MB) mayor que 1 **Nota:** este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menores.



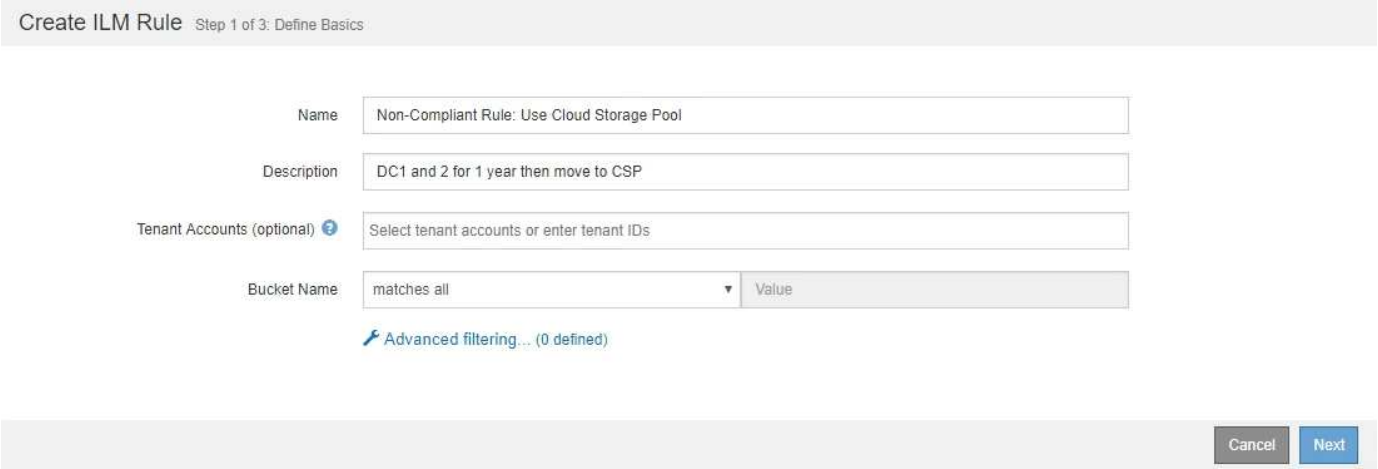
Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 almacenar para siempre
Perfil de código de borrado	• Cree una copia codificada con borrado en los nodos de almacenamiento en tres centros de datos • Utiliza un esquema de codificación de borrado de 6+3



Ejemplo de regla ILM 2 para bloqueo de objetos S3: Regla no conforme a las normativas

Esta regla de ILM de ejemplo almacena inicialmente dos copias de objetos replicadas en nodos de almacenamiento. Después de un año, se almacena una copia en un pool de almacenamiento en cloud para siempre. Como esta regla utiliza un pool de almacenamiento en cloud, no es compatible y no se aplica a los objetos en bloques con el bloqueo de objetos S3 habilitado.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla no conforme a las normativas: Utilizar pool de almacenamiento en cloud
Cuentas de inquilino	No especificado
Nombre del bloque	No se especifica, pero solo se aplica a bloques que no tienen habilitado el bloqueo de objetos de S3 (o la función de cumplimiento heredado).
Filtrado avanzado	No especificado

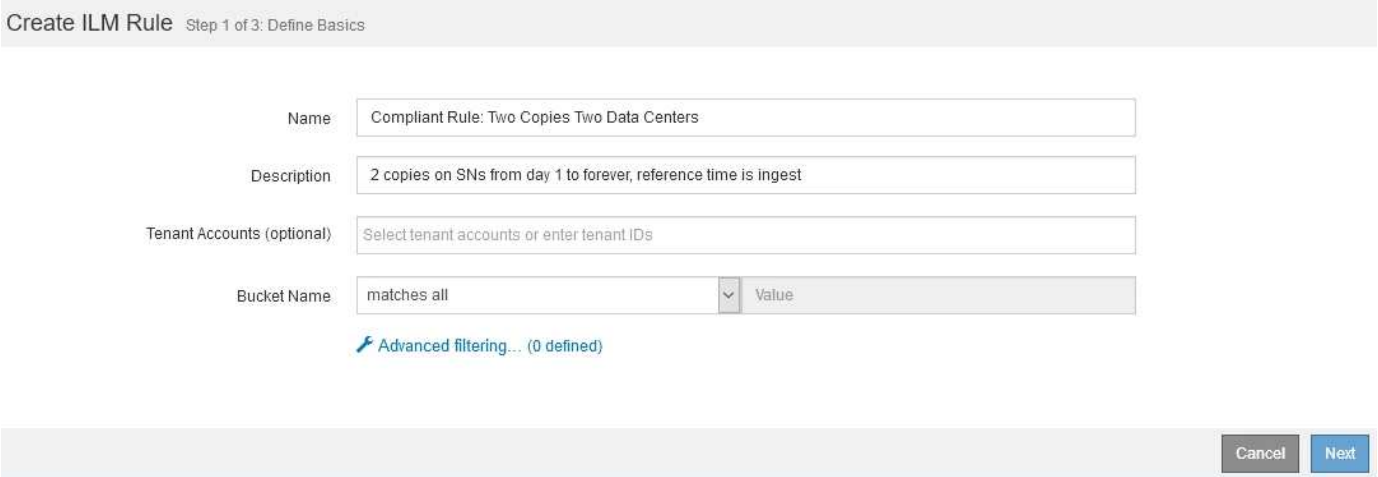


Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	• El día 0, conserve dos copias replicadas en los nodos de almacenamiento en el centro de datos 1 y en el centro de datos 2 durante 365 días • Después de 1 año, mantenga siempre una copia replicada en un pool de almacenamiento en cloud

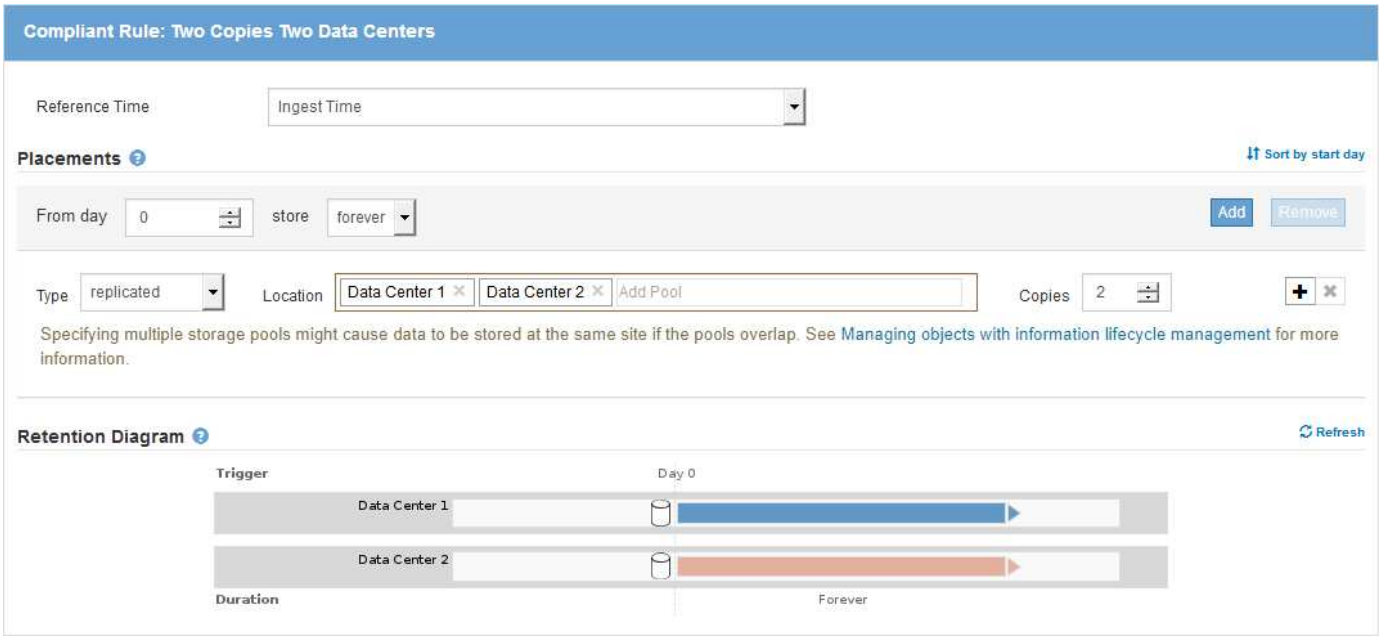
Ejemplo de regla ILM 3 para bloqueo de objetos S3: Regla predeterminada

Esta regla de ILM de ejemplo copia los datos de objetos en dos pools de almacenamiento en dos centros de datos. Esta regla de cumplimiento está diseñada para ser la regla predeterminada de la política de ILM. No incluye ningún filtro, no utiliza el tiempo de referencia no corriente y satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado: Se mantienen dos copias de objetos en los nodos de almacenamiento del día 0 al permanente, utilizando procesamiento como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla de conformidad predeterminada: Dos copias dos centros de datos
Cuenta de inquilino	No especificado
Nombre del bloque	No especificado
Filtrado avanzado	No especificado



Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	De día 0 a siempre, conserve dos copias replicadas (una en los nodos de almacenamiento en el centro de datos 1 y otra en los nodos de almacenamiento en el centro de datos 2).



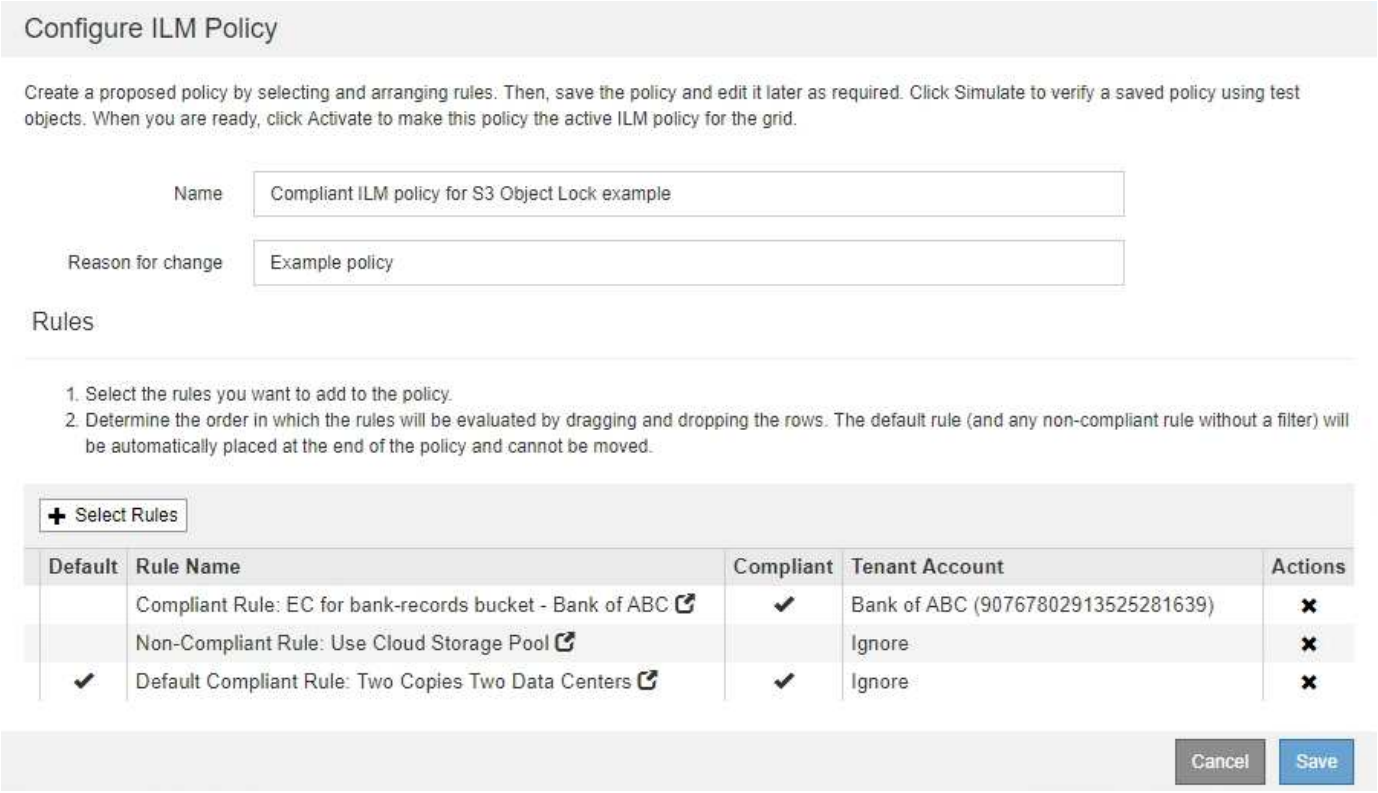
Ejemplo de política de ILM conforme a la normativa para el bloqueo de objetos S3

Para crear una política de ILM que proteja de manera efectiva todos los objetos del sistema, incluidos los que están en bloques con el bloqueo de objetos S3 habilitado, debe seleccionar reglas de ILM que cumplan con los requisitos de almacenamiento para todos los objetos. A continuación, debe simular y activar la directiva propuesta.

Añada reglas a la política

En este ejemplo, la política de ILM incluye tres reglas de ILM, en el siguiente orden:

1. Regla de conformidad que utiliza la codificación de borrado para proteger objetos de más de 1 MB en un bloque específico con el bloqueo de objetos S3 habilitado. Los objetos se almacenan en nodos de almacenamiento del día 0 al permanente.
2. Una regla no conforme a las normativas que crea dos copias de objetos replicados en los nodos de almacenamiento durante un año y, a continuación, mueve una copia de objetos a un Cloud Storage Pool de forma permanente. Esta regla no se aplica a bloques con el bloqueo de objetos S3 habilitado porque utiliza un pool de almacenamiento en cloud.
3. La regla de cumplimiento predeterminada que crea dos copias de objetos replicados en los nodos de almacenamiento desde el día 0 hasta siempre.



Simular la política propuesta

Después de añadir reglas a la política propuesta, elegir una regla de cumplimiento predeterminada y organizar las demás reglas, debe simular la política probando objetos desde el bloque con el bloqueo de objetos S3 habilitado y desde otros bloques. Por ejemplo, al simular la directiva de ejemplo, debería esperar que los objetos de prueba se evaluaran de la siguiente manera:

- La primera regla sólo coincidirán con los objetos de prueba que son superiores a 1 MB en los registros bancarios de bloque para el inquilino Banco de ABC.
- La segunda regla coincidirán con todos los objetos de todos los segmentos no compatibles para todas las demás cuentas de arrendatario.
- La regla predeterminada coincidirán con estos objetos:
  - Objetos de 1 MB o menos en los registros bancarios del bloque para el inquilino del Banco de ABC.
  - Objetos de cualquier otro bloque 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 según lo esperado, puede activarlo.