



Gestión de objetos con ILM

StorageGRID

NetApp
November 04, 2025

This PDF was generated from <https://docs.netapp.com/es-es/storagegrid-118/ilm/index.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión de objetos con ILM	1
Gestión de objetos con ILM	1
Acerca de estas instrucciones	1
Leer más	1
ILM y ciclo de vida de los objetos	1
Cómo funciona ILM a lo largo de la vida de un objeto	1
Cómo se ingieren los objetos	3
Cómo se almacenan los objetos (codificación de borrado o replicación)	8
Cómo se determina la retención de objetos	19
Cómo se eliminan los objetos	21
Crear y asignar grados de almacenamiento	24
Usar pools de almacenamiento	27
¿Qué es un pool de almacenamiento?	27
Directrices para crear pools de almacenamiento	28
Habilite la protección contra pérdida de sitio	30
Cree un pool de almacenamiento	32
Ver detalles del pool de almacenamiento	34
Editar pool de almacenamiento	35
Quitar un pool de almacenamiento	36
Utilice Cloud Storage Pools	36
¿Qué es un pool de almacenamiento en cloud?	36
Ciclo de vida de un objeto de Cloud Storage Pool	39
Cuándo usar Cloud Storage Pools	41
Consideraciones para Cloud Storage Pools	42
Compare los pools de almacenamiento en cloud y la replicación de CloudMirror	45
Cree un pool de almacenamiento en el cloud	47
Editar un pool de almacenamiento en el cloud	52
Quitar un pool de almacenamiento en el cloud	53
Solucione problemas de Cloud Storage Pools	54
Gestione perfiles de código de borrado	56
Consulte los detalles del perfil de código de borrado	57
Cambio el nombre de un perfil de código de borrado	57
Desactivar un perfil de código de borrado	57
Configurar regiones (opcional solo S3)	60
Cree la regla de ILM	61
Cree una regla de ILM: Información general	61
Acceda al asistente Create an ILM Rule	65
Paso 1 de 3: Introduzca los detalles	66
Paso 2 de 3: Definir colocaciones	70
Utilice la última hora de acceso en las reglas de ILM	74
Paso 3 de 3: Seleccione el comportamiento de ingestá	75
Cree una regla de ILM predeterminada	76
Gestionar políticas de ILM	78

Políticas de ILM: Información general	78
Crear políticas de ILM	82
Ejemplo de simulaciones de políticas de ILM	89
Gestione etiquetas de políticas de ILM	92
Comprobar una política de ILM con la búsqueda de metadatos de objetos	93
Funciona con políticas de ILM y reglas de ILM	96
Vea las políticas de ILM	96
Editar una política de ILM	96
Clonar una política de ILM	96
Quitar una política de ILM	97
Vea los detalles de las reglas de ILM	97
Clonar una regla de ILM	98
Editar una regla de ILM	98
Quite una regla de ILM	98
Ver las métricas de ILM	99
Utilice el bloqueo de objetos de S3	100
Gestione objetos con S3 Object Lock	100
Flujo de trabajo para bloqueo de objetos de S3	104
Requisitos para el bloqueo de objetos de S3	105
Habilite el bloqueo de objetos de S3 globalmente	107
Resuelva los errores de coherencia al actualizar la configuración de bloqueo de objetos de S3 o cumplimiento heredado	108
Ejemplo de reglas y políticas de ILM	109
Ejemplo 1: Reglas de ILM y políticas para el almacenamiento de objetos	109
Ejemplo 2: Reglas de ILM y política para el filtrado de tamaño de objetos de EC	111
Ejemplo 3: Reglas de ILM y política para mejorar la protección de los archivos de imagen	113
Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3	114
Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto	117
Ejemplo 6: Cambiar una política de ILM	120
Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3	124
Ejemplo 8: Prioridades para el ciclo de vida del bloqueo de S3 y política de ILM	128

Gestión de objetos con ILM

Gestión de objetos con ILM

Las reglas de gestión de la vida útil de la información (ILM) en una política de ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo gestionar esas copias con el tiempo.

Acerca de estas instrucciones

Diseñar e implementar reglas y políticas 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:

- Conozca más detalles sobre gestión de la vida útil de la información de StorageGRID "[Funcionamiento de ILM a lo largo de la vida de un objeto](#)".
- Aprenda a configurar "[pools de almacenamiento](#)", "[Pools de almacenamiento en cloud](#)", y. "[Reglas de ILM](#)".
- Aprenda cómo "[Cree, simule y active una política de ILM](#)" que protegerá los datos de objetos en uno o más sitios.
- Aprenda cómo "[Gestionar objetos con S3 Object Lock](#)", Que ayuda a garantizar que los objetos en cubos específicos de S3 no se borren o sobrescriban durante un período de tiempo específico.

Leer más

Para obtener más información, consulte estos videos:

- "[Vídeo: Reglas de gestión del ciclo de vida de la información en StorageGRID 11,8](#)".


- "[Vídeo: Políticas de gestión del ciclo de vida de la información en StorageGRID 11,8](#)"


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.

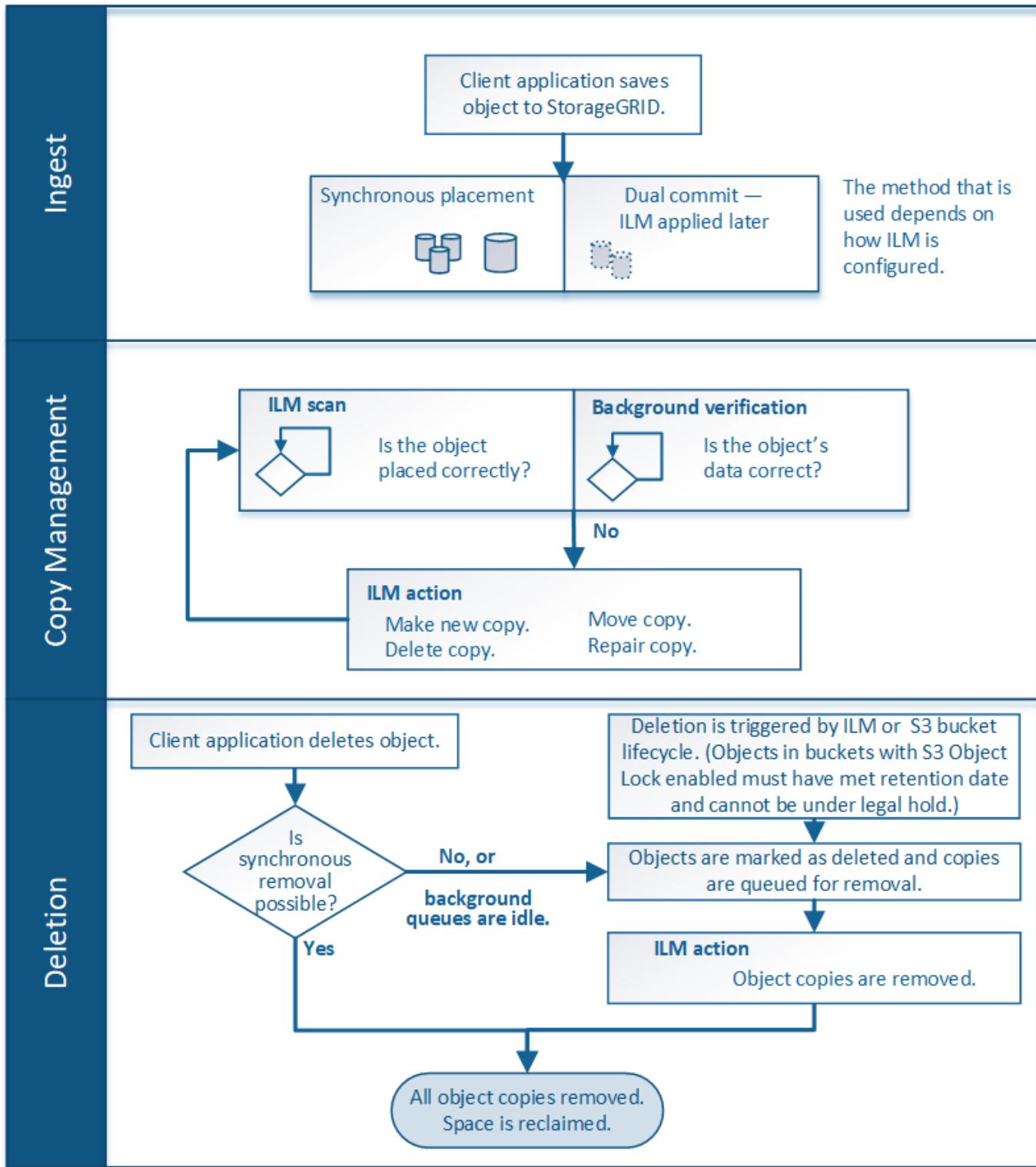
- **Ingreso:** La ingestión comienza cuando una aplicación cliente S3 o Swift establece una conexión para guardar un objeto en el sistema StorageGRID, y se completa cuando StorageGRID devuelve un mensaje de "Ingreso correcto" al cliente. Los datos de objetos se protegen durante la ingestión aplicando 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 con los requisitos de ILM. Cuando se requieren diferentes tipos, números o ubicaciones de copias de objetos, StorageGRID crea, elimina o mueve copias según sea necesario.
 - **Verificación de antecedentes:** StorageGRID realiza continuamente la verificación de fondo para verificar la integridad de los datos de los 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 "["Verifique la integridad del objeto"](#)".
- **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 depósito que tiene S3 Object Lock activado no se pueden eliminar si están en una retención legal o si se ha especificado una fecha de retención hasta que no se cumple.

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



Cómo se ingieren los objetos

Opciones de procesamiento

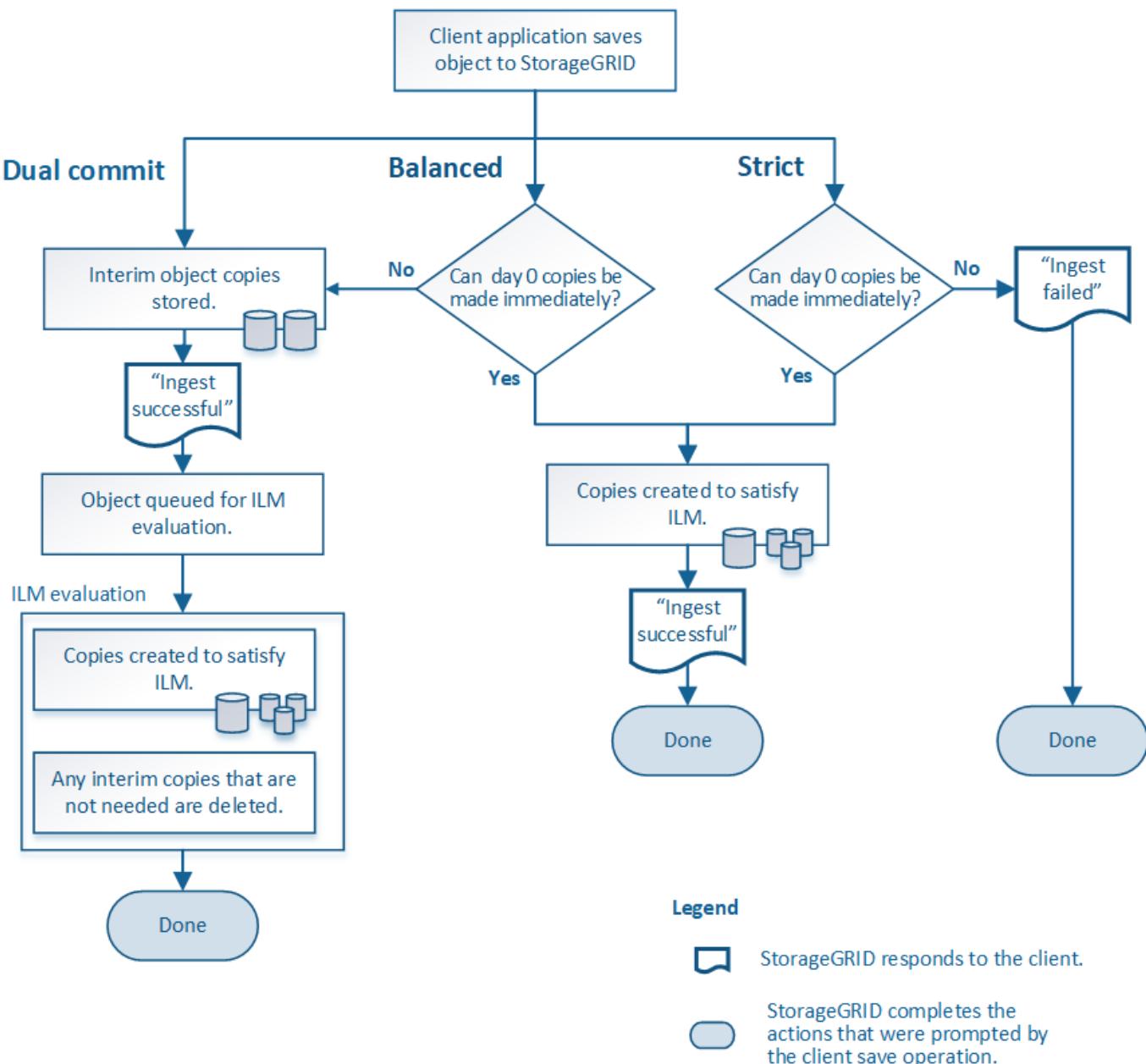
Al crear una regla de ILM, se deben especificar una de estas tres opciones para proteger los objetos durante la ingestión: Dual commit, strict o balanced.

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 opciones de ingestión

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



Registro doble

Cuando selecciona la opción Confirmación doble, StorageGRID realiza de forma inmediata copias de objetos provisionales en dos nodos de almacenamiento diferentes y devuelve un mensaje de procesamiento correcto 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. Si la política de ILM no puede procesarse inmediatamente después de la confirmación doble, la protección contra pérdida de sitio podría tardar tiempo en lograrse.

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 utilizar la confirmación doble, debe asegurarse de que el grid pueda realizar el trabajo adicional de creación y eliminación de las copias de registro doble si no cumplen con el ciclo de vida de la información. 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.

Equilibrada (predeterminado)

Cuando selecciona la opción equilibrada, StorageGRID también utiliza la ubicación síncrona durante la ingestión y hace inmediatamente todas las copias especificadas en las instrucciones de ubicación de la regla. En contraste con la opción estricta, si StorageGRID no puede hacer todas las copias de inmediato, utiliza Confirmación doble en su lugar. Si la política de ILM utiliza ubicaciones en varios sitios y no se puede lograr la protección inmediata contra la pérdida de sitio, se activa la alerta **ILM ubicación inalcanzable**.

Utilice la opción equilibrada para lograr la mejor combinación de protección de datos, rendimiento de grid y éxito de procesamiento. Equilibrada es la opción predeterminada del asistente Create ILM Rule.

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. La ingestión genera un error si StorageGRID no puede crear todas las copias, por ejemplo, porque no está disponible en estos momentos una ubicación de almacenamiento necesaria. El cliente debe volver a intentar la operación.

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 necesite utilizar la opción estricta y un filtro avanzado de restricción de ubicación para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Consulte "[Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto](#)".

Ventajas, desventajas y limitaciones de las opciones de ingestión

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.

Para obtener una descripción general de las opciones de ingestión, consulte "[Opciones de procesamiento](#)".

Ventajas de las opciones equilibradas y estrictas

En comparación con el registro doble, que crea copias provisionales durante la ingestión, las dos opciones de colocación síncrona 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 Balanced a menos que se requiera un comportamiento de ingestión estricto o que el grid cumpla todos los criterios para utilizar Dual commit.
- **(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. Cuando utiliza las opciones equilibradas o estrictas, no se devuelve al cliente un mensaje de ingestión correcta hasta que se creen y almacenen todos los fragmentos con código de borrado o las copias replicadas. Sin embargo, lo más probable es que los datos de objetos lleguen a su ubicación final mucho más rápido.
- **(Estrictas) mayores tasas de fallo de ingestión:** Con la opción estricta, la ingestión falla siempre que StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla de 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 una carga de varias partes de S3 KB, se evalúa ILM para cada parte del objeto conforme se procesa, y para el objeto en su conjunto 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 multipart 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 ingestión del objeto no falla. En su lugar, cualquier pieza que no se coloque correctamente se pone en cola para la reevaluación de ILM y posteriormente se mueve a la ubicación correcta.
 - **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 con 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 multipart 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 ingestión 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 cualquier cambio en la ubicación del objeto que se desencadene por la actualización no se realiza 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 ubicación necesarios (por ejemplo, porque no está disponible una nueva ubicación requerida), el objeto actualizado conserva su ubicación actual hasta que los cambios de ubicación sean posibles.

Limitaciones en la ubicación de objetos con las opciones equilibradas y estrictas

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

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

Estas restricciones se deben a que StorageGRID no puede realizar copias de forma síncrona en un grupo de almacenamiento en la nube o en un nodo de archivado, y una hora de creación definida por el usuario podría resolverse en el presente.

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

Tanto su regla de ILM como su elección de coherencia afectan al modo en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta a la ubicación inicial de las copias del objeto, mientras que la consistencia utilizada cuando se almacena un objeto afecta a la ubicación inicial de los metadatos de objetos. Dado que StorageGRID necesita acceso a los datos y metadatos de un objeto para satisfacer las solicitudes del cliente, seleccionar niveles de protección correspondientes para la consistencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas del sistema más predecibles.

A continuación encontrará un breve resumen de los valores de coherencia disponibles en StorageGRID:

- **Todos**: Todos los nodos reciben metadatos de objeto inmediatamente o la solicitud fallará.
- **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 de objetos 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 después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.



Antes de seleccionar un valor de consistencia, ["lea la descripción completa de la consistencia"](#). Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Un ejemplo de cómo pueden interactuar las reglas de coherencia e ILM

Suponga que tiene un grid de dos sitios con la siguiente regla de ILM y la siguiente consistencia:

- **Norma ILM:** Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Use un comportamiento de ingesta estricto.
- **Consistencia:** Fuerte-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 cambio, utiliza la misma regla de ILM y la coherencia del sitio fuerte, es posible que el cliente reciba un mensaje de éxito después de replicar los datos de objetos en el sitio remoto, pero antes de que los metadatos de los objetos 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 las reglas de coherencia y de 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)

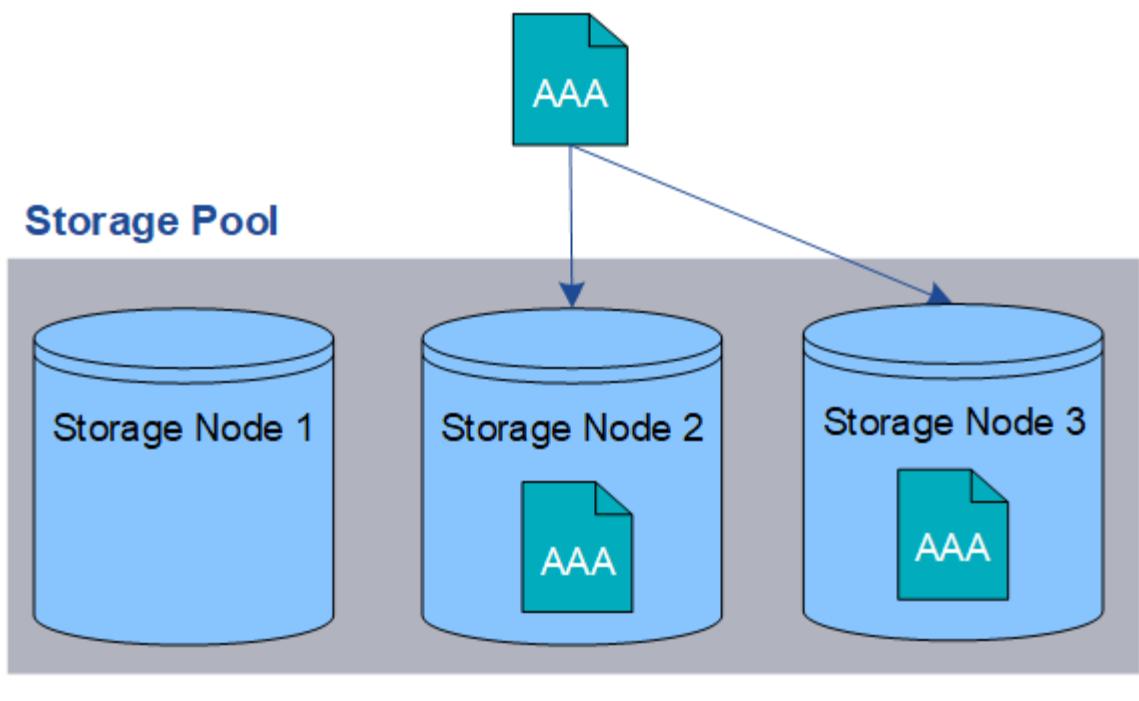
¿Qué es la replicación?

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.

Make 2 Copies



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.

i 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 la codificación de borrado"](#)
- ["Qué es un pool de almacenamiento"](#)
- ["Habilite la protección contra pérdida de sitios mediante replicación y código de borrado"](#)

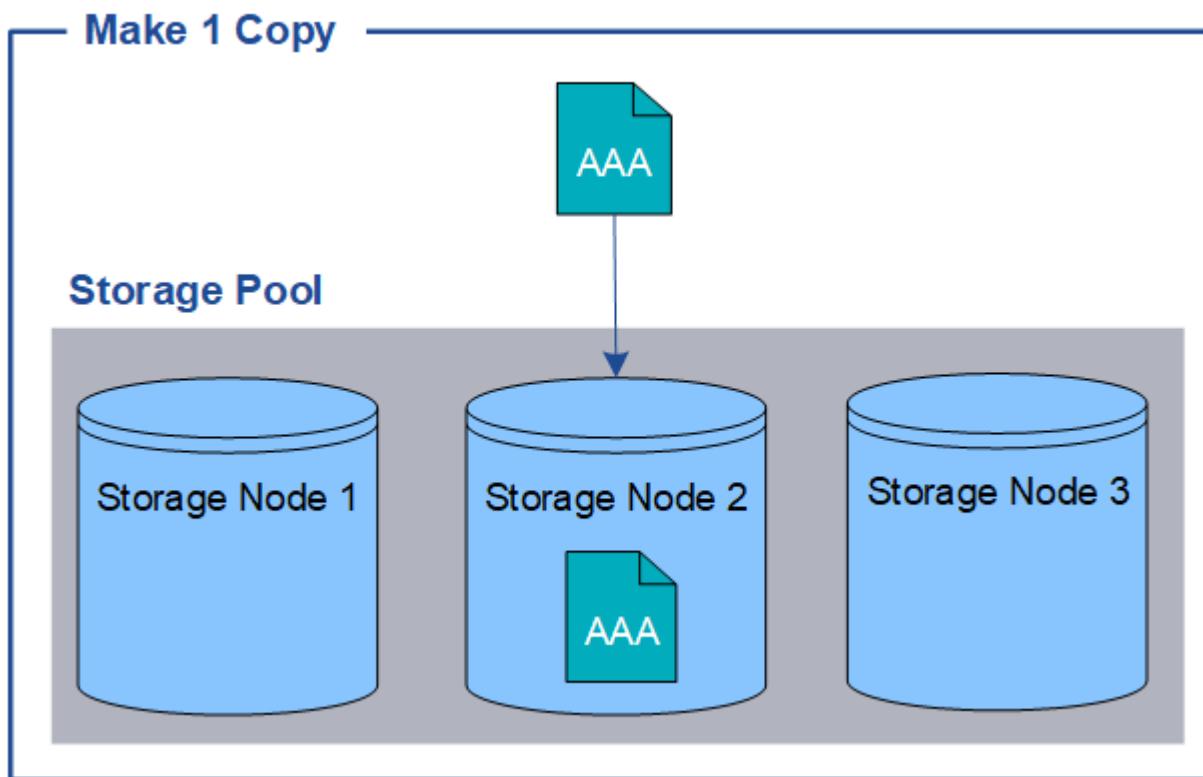
Por qué no se debe utilizar la replicación de copia única

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.

i No utilice una regla de ILM que cree solo una copia replicada durante un período 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.

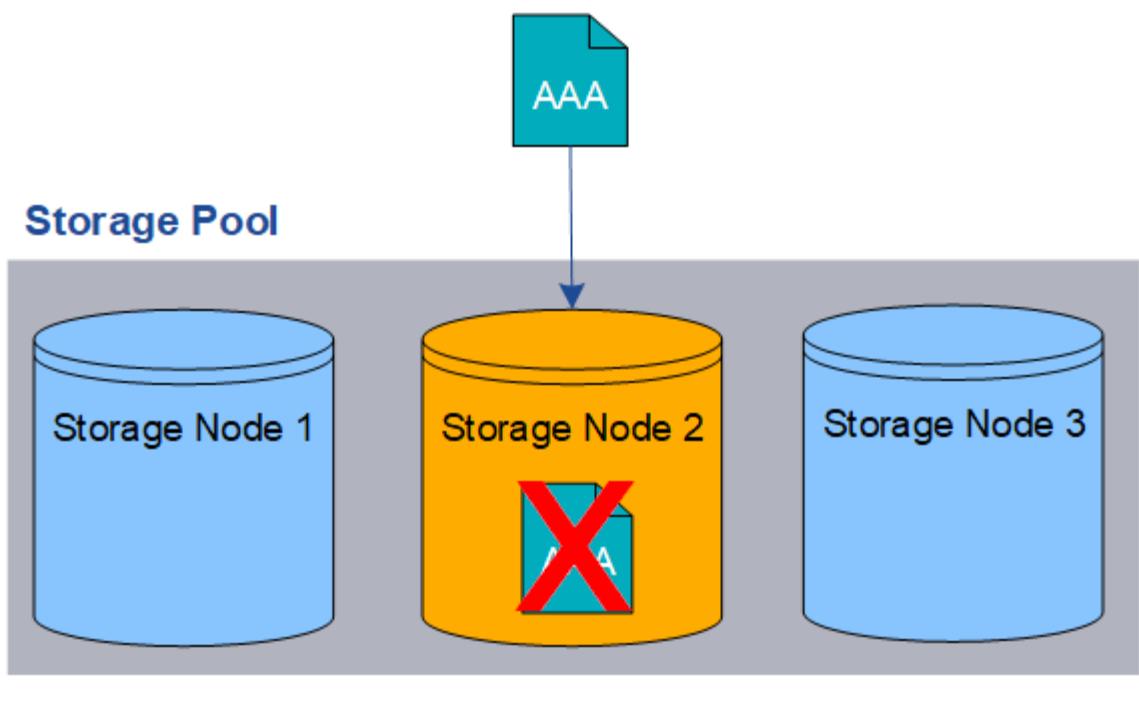
En el ejemplo siguiente, la regla Make 1 Copy ILM especifica que una copia replicada de un objeto se coloca

en un pool de almacenamiento que contiene tres nodos de almacenamiento. Cuando se ingiere un objeto que coincide con esta regla, StorageGRID coloca una sola copia en un solo nodo de almacenamiento.



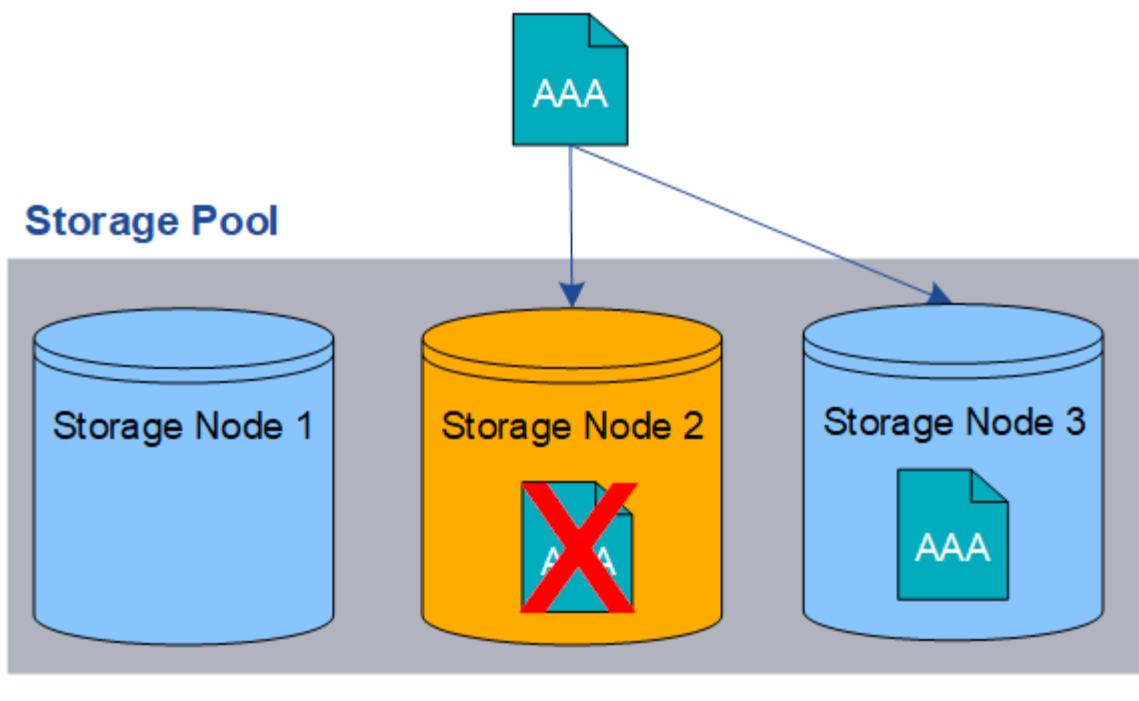
Cuando una regla de ILM crea solo una copia replicada de un objeto, se vuelve inaccesible cuando el nodo de almacenamiento no está disponible. En este ejemplo, perderá temporalmente el acceso al objeto AAA siempre que el nodo de almacenamiento 2 esté desconectado, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA completamente si falla el nodo de almacenamiento 2.

Make 1 Copy



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

Make 2 Copies



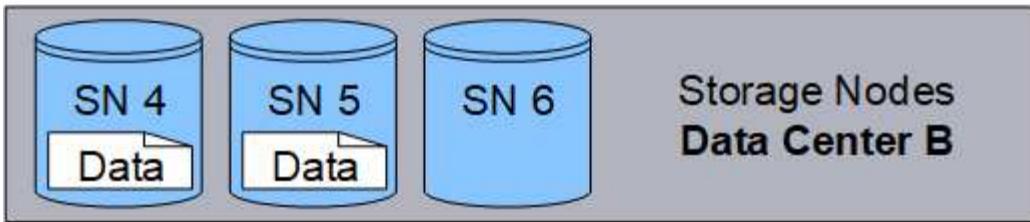
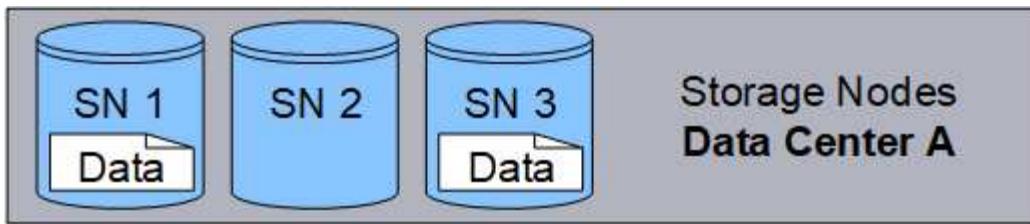
¿Qué es el código de borrado?

El código de borrado es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos. Cuando los objetos coinciden con una regla de ILM que utiliza código de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

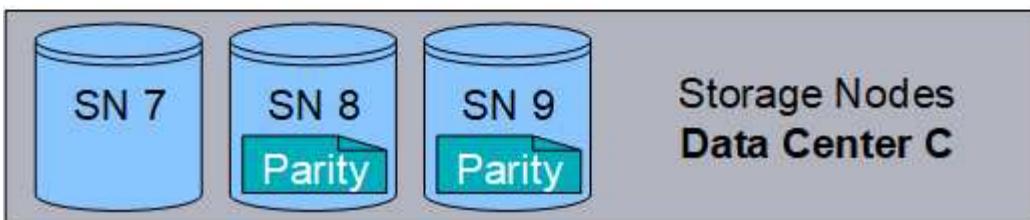
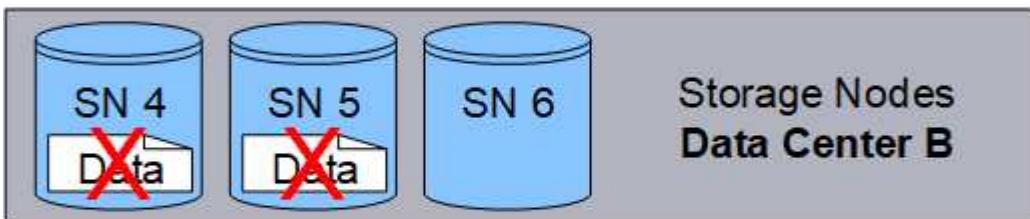
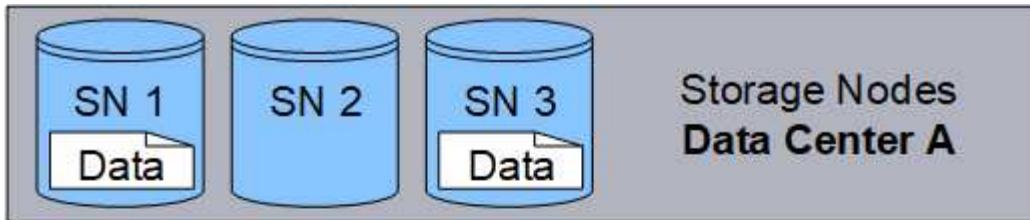
Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un dato o un fragmento de paridad se corrompen o se pierden, el algoritmo de código de borrado puede recrear ese fragmento con un subconjunto de los datos restantes y los fragmentos de paridad.

Al crear reglas de ILM, StorageGRID crea perfiles de código de borrado compatibles con esas reglas. Puede ver una lista de perfiles de codificación de borrado, "["cambie el nombre de un perfil de código de borrado"](#)", o "["Desactive un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM"](#)".

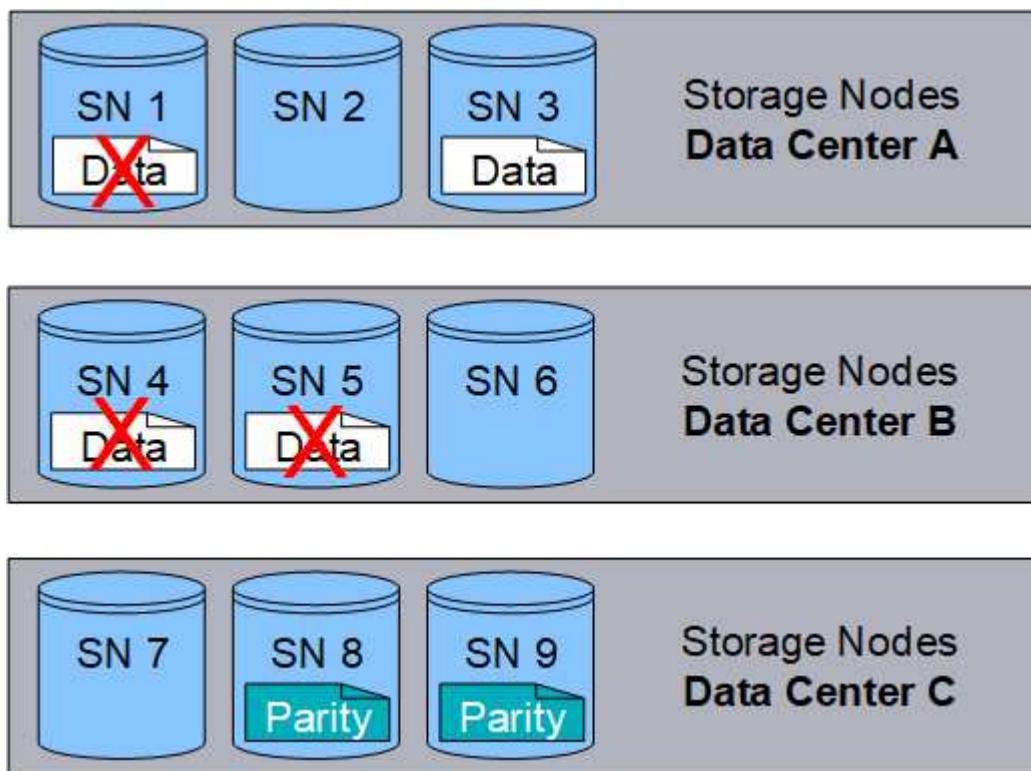
En el siguiente ejemplo, se muestra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir 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 se puede configurar de varias maneras. Por ejemplo, puede configurar un pool de almacenamiento de un único sitio que contenga seis nodos de almacenamiento. Para "protección contra pérdida de sitios", Puede utilizar un pool de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. 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 entero, el objeto aún puede recuperarse o repararse, siempre que se pueda acceder a todos los demás fragmentos.



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



Información relacionada

- ["Qué es la replicación"](#)
- ["Qué es un pool de almacenamiento"](#)
- ["¿Qué son los esquemas de código de borrado"](#)
- ["Cambio el nombre de un perfil de código de borrado"](#)
- ["Desactivar un perfil de código de borrado"](#)

¿Qué son los esquemas de código de borrado?

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

Cuando configura el perfil de código de borrado para una regla de ILM, debe seleccionar un esquema de código de borrado disponible en función del número de nodos de almacenamiento y sitios que componen el pool de almacenamiento que piensa usar.

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo divide un objeto en k fragmentos de datos y cálculos m fragmentos de paridad. La $k + m = n$ los fragmentos se distribuyen n Nodos de almacenamiento para proporcionar protección de datos. Un objeto puede soportar hasta m fragmentos perdidos o corruptos. Para recuperar o reparar un objeto, k se necesitan fragmentos.

Cuando seleccione el pool de almacenamiento que se utilizará en una regla que creará una copia con código de borrado, utilice las siguientes directrices para los pools de almacenamiento:

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



No se puede usar 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 un pool de almacenamiento que incluya el sitio predeterminado, Todos los sitios.
- El pool de almacenamiento debe incluir al menos $k+m+1$ Nodos de almacenamiento que pueden almacenar datos de objetos.



Los nodos de almacenamiento se pueden configurar durante la instalación de modo que solo contengan metadatos de objetos y no datos de objetos. Para obtener más información, consulte ["Tipos de nodos de almacenamiento"](#).

El número mínimo necesario de nodos de almacenamiento es $k+m$. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a evitar fallos de ingestión 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 código de borrado se calcula dividiendo el número de fragmentos de paridad (m) por 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 que tenga el valor total más bajo de $k+m$ que satisface sus necesidades. Los esquemas de código de borrado con un número menor de fragmentos por lo general son más eficientes computacionalmente, ya que se crean y distribuyen menos fragmentos (o se recuperan) por objeto, pueden ofrecer un mejor rendimiento debido al tamaño de fragmento más grande y pueden requerir que se añadan menos nodos en una expansión cuando se necesita más almacenamiento. (Para obtener información sobre cómo planificar una expansión de almacenamiento, consulte ["Instrucciones para ampliar StorageGRID"](#).)

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.

Para esquemas de código de borrado que ofrecen protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el pool de almacenamiento supera $k+m+1$. Dado que cada sitio requiere un mínimo de tres nodos de almacenamiento.

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

 StorageGRID requiere un mínimo de tres nodos de almacenamiento por sitio. Para utilizar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda 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 se incrementa al tener más segmentos de paridad (es decir, cuando m tiene un valor más alto.)
- **Tráfico de red:** Al recuperarse de fallos, utilizando 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.

El número mínimo necesario de nodos de almacenamiento es $k+m$, pero una piscina de almacenamiento con $k+m +1$ Se recomiendan los nodos de almacenamiento. 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 %

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 el objeto con código de borrado en tres sitios con un esquema de código 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 recomienda un mayor número de nodos de almacenamiento y sitios, en función del esquema de código de borrado. Por el contrario, si replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia. Consulte ["Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios"](#) y.. ["Esquemas de codificación de borrado para pools de almacenamiento in situ"](#).
- Aumento del coste y de la complejidad de las ampliaciones del almacenamiento. Para expandir una implementación que utiliza replicación, debe 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 a que los nodos existentes estén llenos al 100 %, debe agregar al menos $k+m$ Nodos de almacenamiento, pero si amplía cuando los nodos existentes estén 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 objetos para un objeto que se codifica para el borrado y se distribuye por sitios remotos tardan más en recuperarse a través de conexiones WAN que un objeto que se replica y está disponible 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 use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

- 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.
 - Una versión de objeto que está bajo una conservación legal no se puede eliminar con ningún método.
 - Antes de que se alcance la fecha de retención hasta la versión de un objeto, esa versión no se puede eliminar con ningún método.
 - Los objetos de los bloques con S3 Object Lock habilitado son conservados por ILM «para siempre». Sin embargo, cuando se alcanza su fecha de retención hasta la fecha, una solicitud de cliente o el vencimiento del ciclo de vida del bloque pueden eliminar una versión de objeto. 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 «Forever» para las instrucciones de colocación.

Independientemente de quién controle el tiempo durante el que se retienen los objetos, los ajustes de ILM controlan qué tipos de copias de objetos (replicadas o con código 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

Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida. 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

Almacene dos copias en los nodos de almacenamiento «por 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

Almacene dos copias en los nodos de almacenamiento «por 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	<p>Cuando cualquiera de las siguientes condiciones se cumple:</p> <ul style="list-style-type: none"> La eliminación automática de objetos ha sido activada por uno de los siguientes eventos: <ul style="list-style-type: none"> 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. <p>Nota: Los objetos en un depósito que tiene S3 Object Lock habilitado no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención hasta la fecha pero aún no se cumplen.</p> <ul style="list-style-type: none"> Un cliente de S3 o Swift solicita la eliminación y se debe cumplir una o varias de estas condiciones: <ul style="list-style-type: none"> Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, una ubicación de objetos no está disponible en este momento. Las colas de eliminación en segundo plano están inactivas.
Los objetos se quitan de inmediato (eliminación síncrona)	<p>Cuando un cliente S3 o Swift realiza una solicitud de eliminación y se cumplen todas las siguientes condiciones:</p> <ul style="list-style-type: none"> 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 S3 o Swift realizan solicitudes de eliminación, StorageGRID empieza añadiendo 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.

Tiempo necesario para 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 con atención el rendimiento de eliminación durante una eliminación masiva, puede observar que la tasa de eliminación parece 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.

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 las 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 los objetos se versionan, 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 objeto crea un marcador de eliminación de cero bytes como la versión actual del objeto, lo que hace que la versión anterior del objeto sea «no actual». Un marcador de supresión de objeto se convierte en un marcador de supresión de objeto caducado cuando es la versión actual y no hay versiones no actuales.

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 o para eliminar marcadores de borrado, utilice una de las siguientes opciones:

- **Solicitud de cliente S3:** Especifique el ID de versión de 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 objetos no se pueden recuperar.

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

Para eliminar marcadores de supresión de objetos caducados, utilice la Expiration acción con una de las siguientes etiquetas: ExpiredObjectDeleteMarker, Days, 0. Date.

- **ILM:** "Clonar una política activa" Y añada dos reglas de ILM a la nueva política:

- Primera regla: Utilice la hora no corriente como hora de referencia para que coincida con las versiones no actuales del objeto. Pulg ["Paso 1 \(introduzca detalles\) del asistente Create an ILM Rule"](#), Seleccione Sí para la pregunta, "¿Aplicar esta regla solo a versiones de objetos más antiguas (en

cubos S3 con control de versiones activado)?"

- Segunda regla: Utilice **tiempo de ingestión** para que coincida con la versión actual. La regla "Tiempo no corriente" debe aparecer en la política sobre la regla **Tiempo de ingestión**.



ILM no se puede utilizar para quitar marcadores de eliminación de objetos actuales. Utilice una solicitud de cliente S3 o un ciclo de vida de cubo S3 para eliminar los marcadores de eliminación de objetos actuales.

- * Eliminar objetos en el cubo *: Utilice el administrador de inquilinos a. "[suprimir todas las versiones de objetos](#)", incluyendo marcadores de borrado, de un cubo.

Cuando se elimina un objeto versionado, StorageGRID crea un marcador de eliminación de cero bytes como la versión actual del objeto. Todos los objetos y marcadores de supresión deben eliminarse para poder eliminar un depósito con versiones.

- Los marcadores de eliminación creados en StorageGRID 11,7 o versiones anteriores solo se pueden eliminar mediante las solicitudes de clientes de S3; además, no se pueden eliminar mediante ILM, las reglas de ciclo de vida de los bloques ni la eliminación de objetos de las operaciones de bloque.
- Elimine los marcadores de un bloque que se haya creado en StorageGRID 11,8 o versiones posteriores puede eliminar mediante ILM, las reglas de ciclo de vida de los bloques, la eliminación de objetos en operaciones de bloque o una eliminación explícita de clientes S3. Los marcadores de eliminación caducados en StorageGRID 11,8 o posterior se deben eliminar mediante reglas de ciclo de vida del bloque o mediante una solicitud de cliente explícita de S3 con un ID de versión especificado.

Información relacionada

- "[USE LA API DE REST DE S3](#)"
- "[Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3](#)"

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 coloquen determinados objetos en ciertos nodos de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Ya tienes "[permisos de acceso específicos](#)".

Acerca de esta tarea

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

El uso de grados de almacenamiento personalizados permite crear pools de almacenamiento ILM que contienen solo un tipo específico de nodo de almacenamiento. Por ejemplo, quizás desee almacenar determinados objetos en los nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash StorageGRID.

 Los nodos de almacenamiento se pueden configurar durante la instalación de modo que solo contengan metadatos de objetos y no datos de objetos. Los nodos de almacenamiento solo de metadatos no se pueden asignar a un grado de almacenamiento. Para obtener más información, consulte ["Tipos de nodos de almacenamiento"](#).

Si el grado de almacenamiento no es una preocupación (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y usar la selección **Incluye todos los grados de almacenamiento** para el grado de almacenamiento cuando usted ["cree pools de almacenamiento"](#). El uso de esta selección garantiza que el pool de almacenamiento incluirá todos los nodos de almacenamiento en el sitio, independientemente de su grado de almacenamiento.

 No cree más grados de almacenamiento de los necesarios. Por ejemplo, no cree una categoría 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. Definir grados de almacenamiento personalizados:
 - a. Para cada grado de almacenamiento personalizado que desee agregar, seleccione **Insertar**  para agregar una fila.
 - b. Introduzca una etiqueta descriptiva.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions



Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Seleccione **aplicar cambios**.

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



No se pueden eliminar los grados de almacenamiento.

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

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

b. Seleccione el grado de almacenamiento adecuado en la lista.

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	disk	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes 



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.

- Seleccione **aplicar cambios**.

Usar 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.

Al instalar StorageGRID, se crea automáticamente un pool de almacenamiento por sitio. Es posible configurar pools de almacenamiento adicionales según sea necesario para cumplir sus requisitos de almacenamiento.



Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan datos de objetos y metadatos de objetos, o solo metadatos del objeto. Los nodos de almacenamiento solo de metadatos no se pueden usar en pools de almacenamiento. Para obtener más información, consulte "[Tipos de nodos de almacenamiento](#)".



La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.

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.

Los pools de almacenamiento se utilizan en las reglas de ILM para determinar dónde se almacenan los datos de objetos y el tipo de almacenamiento utilizado. 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

Configura y utiliza pools de almacenamiento para protegerse frente a la pérdida de datos distribuyendo los datos entre varios sitios. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de pools de almacenamiento.

Consulte "[Ejemplos de habilitación de la protección contra pérdida de sitios mediante replicación y código de borrado](#)".

Directrices para todos los pools de almacenamiento

- 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.
- En general, no use el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) ni el sitio Todos los sitios. Estos elementos se actualizan automáticamente para incluir los nuevos sitios que agregue en una expansión, lo cual podría no ser el comportamiento que desea.

Directrices para los pools de almacenamiento utilizados para copias replicadas

- De protección contra pérdida de sitio con "[replicación](#)", especifique uno o más pools de almacenamiento específicos del sitio en la "[Instrucciones de colocación para cada regla de ILM](#)".

Se crea automáticamente un pool de almacenamiento para cada sitio durante la instalación de StorageGRID.

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 pool de almacenamiento que contenga solo el nuevo sitio. A continuación, "[Actualice las reglas de ILM](#)" para controlar qué objetos se almacenan en el nuevo sitio.
- Si la cantidad de copias es inferior a la cantidad de pools de almacenamiento, el sistema distribuye las copias para equilibrar el uso de disco entre los pools.
- 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.

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

- De protección contra pérdida de sitio con "[código de borrado](#)", cree pools de almacenamiento que consten de al menos tres sitios. Si un pool de almacenamiento incluye solo dos sitios, no puede usar ese pool de almacenamiento para el código de borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.
- La cantidad de nodos de almacenamiento y sitios incluidos en el pool de almacenamiento determina cuáles "[esquemas de código de borrado](#)" están disponibles.
- 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.
- Si tiene requisitos de alto rendimiento, no se recomienda el uso de 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 alcanzables de ingesta y recuperación de objetos (cuando se seleccionan equilibrados o estrictos como comportamiento de procesamiento) o puede provocar retrasos en la cola de ILM (cuando se selecciona Dual commit como comportamiento de procesamiento). Consulte "[Comportamiento de procesamiento de reglas de ILM](#)".



Si su grid incluye solo un sitio, no podrá usar el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) o el sitio predeterminado Todos los sitios en un perfil de código de borrado. Este comportamiento evita que el perfil no sea válido si se agrega un segundo sitio.

- No se pueden usar nodos de archivo para datos con código de borrado.

Directrices para los pools de almacenamiento utilizados para copias archivadas

La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.



La opción Cloud Tiering - Simple Storage Service (S3) también queda obsoleta. Si está utilizando un nodo de archivado con esta opción, "[Migre sus objetos a un pool de almacenamiento en la nube](#)" en su lugar.

Además, debe eliminar los nodos de archivado de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o versiones anteriores. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "[Trabajar con reglas de ILM y políticas de ILM](#)".

- No puede crear un pool de almacenamiento que incluya nodos de almacenamiento y nodos de archivado.

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 Bloqueo de objetos S3 está habilitada y está creando una regla de ILM compatible, no puede utilizar un pool de almacenamiento que incluya 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.

Habilite la protección contra pérdida de sitio

Si la implementación de StorageGRID incluye más de un sitio, puede usar la replicación y el código de borrado con los pools de almacenamiento configurados correctamente para habilitar la protección contra pérdida de sitio.

La replicación y el código de borrado necesitan diferentes configuraciones de pools de almacenamiento:

- Para utilizar la replicación para la protección contra pérdida de sitio, utilice los pools de almacenamiento específicos de sitios que se crean automáticamente durante la instalación de StorageGRID. A continuación, cree reglas de ILM con "[Instrucciones de colocación](#)" esto especifica varios pools de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar código de borrado para la protección contra pérdida de sitio, "[cree pools de almacenamiento que consten de varios sitios](#)". A continuación, cree reglas de ILM que usen un pool de almacenamiento que conste de varios sitios y cualquier esquema de código de borrado disponible.

 A la hora de configurar su implementación de StorageGRID para la protección contra pérdida de sitio, también debe tener en cuenta los efectos de "[opciones de procesamiento](#)" y.. "[coherencia](#)".

Ejemplo de replicación

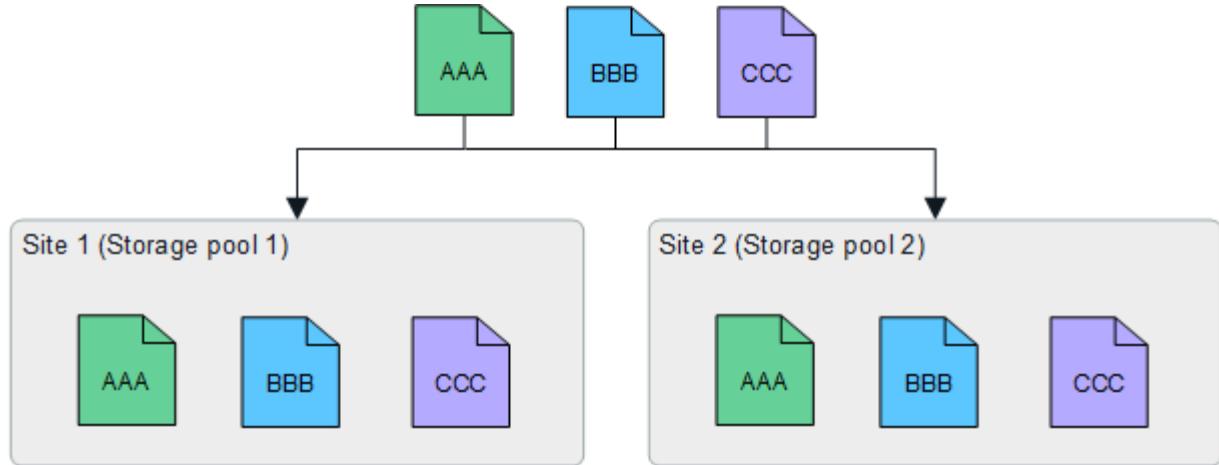
De forma predeterminada, se crea un pool de almacenamiento para cada sitio durante la instalación de StorageGRID. Tener pools de almacenamiento compuestos solo por un sitio le permite configurar reglas de ILM que utilizan la replicación para la protección contra pérdida de sitio. En este ejemplo:

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

Ubicaciones de reglas de ILM:

Store objects by replicating 1 copies at Site 1  

and store objects by replicating 1 copies at Site 2  



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

Ejemplo de código de borrado

Tener pools de almacenamiento compuestos por más de un sitio por pool de almacenamiento permite configurar reglas de ILM que utilicen código de borrado para la protección contra pérdida de sitio. En este ejemplo:

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

Ubicaciones de reglas de ILM:

Store objects by erasure coding using 4+2 EC at Storage pool 1 (3 sites)  

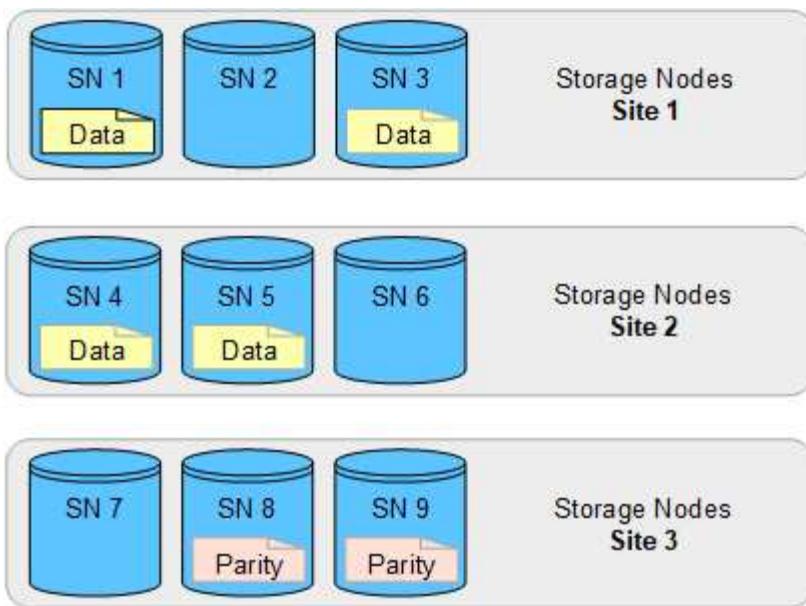
En este ejemplo:

- La regla de ILM utiliza un esquema de código 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.

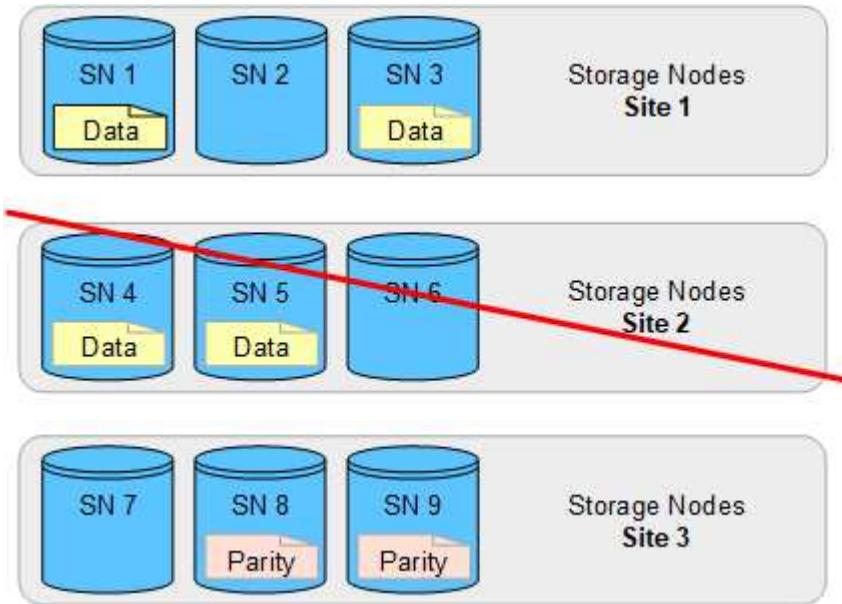


Se permite el código de borrado en pools de almacenamiento que contienen cualquier número de sitios **excepto** dos sitios.

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



Si se pierde un sitio, es posible recuperar los datos:



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.



Cuando se instala StorageGRID 11,8 en un nuevo grid, se crean automáticamente pools de almacenamiento para cada sitio. Sin embargo, si instaló inicialmente StorageGRID 11,6 o una versión anterior, los pools de almacenamiento no se crean automáticamente para cada sitio.

Si desea crear pools de almacenamiento en cloud para almacenar datos de objetos fuera del sistema StorageGRID, consulte ["Información sobre el uso de Cloud Storage Pools"](#).

Antes de empezar

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



No incluya el sitio Todos los sitios en un pool de almacenamiento que se utilizará en un perfil de código de borrado. En su lugar, agregue una entrada independiente al pool de almacenamiento para cada sitio que almacene los datos con código de borrado. Consulte [este paso](#) por ejemplo.

- Si 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**.

En la pestaña Storage Pools, se muestra todos los pools de almacenamiento definidos.



Para las instalaciones nuevas de StorageGRID 11,6 o versiones anteriores, el pool de almacenamiento Todos los nodos de almacenamiento se actualiza automáticamente cada vez que se añaden sitios de centros de datos nuevos. No utilice este pool en reglas de ILM.

2. Para crear una nueva agrupación de almacenamiento, seleccione **Crear**.
3. Introduzca un nombre único para el pool de almacenamiento. Utilice un nombre que sea 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 Todos los sitios en ningún pool 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 **Storage grade**, seleccione el tipo de almacenamiento que se utilizará si una regla de ILM utiliza este grupo de almacenamiento.

El grado de almacenamiento, *incluye todos los grados 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 grupo de almacenamiento en un perfil de codificación de borrado de varios sitios, seleccione **Agregar más nodos** para agregar una entrada para cada sitio al grupo de almacenamiento.



Se le impide crear entradas duplicadas o crear un pool de almacenamiento que incluya tanto el grado de almacenamiento de los nodos de archivado como cualquier grado de almacenamiento que contenga nodos de almacenamiento.

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

Para eliminar una entrada, seleccione el icono de eliminación

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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "[permisos de acceso específicos](#)".

Pasos

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

La tabla Storage Pools incluye la siguiente información para cada pool de almacenamiento que incluye nodos de almacenamiento:

- **Nombre:** El nombre exclusivo para mostrar de la agrupación de almacenamiento.
- **Node count:** El número de nodos en el pool de almacenamiento.
- **Uso de almacenamiento:** El porcentaje del espacio total utilizable que se ha utilizado para los datos de objetos en este nodo. Este valor no incluye metadatos de objetos.
- * **Capacidad total*:** El tamaño del pool de almacenamiento, que equivale a la cantidad total de espacio utilizable para los datos de objetos para todos los nodos del pool de almacenamiento.
- **Uso de ILM:** Cómo se está utilizando actualmente el pool de almacenamiento. Es posible que un pool de almacenamiento no se utilice o que se utilice en una o más reglas de ILM, perfiles de código de borrado, o ambas.



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

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

Se muestra la página de detalles del pool de almacenamiento.

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

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

- Nombre del nodo
- Nombre del sitio
- Grado de almacenamiento
- Uso de almacenamiento: El porcentaje del espacio útil total para datos de objeto que se ha utilizado para el nodo de almacenamiento. Este campo no está visible para los pools de nodos de archivado.



El mismo valor de Uso de almacenamiento (%) 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 **ILM usage** para determinar si el pool de almacenamiento se está utilizando actualmente en reglas de ILM o perfiles de codificación de borrado.
5. Opcionalmente, vaya a la página de reglas de ILM * para conocer y administrar las reglas que utilizan el grupo de almacenamiento.

Consulte "[Instrucciones para trabajar con reglas 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "[permisos de acceso específicos](#)".
- Ha revisado el "[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 sitio o nivel de almacenamiento a un pool de almacenamiento que se usa en la política de ILM activa, tenga en cuenta que los nodos de almacenamiento del sitio nuevo o el grado de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a utilizar un sitio o nivel de almacenamiento nuevo, debe activar una nueva política de ILM después de guardar el pool de almacenamiento editado.

Pasos

1. Seleccione **ILM > agrupaciones de almacenamiento**.
2. Seleccione la casilla de comprobación del pool de almacenamiento que desea editar.

No se puede editar el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y versiones anteriores).

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.



Se le impide cambiar el sitio o el grado de almacenamiento si el grupo de almacenamiento se utiliza en un perfil de código de borrado y el cambio provocaría que el esquema de código de borrado dejara de ser 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 añadió un nuevo sitio o grado de almacenamiento a un pool de almacenamiento usado en la política de gestión del ciclo de vida de la información activa, active una nueva política de gestión del ciclo de vida de la información para forzar a StorageGRID a usar el nuevo sitio o el grado de almacenamiento. Por ejemplo, Clone la política de ILM existente y luego active el clon. Consulte "[Trabaje con las reglas de ILM y las políticas de ILM](#)".

Quitar un pool de almacenamiento

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Usted tiene la "[permisos de acceso requeridos](#)".

Pasos

1. Seleccione **ILM > agrupaciones de almacenamiento**.
2. Revise la columna Uso de ILM de la tabla para determinar si se puede quitar el pool de almacenamiento.

No se puede quitar un pool de almacenamiento si se está utilizando en una regla de gestión de la vida útil de la información o en un perfil de código de borrado. Según sea necesario, seleccione **storage pool name > ILM usage** para determinar dónde se utiliza el pool de almacenamiento.

3. Si el pool de almacenamiento que desea quitar no se está utilizando, seleccione la casilla de comprobación.
4. Seleccione **Quitar**.
5. Seleccione **OK**.

Utilice Cloud Storage Pools

¿Qué es un pool de almacenamiento en 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 desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en cloud de bajo coste,

como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivado en el almacenamiento de 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).

 El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API S3 está obsoleto y ha sido reemplazado por pools de almacenamiento en la nube de ILM, que ofrecen más funcionalidad. Si actualmente está utilizando un nodo de archivado con la opción Cloud Tiering - Simple Storage Service (S3), ["Migre sus objetos a un pool de almacenamiento en la nube"](#) en su lugar.

La tabla compara los pools de almacenamiento con los pools de almacenamiento en cloud y muestra las similitudes y las diferencias a alto nivel.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Cómo se crea?	Uso de la opción ILM > agrupaciones de almacenamiento en Grid Manager.	Usando la opción ILM > Storage Pools > Cloud Storage Pools 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.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento o nodos de archivado dentro de StorageGRID.	<p>En un bloque de Amazon S3, un contenedor de almacenamiento de Azure Blob o Google Cloud externo al sistema StorageGRID.</p> <p>Si Cloud Storage Pool es un bloque de Amazon S3:</p> <ul style="list-style-type: none"> 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 S3 RestoreObject. 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. <p>Si Cloud Storage Pool es un contenedor de almacenamiento de Azure Blob, StorageGRID realiza la transición del objeto al nivel de archivado.</p> <p>Nota: En general, no configure la gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor utilizado para un Cloud Storage Pool. Las operaciones de RestoreObject en objetos del Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.</p>
¿Qué controla la ubicación de objetos?	Una regla de ILM en las políticas de ILM activas.	Una regla de ILM en las políticas de ILM activas.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.
¿Cuántas copias de cada objeto se permiten?	Múltiples.	<p>Una copia en el pool de almacenamiento cloud y, opcionalmente, una o varias copias en StorageGRID.</p> <p>Nota: No puedes almacenar un objeto en más de un Pool de almacenamiento en la nube en un momento dado.</p>
¿Cuáles son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
		Nota: Los datos de FabricPool no se pueden organizar en niveles en los grupos de almacenamiento en la nube. Los objetos con bloqueo de objetos S3 activado no se pueden colocar en pools de Cloud Storage.

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

Los pasos describen las etapas del ciclo de vida de un objeto que se almacena en un pool de almacenamiento en cloud S3.

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

 Google Cloud Platform (GCP) admite la recuperación de objetos 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 ha movido al pool de almacenamiento en la nube de S3, la aplicación cliente puede recuperarlo mediante una solicitud GetObject de S3 de StorageGRID, a menos que el objeto se haya trasladado al almacenamiento de 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 del ciclo de vida para el bucket externo de S3, y debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API S3 RestoreObject.



No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. SWIFT no admite las solicitudes `RestoreObject`, por lo que StorageGRID no podrá recuperar ningún objeto Swift que se haya realizado la transición 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 utilizar una solicitud `S3 HeadObject` para supervisar el estado del objeto.

4. Objeto restaurado desde el almacenamiento Glacier

Si se ha realizado la transición de un objeto al almacenamiento de Glacier, la aplicación cliente puede emitir una solicitud `S3 RestoreObject` para restaurar una copia que se pueda recuperar en el Cloud Storage Pool 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 existen una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier emitiendo una solicitud `RestoreObject`. En su lugar, la copia local se puede recuperar directamente mediante una solicitud `GetObject`.

5. Objeto recuperado

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

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

Los pasos describen las etapas del ciclo de vida de un objeto que se almacena 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 gestión de la vida útil de la información que utiliza un pool de almacenamiento en cloud de Azure como ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento externo de Azure Blob especificado por el pool de almacenamiento en cloud.



No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. SWIFT no admite las solicitudes `RestoreObject`, por lo que StorageGRID no podrá recuperar ningún objeto Swift que se haya realizado la transición 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 un objeto se ha trasladado al nivel de archivado, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en Azure Cloud Storage Pool.

Cuando StorageGRID recibe el RestoreObject, hace la transición temporal del objeto al nivel Cool de almacenamiento de Azure Blob. Tan pronto como se alcanza la fecha de caducidad en la solicitud RestoreObject, StorageGRID devuelve el objeto al nivel Archive.



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

5. Objeto recuperado

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

Información relacionada

["USE LA API DE REST DE S3"](#)

Cuándo usar Cloud Storage Pools

Con Cloud Storage Pools, puede crear un backup o organizar los datos en niveles en una ubicación externa. Además, puede hacer backups o organizar los datos en más de un cloud.

Backup de datos de StorageGRID en ubicaciones externas

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 necesite emitir una solicitud S3 RestoreObject para acceder a la copia del objeto de backup en 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.

Organice los datos en niveles desde StorageGRID a 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 extremos de Cloud Storage Pool si desea organizar en niveles o realizar backups de datos de objetos en más de una nube. Los filtros de las reglas de ILM permiten especificar los objetos que se almacenan en cada Cloud Storage Pool. Por ejemplo, es posible que desee almacenar objetos de algunos clientes o buckets en Amazon S3 Glacier y objetos de otros inquilinos o buckets 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 se utilizan varios extremos de Cloud Storage Pool, tenga en cuenta que un objeto se puede almacenar solo en un Cloud Storage Pool 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 utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. SWIFT no admite las solicitudes `RestoreObject`, por lo que StorageGRID no podrá recuperar ningún objeto Swift que se haya

realizado la transición al almacenamiento S3 Glacier o 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).

- No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.
- Los objetos con bloqueo de objetos S3 activado no se pueden colocar en pools de Cloud Storage.
- Si el bucket S3 de destino para un pool de almacenamiento en la nube tiene S3 Object Lock habilitado, el intento de configurar la replicación de bucket (PutBucketReplication) fallará con un error ACCESSDENIED.

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 "["configurar 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, volverá a configurar las reglas y políticas 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 de S3 externo especificado en el pool de almacenamiento en cloud está controlado por las reglas de ILM y las políticas de ILM activas 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 depósito externo de S3, y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

Por ejemplo, supongamos que desea que 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 use gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor que se usa con un pool de almacenamiento en cloud. 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"](#)

Compare 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?	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. Esto es, en lugar de conservar dos copias en el sitio, puede conservar una copia dentro de StorageGRID y enviar una copia al Pool de almacenamiento en cloud.	Permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) a un bloque S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente.
¿Cómo se configura?	Se definen del mismo modo que los pools de almacenamiento, mediante Grid Manager o la API de gestión de grid. Se puede seleccionar 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?	<ul style="list-style-type: none"> • Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Nivel de Azure Blob Archive • Google Cloud Platform (GCP) 	<ul style="list-style-type: none"> • Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Google Cloud Platform (GCP)
¿Qué hace que los objetos se muevan al destino?	Una o más reglas de ILM en las políticas de ILM activas. Las reglas de ILM definen los objetos que StorageGRID se mueve al Cloud Storage Pool y cuándo se mueven los objetos.	Acción de ingerir un nuevo objeto en un depósito de origen que se haya configurado con un punto final de CloudMirror. Los objetos que existían en el bloque de origen antes de que se configurara con el extremo de CloudMirror no se replican, a menos que se modifiquen.

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿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 transfiere 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 del 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

Un Cloud Storage Pool especifica un único bloque externo de Amazon S3 u otro proveedor compatible con S3 o contenedor de almacenamiento de Azure Blob.

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

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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la ["permisos de acceso requeridos"](#).
- Ha revisado el ["Consideraciones para Cloud Storage Pools"](#).
- Ya existe el depósito o contenedor externo al que hace referencia Cloud Storage Pool y conoce su nombre y ubicación.
- Para acceder al depósito o contenedor, tiene la siguiente información para el tipo de autenticación que elegirá:

Tecla de acceso S3

Para el cubo externo S3

- El ID de clave de acceso de la cuenta que posee el bloque externo.
- La clave de acceso secreta asociada.

Como alternativa, puede especificar Anonymous para el tipo de autenticación.

Portal de acceso C2S

Para servicios en la nube comercial (C2S) S3 SERVICE

Tiene lo siguiente:

- URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor del portal de acceso C2S (CAP), incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
- Certificado de CA de servidor emitido por una entidad de certificación (CA) gubernamental apropiada. StorageGRID utiliza este certificado para comprobar la identidad del servidor CAP. El certificado de CA del servidor debe utilizar la codificación PEM.
- Certificado de cliente emitido por una autoridad de certificación gubernamental (CA) apropiada. 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.
- Clave privada codificada con PEM para el certificado de cliente.
- Frase de acceso para descifrar la clave privada para el certificado de cliente, si está cifrada.



Si el certificado de cliente se cifrará, utilice el formato tradicional para el cifrado. El formato cifrado PKCS #8 no es compatible.

Almacenamiento de Azure Blob

Para el contenedor externo

- Identificador de Recursos Uniforme (URI) utilizado para acceder al contenedor Blob Storage.
- Nombre de la cuenta de almacenamiento y la clave de cuenta. Puede usar el portal de Azure para encontrar estos valores.

Pasos

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

Campo	Descripción
Nombre de Cloud Storage Pool	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	<p>Qué proveedor de cloud utilizará para este pool de almacenamiento en cloud:</p> <ul style="list-style-type: none"> • Amazon S3/GCP: Seleccione esta opción para un proveedor compatible con Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • Almacenamiento de Azure Blob
Cubo o contenedor	El nombre del bloque externo de S3 o contenedor de Azure. No se puede cambiar este valor después de guardar Cloud Storage Pool.

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

Amazon S3/GCP

- a. Para el protocolo, seleccione HTTPS o HTTP.



No utilice conexiones HTTP para datos confidenciales.

- b. Introduzca el nombre de host. Ejemplo:

`s3-aws-region.amazonaws.com`

- c. Seleccione el estilo de URL:

Opción	Descripción
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.
Estilo hospedado virtual	Use una URL de estilo alojada virtual para acceder al bloque. Las URL de estilo hospedado virtual incluyen el nombre del bucket como parte del nombre de dominio. Ejemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo de ruta	Utilice una dirección URL de estilo de ruta para acceder al bloque. Las URL de estilo de ruta incluyen el nombre del cubo al final Ejemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: La opción de URL de estilo de ruta no se recomienda y se descartará en una futura versión de StorageGRID.

- d. De manera opcional, introduzca el número de puerto o utilice el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de Azure Blob

- a. Con uno de los siguientes formatos, introduzca el URI para el punto final de servicio.

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

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

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

4. Seleccione **continuar**. A continuación, seleccione el tipo de autenticación e introduzca la información requerida para el extremo de Cloud Storage Pool:

Clave de acceso

Solo para el tipo de proveedor de Amazon S3/GCP

- a. Para **ID de clave de acceso**, ingrese el ID de clave de acceso de la cuenta que posee el depósito externo.
- b. Para **Clave de acceso secreta**, ingrese la clave de acceso secreta.

CAP (portal de acceso C2S)

Para servicios en la nube comercial (C2S) S3 SERVICE

- a. Para **URL de credenciales temporales**, ingrese la URL completa que StorageGRID usará para obtener credenciales temporales del servidor CAP, incluyendo todos los parámetros API requeridos y opcionales asignados a su cuenta C2S.
- b. Para **Certificado CA de servidor**, seleccione **Examinar** y cargue el certificado CA codificado con PEM que StorageGRID utilizará para verificar el servidor CAP.
- c. Para **Certificado de cliente**, seleccione **Examinar** y cargue el certificado codificado con PEM que StorageGRID utilizará para identificarse en el servidor CAP.
- d. Para **Clave privada del cliente**, seleccione **Examinar** y cargue la clave privada codificada con PEM para el certificado del cliente.
- 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 **Client private key passphrase**.

Almacenamiento de Azure Blob

- a. Para **Nombre de cuenta**, ingrese el nombre de la cuenta de almacenamiento de Blob que posee el contenedor de servicio externo.
- b. Para **Clave de cuenta**, ingresa la clave secreta para la cuenta de almacenamiento de Blob.

Anónimo

No se requiere información adicional.

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

Opción	Descripción
Utilice los certificados de CA raíz en el sistema operativo del nodo de almacenamiento	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 Browse y cargue el certificado codificado PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

6. Seleccione **Guardar**.

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

- Valida que el depósito o contenedor y el punto final del servicio existen y que se puede acceder a ellos mediante las credenciales que ha especificado.
- Escribe un archivo de marcador en el bloque o contenedor para identificarlo como un Cloud Storage Pool. 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, puede que se informe un error si hay un error de certificado o si el bloque o el contenedor especificados no existen ya.

7. Si se produce un error, consulte "[Instrucciones para solucionar problemas de Cloud Storage Pools](#)", Resuelva cualquier problema y, a continuación, intente guardar el Pool de almacenamiento en cloud de nuevo.

Editar un pool de almacenamiento en el cloud

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Ya tienes "[permisos de acceso específicos](#)".
- Ha revisado el "[Consideraciones para Cloud Storage Pools](#)".

Pasos

1. Selecciona **ILM > Pools de almacenamiento > Pools de almacenamiento en la nube**.

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

2. Selecciona la casilla de verificación para el pool de almacenamiento en la nube que desea editar.
3. Selecciona **Acciones > 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, el bucket de S3 o el contenedor de Azure para un Cloud Storage Pool.

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

5. Selecciona **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 si no se utiliza en una regla de gestión de la vida útil de la información y no contiene datos de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Usted tiene la "[permisos de acceso requeridos](#)".

Si es necesario, utilice ILM para mover datos de objetos

Si el Cloud Storage Pool que desea quitar contiene datos de objetos, debe usar ILM para mover los datos a otra ubicación. Por ejemplo, puede mover los datos a Nodos de almacenamiento en el grid o a otro Pool de almacenamiento en la nube.

Pasos

1. Selecciona **ILM > Pools de almacenamiento > Pools de almacenamiento en la nube**.
2. Observe la columna Uso de ILM en la tabla para determinar si puede quitar Cloud Storage Pool.

No puede quitar un pool de almacenamiento de cloud si se está utilizando en una regla de gestión de la vida útil de la información o en un perfil de código de borrado.

3. Si se está utilizando Cloud Storage Pool, seleccione **cloud storage pool name > ILM usage**.
4. "[Clone cada regla de ILM](#)" Que actualmente coloca objetos en el Cloud Storage Pool que desea eliminar.
5. Determine dónde desea mover los objetos existentes gestionados por cada regla clonada.

Puede utilizar uno o más pools de almacenamiento o un pool de almacenamiento en cloud diferente.

6. Edite cada una de las reglas clonadas.

Para el Paso 2 del Asistente para crear reglas de ILM, seleccione la nueva ubicación en el campo **Copias en**.

7. "[Cree una nueva política de ILM](#)" y reemplace cada una de las reglas antiguas por una regla clonada.
8. Activar la nueva política.
9. Espere a que ILM elimine objetos del Cloud Storage Pool y colóquelos en la nueva ubicación.

Eliminar Pool de Almacenamiento en Nube

Cuando el pool de almacenamiento en cloud está vacío y no se usa en ninguna regla de ILM, puede eliminarlo.

Antes de empezar

- QUITÓ todas las reglas de ILM que pueden haber utilizado el pool.
- 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 tiene el nombre `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Si la columna ILM usage indica que Cloud Storage Pool no se está usando, seleccione la casilla de comprobación.
3. Seleccione **acciones** > **Quitar**.
4. Seleccione **OK**.

Solucionar problemas de Cloud Storage Pools

Utilice estos pasos de solución de problemas para resolver los errores que puede encontrar al crear, editar o eliminar un pool de almacenamiento en la nube.

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 última columna de error de la tabla Cloud Storage Pools de 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 Grupos de almacenamiento (seleccione **ILM** > **Grupos de almacenamiento**), revise los mensajes de error en la última columna de error y consulte las directrices para la solución de problemas que aparecen a continuación.

Compruebe si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. En la página Cloud Storage Pool, seleccione el punto final 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 se mostrará en la última columna de error en unos pocos 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 punto final de servicio utilizado para el pool de almacenamiento en la nube no utiliza HTTP para un contenedor o depósito 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 depósito.
- 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 allí mediante ILM, datos que estaban en el depósito antes de configurar el pool de almacenamiento en cloud o datos que algún otro origen puso en el depósito después de crear el pool de almacenamiento en cloud.

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

- Siga las instrucciones para volver a mover objetos a StorageGRID en «Ciclo de vida de un objeto de pool 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 configuró un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el extremo externo S3 utilizado para el pool de almacenamiento en nube. Este error se produce si el servidor proxy externo no puede alcanzar el punto final 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 redes del servidor proxy de almacenamiento.

Información relacionada

["Ciclo de vida de un objeto de Cloud Storage Pool"](#)

Gestione perfiles de código de borrado

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).

- Usted tiene la "[permisos de acceso requeridos](#)".

Consulte los detalles del perfil de código de borrado

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

Pasos

1. Seleccione **ILM > codificación de borrado**.
2. Seleccione el perfil. Aparece la página de detalles del perfil.
3. De manera opcional, consulte la pestaña reglas de ILM para ver una lista de reglas de ILM que utilizan el perfil y las políticas de ILM que utilizan esas reglas.
4. Opcionalmente, consulte la pestaña Nodos de almacenamiento para obtener más información sobre cada nodo de almacenamiento en el pool de almacenamiento del perfil, como el sitio donde se encuentra y el uso del almacenamiento.

Cambie el nombre de un perfil de código de borrado

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

Pasos

1. Seleccione **ILM > codificación de borrado**.
2. Seleccione el perfil al que desea cambiar el nombre.
3. Seleccione **Cambiar nombre**.
4. Introduzca un nombre único para el perfil de codificación de borrado.

El nombre del perfil de codificación de borrado se añade al nombre del pool de almacenamiento en la instrucción de ubicación para una regla de ILM.



Los nombres de perfil 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 está utilizando en ninguna regla de ILM.



Confirme que no hay operaciones de reparación de datos con código de borrado ni procedimientos de decomiso en curso. Se devuelve un mensaje de error si se intenta desactivar un perfil de código de borrado mientras se realiza alguna de estas operaciones.

Acerca de esta tarea

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

- El perfil de código de borrado se utiliza actualmente en una regla de ILM.

- El perfil de código de borrado ya no se usa en ninguna regla de ILM, pero los datos de objetos y fragmentos de paridad del perfil siguen existiendo.

Pasos

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

No puede desactivar un perfil de código de borrado si se utiliza en alguna regla de ILM. En el ejemplo, se utiliza el perfil de centro de datos 2+1 1 en al menos una regla de ILM.

<input type="checkbox"/> Profile name	Status	Storage pool	Erasure-coding scheme
<input type="checkbox"/> 2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
<input type="checkbox"/> New profile	Deactivated	Data Center 1	2+1

3. Si el perfil se utiliza en una regla de ILM, siga estos pasos:
 - a. Selecciona **ILM > Reglas**.
 - b. Seleccione cada regla y revise el diagrama de retención para determinar si la regla utiliza el perfil de codificación de borrado que desea desactivar.
 - c. Si la regla de ILM utiliza el perfil de código de borrado que desea desactivar, determine si la regla se utiliza en alguna política de ILM.
 - d. Complete los pasos adicionales de la tabla, en función del perfil de código de borrado que se utilice.

¿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.	<i>Ninguno</i>
En una regla de ILM que nunca se haya usado en ninguna política de ILM	<ol style="list-style-type: none"> 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 está actualmente en una política de ILM activa	<p>i. Clone la política.</p> <p>ii. Elimine la regla de ILM que utilice el perfil de código de borrado.</p> <p>iii. Añada una o varias reglas nuevas de ILM para garantizar la protección de los objetos.</p> <p>iv. Guarde, simule y active la nueva directiva.</p> <p>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.</p> <p>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.</p> <p>Aunque puede intentar desactivar de forma segura un perfil de codificación de borrado mientras aún está asociado a los datos, la operación de desactivación fallará. Un mensaje de error le informará si el perfil aún no está listo para ser desactivado.</p> <p>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.</p> <p>vii. Continúe con este procedimiento.</p>	<p>"Cree una política de ILM"</p> <p>"Trabaje con las reglas de ILM y las políticas de ILM"</p>
En una regla de ILM que está actualmente en una política de ILM	<p>i. Edite la política.</p> <p>ii. Elimine la regla de ILM que utilice el perfil de código de borrado.</p> <p>iii. Añada una o varias reglas nuevas de ILM para garantizar que todos los objetos estén protegidos.</p> <p>iv. Guarde la política.</p> <p>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.</p> <p>vi. Continúe con este procedimiento.</p>	<p>"Cree una política de ILM"</p> <p>"Trabaje con las reglas de ILM y las políticas de ILM"</p>

- e. Refresque la página de perfiles de codificación de borrado para asegurarse de que el perfil no se utiliza 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 codificación de borrado.



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

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

Resultados

- Si StorageGRID puede desactivar el perfil de código de borrado, su estado es Desactivado. Ya no puede seleccionar este perfil para ninguna regla de ILM. No puede reactivar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto 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.



No puede cambiar la región de un depósito después de haber creado el depósito.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "[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 se aplique sólo a los objetos de los cubos S3 creados en el `us-west-2` región. 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 cubos pertenecen al `us-east-1` región.
- 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 entre mayúsculas y minúsculas. 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 puede eliminar ni modificar una región si se utiliza en una regla asignada a cualquier política (activa o inactiva).
- Si utiliza una región no válida como filtro avanzado en una regla de ILM, no puede agregar esa regla a una política.

Se puede producir una región no válida si utiliza una región como filtro avanzado en una regla de ILM, pero posteriormente 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 o eliminar.

2. Para agregar una región:

a. Selecciona **Añadir otra región**.

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 cualquier política (activa o inactiva).

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

Ahora puede seleccionar estas regiones en la sección Advanced Filters en el paso 1 del asistente de creación de reglas de ILM. Consulte "["Usar filtros avanzados en las reglas de ILM"](#)".

Cree la regla de ILM

Cree una regla de ILM: Información general

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.



Los metadatos de objetos no se gestionan 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.

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 ingestión:** El comportamiento de ingestión de una regla le permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 o Swift guarda un objeto en la cuadrícula).

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 objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Estos filtros le permiten aplicar una regla a cuentas de inquilino específicas, cubos S3 específicos o contenedores Swift, o ambos.

Los filtros básicos le dan una manera 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.

- Los filtros avanzados le proporcionan un control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades de objeto:
 - Tiempo de ingestión
 - Hora del último acceso
 - Todo o parte del nombre del objeto (clave)
 - Restricción de ubicación (sólo S3)
 - Tamaño del objeto
 - Metadatos del usuario

- Etiqueta de objeto (solo S3)

Puede filtrar objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de imágenes de un hospital pueden usarse con frecuencia cuando tienen menos de 30 días 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.

Puede combinar filtros 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, puede crear reglas que filtren por cuenta de arrendatario para segregar los registros de cada departamento, mientras utiliza filtros en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

Instrucciones para colocar las 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 puede comenzar 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 solo período de tiempo, seleccione **Añadir otro tipo o ubicación** para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione **Agregar otro período de tiempo** para agregar el siguiente período de tiempo. A continuación, especifique una o más líneas dentro del período de tiempo.

En el ejemplo se muestran dos instrucciones de colocación en la página Definir ubicaciones del asistente Crear reglas de ILM.

Time period and placements

[Sort by start date](#)

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

The screenshot shows the StorageGRID rule configuration interface. It displays two time periods with their respective placement rules:

- Time period 1:** From Day 0 store for 365 days. This rule includes:
 - Store objects by replicating 2 copies at Data Center 1 and Data Center 2.
 - and store objects by erasure coding using a 6+3 EC scheme at all sites.
- Time period 2:** From Day 365 store forever. This rule includes:
 - Store objects by replicating 2 copies at Data Center 3.

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

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

La segunda instrucción de colocación ② crea dos copias al año siguiente y guarda 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.

Comportamiento de procesamiento de reglas de ILM

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. Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Balanceado:** StorageGRID intenta hacer todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Estricto:** Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **Confirmación doble:** StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el

éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Información relacionada

- ["Opciones de procesamiento"](#)
- ["Ventajas, desventajas y limitaciones de las opciones de ingestá"](#)
- ["Cómo interactúan las reglas de coherencia e ILM para afectar a la protección de datos"](#)

Regla de ILM de ejemplo

Por ejemplo, una regla de ILM podría especificar lo siguiente:

- Aplicar solo a los objetos que pertenecen al inquilino A..
- Realice dos copias replicadas de dichos objetos y almacene cada copia en un sitio diferente.
- Conservar las dos copias «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que se eliminen mediante una solicitud de eliminación del cliente o cuando finalice el ciclo de vida de un bloque.
- Use la opción Equilibrada para el comportamiento de ingestá: La instrucción de ubicación de dos sitios se aplica en cuanto el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible hacer inmediatamente las dos copias requeridas.

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

- ["Qué es un pool de almacenamiento"](#)
- ["Qué es un pool de almacenamiento en la nube"](#)

Acceda al asistente Create an 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 an ILM Rule.



Si desea crear la regla de ILM predeterminada para una política, siga el ["Instrucciones para crear una regla de ILM predeterminada"](#) en su lugar.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes ["permisos de acceso específicos"](#).
- Si desea especificar a qué cuentas de arrendatario se aplica esta regla, tiene la ["Permiso para cuentas de inquilino"](#) O ya sabes el ID de cuenta de cada cuenta.
- Si desea que la regla filtre objetos en los metadatos de la última hora de acceso, las actualizaciones de la última hora de acceso deben habilitarse mediante bloque para S3 o por contenedor para Swift.
- Ha configurado los pools de Cloud Storage que desee utilizar. Consulte ["Cree el pool de almacenamiento en el cloud"](#).
- Usted está familiarizado con el ["opciones de procesamiento"](#).
- 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 gestión del ciclo de vida de la información en StorageGRID 11,8".

■

Acerca de esta tarea

Al crear reglas de ILM:

- Considere la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Piense en qué tipos de copias de objetos desea realizar (replicadas o con código de 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 de ingestión utilizar (Compromiso equilibrado, estricto o doble).

Pasos

1. Selecciona **ILM > Reglas**.
2. Selecciona **Crear**. "[Paso 1 \(Introducir detalles\)](#)" Se mostrará el asistente Crear una regla de ILM.

Paso 1 de 3: Introduzca los detalles

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

La introducción de una descripción y la definición de filtros para la regla son opcionales.

Acerca de esta tarea

Al evaluar un objeto contra un "[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**.
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.

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 tiene el permiso de acceso raíz o las cuentas de inquilino, no puede seleccionar arrendatarios de 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 **Aplica a todos los cubos** (predeterminado), la regla se aplica a todos los cubos S3 o contenedores Swift.

5. Para los inquilinos S3, opcionalmente seleccione **Sí** para aplicar la regla solo a versiones de objetos más antiguas en cubos S3 que tienen el control de versiones activado.

Si selecciona **Sí**, la opción “Hora no corriente” se seleccionará automáticamente para la Hora de referencia en [“Paso 2 del asistente Crear una regla de ILM”](#).



La hora no actual se aplica solo a objetos S3 en bloques con control de versiones activado. Consulte ["Operaciones en cucharones, PutBucketVersioning"](#) y.. ["Gestione objetos con S3 Object Lock"](#).

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"](#).

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

Si no configura el filtrado avanzado, la regla se aplica a todos los objetos que coincidan con los filtros básicos. Para obtener más información sobre el filtrado avanzado, consulte [Usar filtros avanzados en las reglas de ILM](#) y.. [Especifique varios tipos y valores de metadatos](#).

7. Seleccione **continuar**. ["Paso 2 \(Definir ubicaciones\)"](#) Se mostrará el asistente Crear una regla de ILM.

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 ingestión	<ul style="list-style-type: none">• es• no lo es• es antes• es el o antes• es posterior• es el o después	<p>Hora y fecha en la que se ingirió el objeto.</p> <p>Nota: Para evitar problemas de recursos al activar una nueva política de ILM, puede usar el filtro avanzado de tiempo de ingestión en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de procesamiento en 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.</p>

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Clave	<ul style="list-style-type: none"> • es igual a • no es igual • contiene • no contiene • comienza con • no empieza por • termina con • no termina con 	<p>Todo o parte de una clave de objeto S3 o Swift única.</p> <p>Por ejemplo, quizás desee hacer coincidir los objetos que terminan con <code>.txt</code> o empiecen por <code>test-object/</code>.</p>
Hora del último acceso	<ul style="list-style-type: none"> • es • no lo es • es antes • es el o antes • es posterior • es el o después 	<p>Hora y fecha en la que se recuperó por última vez el objeto (leído o visualizado).</p> <p>Nota: Si planeas hacerlo "utilizar la hora del último acceso" Como filtro avanzado, las actualizaciones de la hora del último acceso deben estar habilitadas para el depósito S3 o el contenedor Swift.</p>
Restricción de ubicación (sólo S3)	<ul style="list-style-type: none"> • es igual a • no es igual 	<p>Región en la que se creó un bloque de S3. Utilice ILM > Regiones para definir las regiones que se muestran.</p> <p>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. Consulte ""Configurar regiones (opcional solo S3)"".</p>
Tamaño del objeto	<ul style="list-style-type: none"> • es igual a • no es igual • menor que • menor o igual que • mayor que • mayor o igual que 	<p>Tamaño del objeto.</p> <p>El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.</p>

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Metadatos del usuario	<ul style="list-style-type: none"> • contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza por 	<p>Par clave-valor, donde Nombre de metadatos de usuario es la clave y Valor de metadatos es el valor.</p> <p>Por ejemplo, para filtrar objetos con metadatos de usuario de <code>color=blue</code>, especifique <code>color</code> Para Nombre de metadatos de usuario, <code>equals</code> para el operador, y. <code>blue</code> Para Valor de metadatos.</p> <p>Nota: Los nombres de metadatos de usuario no son sensibles a mayúsculas/minúsculas; los valores de metadatos de usuario son sensibles a mayúsculas/minúsculas.</p>
Etiqueta de objeto (solo S3)	<ul style="list-style-type: none"> • contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza por 	<p>Par clave-valor, donde Object tag name es la clave y Object tag value es el valor.</p> <p>Por ejemplo, para filtrar objetos que tienen una etiqueta de objeto de <code>Image=True</code>, especifique <code>Image</code> Para Nombre de etiqueta de objeto, <code>equals</code> para el operador, y. <code>True</code> Para Object tag value.</p> <p>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.</p>

Especifique varios tipos y valores de metadatos

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.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: X

Object size	greater than or equal to	10	MB
and	Object size	less than or equal to	100
			MB

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

MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

User metadata camera_type equals Brand A

Add another advanced filter

or Filter group 2 Objects with all of following metadata will be evaluated by this rule:

User metadata camera_type equals Brand B

and Object size less than or equal to 10 MB MB

Add another advanced filter

Paso 2 de 3: Definir colocaciones

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

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.

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

Time period 1 From Day 0 store for 365 days X

Store objects by replicating 1 copies at Site 1 X Edit Delete

and store objects by replicating 1 copies at Site 2 X Edit Delete

[Add other type or location](#)

Time period 2 From Day 365 store forever X

Store objects by erasure coding using 2+1 EC scheme at Site 3 X Edit

[Add other type or location](#)

Pasos

1. Para **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 usar esta opción, las actualizaciones de la hora de último acceso deben estar habilitadas para el cubo S3 o el contenedor Swift. Consulte "Utilice la última hora de acceso en las reglas de ILM" .
Hora de creación definida por el usuario	Hora especificada en los metadatos definidos por el usuario.
Hora no corriente	Se selecciona automáticamente "Hora no corriente" si seleccionó Sí para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores (en bloques S3 con control de versiones activado)? pulg "Paso 1 del asistente Crear una regla de ILM" .



Si desea crear una regla compatible, debe seleccionar **tiempo de ingesta**. Consulte ["Gestione objetos con S3 Object Lock"](#).

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

Por ejemplo, puede especificar dónde almacenar objetos para el primer año (*from día 0 store for 365 days*). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:

- En la lista desplegable **Store objects by**, selecciona **Replicating**.
- 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 el riesgo, realice una o más de las siguientes acciones:

- Aumentar el número de copias durante el período de tiempo.
- Añada copias a otros pools de almacenamiento o a un pool de almacenamiento en cloud.
- Seleccione **código de borrado** en lugar de **Replicating**.

Puede ignorar con toda tranquilidad esta advertencia si esta regla ya crea varias copias para todos los períodos de tiempo.

c. En el campo **Copias en**, seleccione los pools de almacenamiento que desea 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 el grid incluye tres nodos de almacenamiento y selecciona 4 como número de copias, solo se crearán 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 se especifica el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) y otro pool de almacenamiento.

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

a. En la lista desplegable **Almacenar objetos por**, selecciona **código de borrado**.



El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

b. Si no ha agregado un filtro de tamaño de objeto para un valor superior a 200 KB, seleccione **Anterior** para volver al paso 1. Luego, selecciona **Agregar un filtro avanzado** y establece un filtro **Tamaño de objeto** en cualquier valor mayor que 200 KB.

- c. Seleccione el pool de almacenamiento que desea añadir y el esquema de código de borrado que desea usar.

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

5. Opcionalmente:

- Seleccione **Añadir otro tipo o ubicación** para crear copias adicionales en diferentes ubicaciones.
- Seleccione **Añadir otro período** para agregar diferentes períodos de tiempo.



Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que otro período de tiempo termine con **Forever**.

6. Si desea almacenar objetos en un pool de almacenamiento en cloud:

- En la lista desplegable **Store objects by**, selecciona **Replicating**.
- Seleccione el campo **Copias en** y, a continuación, seleccione un Pool de almacenamiento en la nube.

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

- No se puede seleccionar más de un Cloud Storage Pool en una sola instrucción de colocación. De forma similar, no puede seleccionar un Cloud Storage Pool y un pool de almacenamiento en las mismas instrucciones de colocación.
- 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 es posible almacenar más de una copia de objeto 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 a la vez que el objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debe incluir más de una línea en la instrucción de colocación para el período de tiempo, de modo que pueda especificar el número y los tipos de copias para cada ubicación.

7. En el diagrama de retención, confirme las instrucciones de colocación.

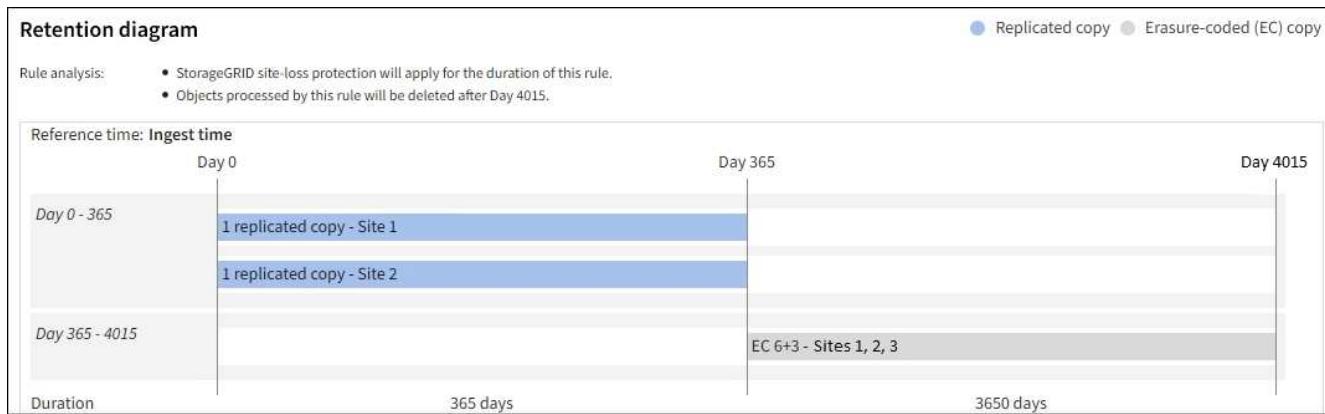
En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y una copia replicada en el sitio 2 durante el primer año. Transcurrido un año y durante 10 años más, se guardará una copia con código de borrado de 6+3 en tres instalaciones. Después de 11 años en total, los objetos se eliminarán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

La sección de análisis de reglas del diagrama de retención indica lo siguiente:

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



Consulte "[Habilite la protección contra pérdida de sitio.](#)"



8. Seleccione **continuar**. ["Paso 3 \(Seleccionar comportamiento de ingesta\)"](#) Se mostrará el asistente Crear una regla de ILM.

Utilice la última hora de acceso en las reglas de ILM

Puede utilizar la última hora de acceso 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 última hora de acceso como filtro avanzado si desea que una regla de ILM se aplique únicamente a los objetos a los que se accedió por última vez en una fecha específica.

Acerca de esta tarea

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

- Cuando se utiliza el último tiempo de acceso como hora de referencia, tenga en cuenta que el cambio de la hora del último acceso de un objeto no desencadena una evaluación inmediata del ciclo de vida de la información útil de la información. 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 último tiempo de acceso y evite ubicaciones que utilicen períodos de tiempo cortos (menos de un mes).

- Al utilizar la última hora de acceso como filtro avanzado o como hora de referencia, debe habilitar las actualizaciones de la última hora de acceso para los bloques S3. Puede utilizar 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 siguiente tabla se resume si se actualiza la hora del último acceso para todos los objetos del depósito para distintos tipos de solicitudes.

Tipo de solicitud	Si se actualiza la hora del último acceso cuando se desactivan las actualizaciones de la última hora de acceso	Si se actualiza la hora del último acceso 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	<ul style="list-style-type: none"> • No, para la copia de origen • Sí, para la copia de destino 	<ul style="list-style-type: none"> • 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

Paso 3 de 3: Seleccione el comportamiento de ingestión

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

Acerca de esta tarea

StorageGRID puede hacer copias provisionales y poner en cola los objetos para 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 ["comportamiento de ingestión"](#) para utilizar.

Para obtener más información, consulte ["Ventajas, desventajas y limitaciones de las opciones de ingestión"](#).

No puede utilizar la opción Equilibrado o Estricto si 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 nube o un nodo de archivado cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia

Consulte ["Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto"](#).

2. Seleccione **Crear**.

Se crea la regla de ILM. La regla no se activa hasta que se agrega a un ["Política de ILM"](#) y esa política se activa.

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

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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "[permisos de acceso específicos](#)".

Acerca de esta tarea

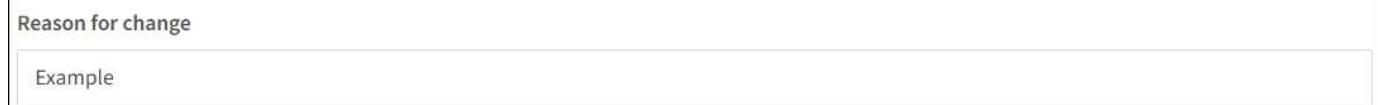
La regla predeterminada es la última regla que se debe evaluar en una política de ILM, por lo que no puede utilizar ningún filtro. Las instrucciones de colocación para la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla de la política.

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



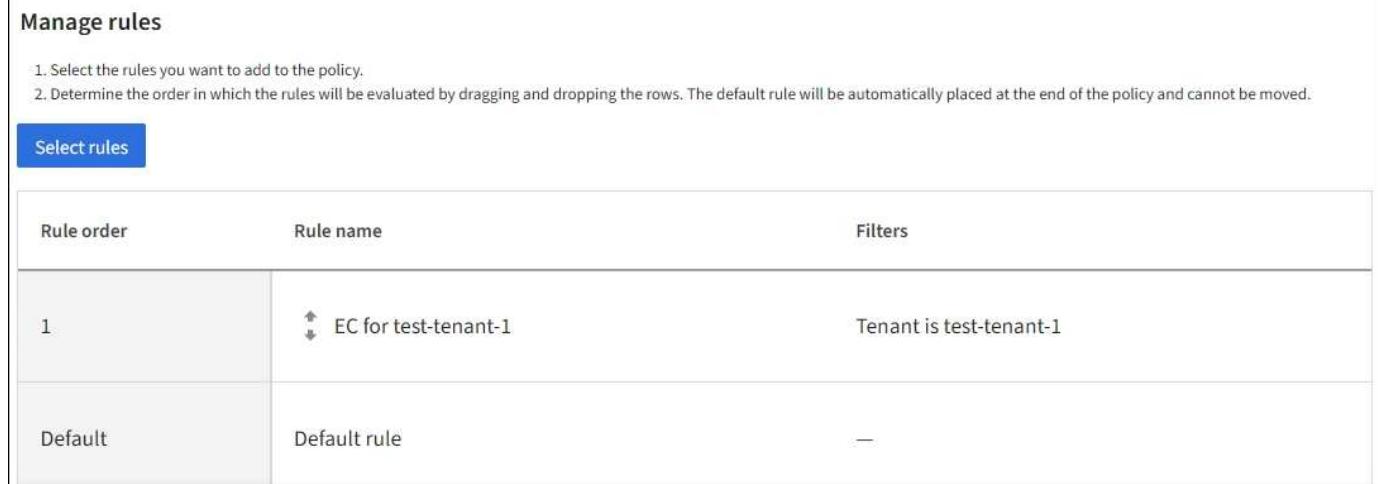
Proposed policy name

Example ILM policy



Reason for change

Example



Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

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

- La regla predeterminada se colocará automáticamente como la última regla cuando la agregue a una política.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones de objetos.
- 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 código de borrado deberían usar un filtro avanzado para evitar que los objetos más pequeños se codifiquen y se borren.

- En general, la regla predeterminada debería retener objetos para siempre.
- Si está utilizando (o planea habilitar) la configuración global S3 Object Lock, la regla predeterminada debe ser compatible.

Pasos

1. Selecciona **ILM > Reglas**.

2. Selecciona **Crear**.

Se muestra el paso 1 (introduzca detalles) del asistente Crear regla de ILM.

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

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

6. Deje la selección desplegable Nombre del cucharón como **Aplica a todos los cubos**.

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

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

La regla predeterminada no puede especificar ningún filtro.

9. Selecciona **Siguiente**.

Aparece el paso 2 (Definir ubicaciones).

10. En Tiempo de referencia, seleccione cualquier opción.

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

11. 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 avanzado **Tamaño de objeto (MB) mayor que 200 KB** para evitar que los objetos más pequeños sean codificados de 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 la nube.
 - 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 ingestión como hora de referencia.
 - Al menos una línea de las instrucciones de colocación debe ser “Para siempre”.

12. Consulte el diagrama de retención para confirmar las instrucciones de colocación.

13. Seleccione **continuar**.

Aparece el paso 3 (Seleccionar comportamiento de ingestión).

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

Gestionar políticas de ILM

Políticas de ILM: Información general

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.

 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.

Política de ILM predeterminada

Al instalar StorageGRID y agregar sitios, se crea automáticamente una política de ILM predeterminada, de la siguiente manera:

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

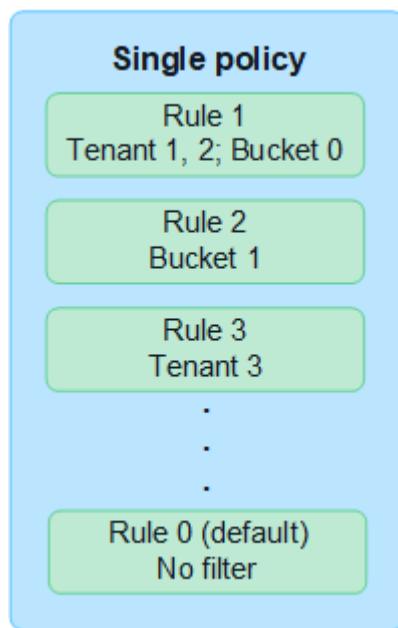
Si la política predeterminada no cumple con sus requisitos de almacenamiento, puede crear sus propias reglas y políticas. Consulte ["Cree una regla de ILM"](#) y.. ["Cree una política de ILM"](#).

¿Una o muchas políticas de ILM activas?

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

Una política

Si su grid utilizará un esquema de protección de datos simple con pocas reglas específicas para inquilinos y bloques, use una única política de ILM activa. Las reglas de ILM pueden contener filtros para gestionar diferentes bloques o inquilinos.



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

Múltiples políticas

Para proporcionar diferentes opciones de calidad de servicio a clientes, se puede tener más de una política activa a la vez. Cada política puede administrar inquilinos específicos, bloques de S3 y objetos. Al aplicar o cambiar una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

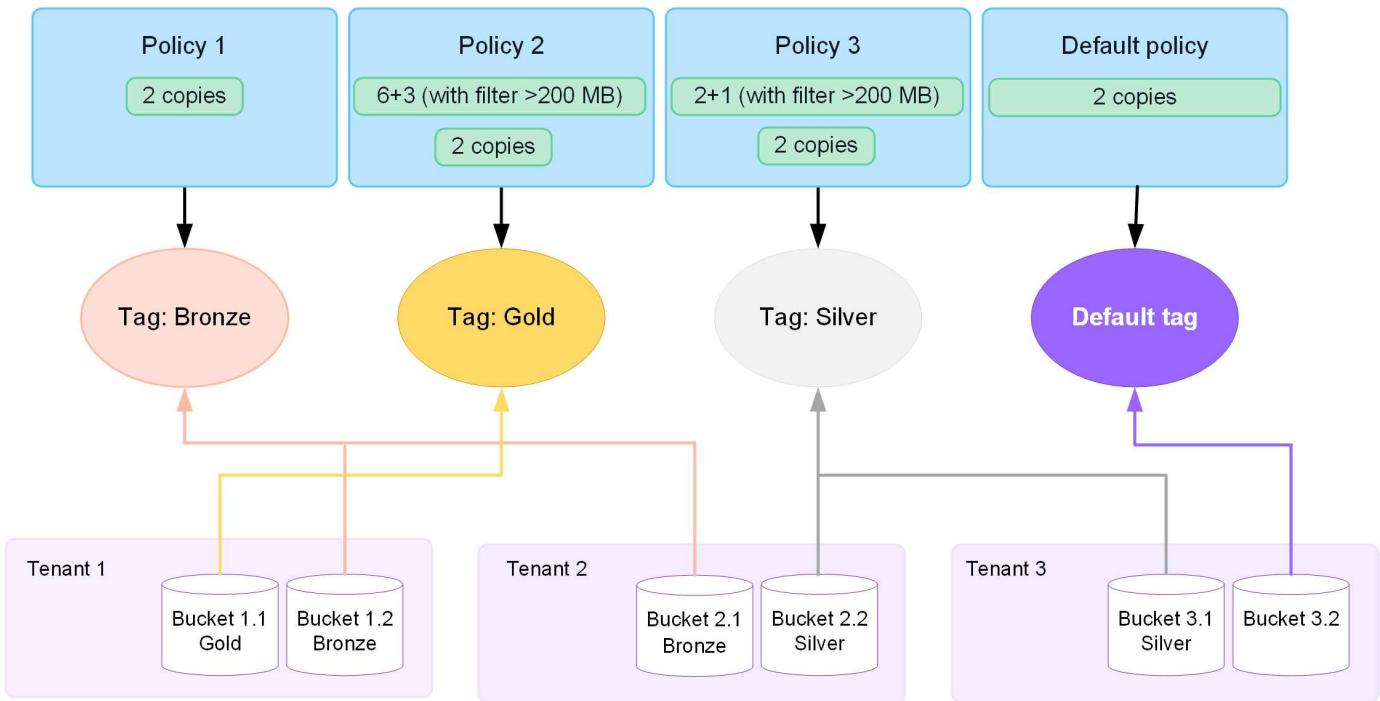
Etiquetas de políticas de ILM

Si desea permitir a los inquilinos cambiar fácilmente entre varias políticas de protección de datos por bloque, use varias políticas de ILM con *ILM policy tags*. Debe asignar cada política de ILM a una etiqueta y, a continuación, los inquilinos etiquetan un bloque para aplicar la política a ese bloque. Solo puede establecer etiquetas de políticas de ILM en bloques de S3.

Por ejemplo, puede tener tres etiquetas llamadas Gold, Silver y Bronze. Puede asignar una política de ILM a cada etiqueta, en función del tiempo y la ubicación en la que esa política almacena objetos. Los inquilinos pueden elegir la política que quieren usar etiquetando sus bloques. Un bloque con la etiqueta Gold se gestiona mediante la política Gold y recibe el nivel Gold de protección de datos y rendimiento.

Etiqueta de política de ILM predeterminada

Una etiqueta de política de ILM predeterminada se crea automáticamente al instalar StorageGRID. Cada cuadrícula debe tener una política activa asignada a la etiqueta predeterminada. La política predeterminada se aplica a todos los objetos de contenedores Swift y a todos los bloques S3 sin etiquetar.



¿Cómo evalúa objetos una política de ILM?

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

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

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se 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 con cada regla subsiguiente de la política hasta que se realiza 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, a todos los cubos S3 o a los contenedores Swift y a todas las versiones de objetos y no puede utilizar ningún filtro avanzado.

Ejemplo de política de ILM

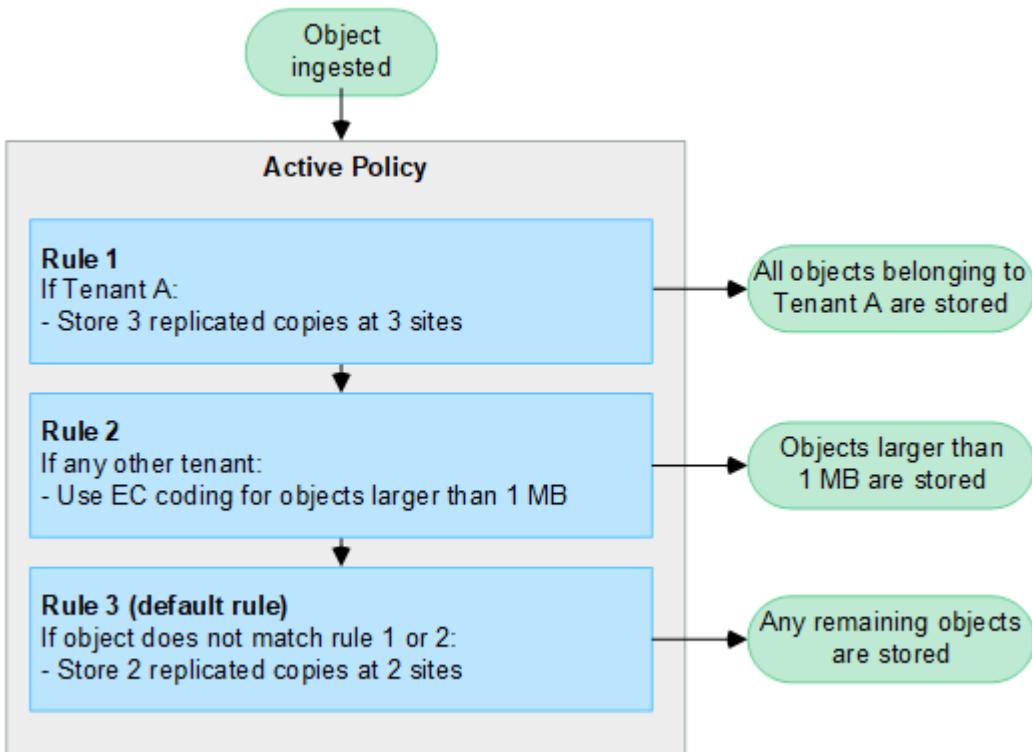
Por ejemplo, una política de ILM podría contener tres reglas de ILM que especifiquen lo siguiente:

- **Regla 1: Copias replicadas para el Inquilino A**
 - Haga coincidir todos los objetos que pertenecen al inquilino A..
 - Almacene estos objetos como tres copias replicadas en tres sitios.
 - Los objetos que pertenecen a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.
- **Regla 2: Codificación de borrado para objetos mayores de 1 MB**
 - Hacer coincidir todos los objetos de otros inquilinos, pero solo si son mayores de 1 MB. Estos objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones.

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

- **Regla 3: 2 copias 2 data centers** (predeterminado)

- Es la última regla y la predeterminada de la política. No utiliza filtros.
- Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenezcan al arrendatario A que tengan 1 MB o menos).



¿Qué son las políticas activas e inactivas?

Cada sistema StorageGRID debe tener al menos una política de ILM activa. Si desea tener más de una política de ILM activa, debe crear etiquetas de políticas de ILM y asignar una política a cada etiqueta. A continuación, los inquilinos aplican las etiquetas a bloques de S3. La política predeterminada se aplica a todos los objetos de los cubos que no tengan una etiqueta de política asignada.

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

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

Si activa más de una política de ILM a la vez, y los inquilinos aplican etiquetas de políticas a bloques de S3, los objetos de cada bloque se gestionarán según la política asignada a la etiqueta.

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

Consideraciones que tener en cuenta para crear una política de ILM

- Utilice únicamente la política proporcionada por el sistema, la política de copias de línea base 2, en los sistemas de prueba. Para StorageGRID 11,6 y versiones anteriores, la regla Crear 2 copias en 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.



El pool de almacenamiento Todos los nodos de almacenamiento se crea automáticamente durante la instalación de StorageGRID 11,6 y versiones anteriores. Si actualiza a una versión posterior de StorageGRID, el pool de Todos los nodos de almacenamiento seguirá existiendo. Si instala StorageGRID 11,7 o una versión posterior como una instalación nueva, no se crea el pool Todos los nodos de almacenamiento.

- 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, ese objeto no será evaluado por ninguna otra regla.
- La última regla de todas las políticas de ILM es la regla de ILM predeterminada, 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.

Crear políticas de ILM

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

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

Tener varias políticas de ILM activas permite aplicar las reglas de ILM adecuadas a inquilinos y bloques específicos para satisfacer múltiples requisitos de calidad de servicio.

Cree una política de ILM

Acerca de esta tarea

Antes de crear su propia política, compruebe que ["Política de ILM predeterminada"](#) no cumple los requisitos de almacenamiento.



Utilice únicamente las políticas proporcionadas por el sistema, la política de 2 copias (para cuadrículas de un sitio) o la copia 1 por sitio (para cuadrículas de varios sitios), en los sistemas de prueba. Para StorageGRID 11,6 y versiones anteriores, la regla predeterminada 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.



Si la "Se ha activado la configuración de bloqueo de objeto global S3", Debe asegurarse de que la política de ILM cumple con los requisitos de los depósitos que tienen S3 Object Lock activado. En esta sección, siga las instrucciones que mencionan tener S3 Object Lock habilitado.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Ya tienes "Reglas de ILM creadas" En función de si el bloqueo de objetos S3 está activado.

S3 Bloqueo de objetos no activado

- Ya tienes "Se han creado las reglas de ILM" desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y, a continuación, editar la política para agregar las nuevas reglas.
- Ya tienes "Se ha creado una regla de ILM predeterminada" que no contiene ningún filtro.

S3 Bloqueo de objetos activado

- La "La configuración de bloqueo de objetos global S3 ya está activada" Para el sistema StorageGRID.
- Ya tienes "Se han creado las reglas de ILM conforme a las normativas y no conformes" desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y, a continuación, editar la política para agregar las nuevas reglas.
- 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 gestión del ciclo de vida de la información en StorageGRID 11,8"



Consulte también "Cree una política de ILM: Información general".

Pasos

1. Seleccione **ILM > políticas**.

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

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

Crear una nueva política

- a. Seleccione **Crear política**.

Clone la política existente

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

Edite la política existente

- a. Si una política está inactiva, puede editarla. Seleccione la casilla de verificación para la política inactiva con la que desea comenzar y, a continuación, seleccione **Editar**.

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

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 usa un filtro, se le solicitará que seleccione una nueva regla predeterminada.
- Si la regla predeterminada no es la última regla, puede mover la regla al final de la nueva política.

S3 Bloqueo de objetos no activado

- a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **ILM rules page**.

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.



No utilice la regla Make 2 copies como regla predeterminada para una política. 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.

S3 Bloqueo de objetos activado

- a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **ILM rules page**.

La lista de reglas contiene solo las reglas que son compatibles y no utilizan ningún filtro.



No utilice la regla Make 2 copies como regla predeterminada para una política. 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.

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

Por ejemplo, es posible que desee utilizar un pool de almacenamiento en la nube para almacenar objetos en depósitos que no tienen S3 Object Lock habilitado.



Sólo puede seleccionar una regla no compatible que no utilice un filtro.

Consulte también "[Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3](#)".

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

La ventana Crear una política muestra ahora las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima.

Si el bloqueo de objetos S3 está activado y también ha seleccionado una regla predeterminada no compatible, dicha regla se agrega como la segunda regla en la política.



Aparece una advertencia si alguna regla no retiene los objetos para siempre. Al activar esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurran las instrucciones de colocación de la regla por defecto (a menos que un ciclo de vida del depósito mantenga los objetos durante un período de tiempo más largo).

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

No puede mover la regla predeterminada. Si el bloqueo de objetos S3 está activado, tampoco puede mover la regla predeterminada no compatible si se ha seleccionado una.



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.

9. Según sea necesario, seleccione **Seleccionar reglas** para agregar o eliminar reglas.
10. Cuando haya terminado, seleccione **Guardar**.
11. Repita estos pasos para crear políticas de ILM adicionales.
12. [Simule una política de gestión de la vida útil](#). Siempre debe simular una política antes de activarla para asegurarse de que funciona como se esperaba.

Simular una política

Simule una política sobre objetos de prueba antes de activar la política y aplicarla a los datos de producción.

Antes de empezar

- Conoce el bloque/clave-objeto de S3 o el contenedor/nombre-objeto Swift para cada objeto que desea probar.

Pasos

1. Use un cliente S3 o Swift o el ["S3 Consola"](#), ingerir los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, seleccione la casilla de verificación de la política y, a continuación, seleccione **Simular**.
3. En el campo **Object**, ingrese el S3 bucket/object-key O el Swift container/object-name para un objeto de prueba. Por ejemplo: bucket-01/filename.png.
4. Si el control de versiones S3 está activado, opcionalmente introduzca un ID de versión para el objeto en el campo **ID de versión**.
5. Seleccione **simular**.
6. En la sección Resultados de Simulation, confirme que la regla correcta coincide con cada objeto.
7. Para determinar qué pool de almacenamiento o perfil de código de borrado está en vigor, seleccione el nombre de la regla coincidente para ir a la página de detalles de regla.



Revise cualquier cambio en la ubicación de los objetos existentes replicados y con código de borrado. 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.

Resultados

Cualquier modificación de las reglas de la política se reflejará en los resultados de Simulation y mostrará la

nueva coincidencia y la anterior. La ventana de política de simulación conserva los objetos que ha probado hasta que seleccione **Borrar todo** o el icono Eliminar  Para cada objeto de la lista de resultados de Simulation.

Información relacionada

["Ejemplo de simulaciones de políticas de ILM"](#)

Activar una política

Cuando se activa una única nueva política de ILM, los objetos existentes y los objetos recién procesados se gestionan con esa política. Al activar varias políticas, las etiquetas de políticas de ILM asignadas a bloques determinan los objetos que se van a gestionar.

Antes de activar una nueva política:

1. Simule la política para confirmar que se comporta como se espera.
2. Revise cualquier cambio en la ubicación de los objetos existentes replicados y con código de borrado. 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.



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

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 implementar una nueva política activa para garantizar que los objetos de cuadrícula no se eliminan accidentalmente. Específicamente:

- Si realiza cambios en las políticas que **aumenten la redundancia o durabilidad de los datos**, esos cambios se implementarán inmediatamente. 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 de política que **podrían disminuir la redundancia o durabilidad de los datos**, esos cambios no se implementarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activa una nueva política que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva política aparecerá en la pestaña Política activa, pero no surtirá efecto hasta que todos los nodos estén en línea y disponibles.

Pasos

Siga los pasos para activar una política o varias políticas:

Active una política

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

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

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

2. En la pestaña Políticas, seleccione la casilla de verificación de la política que desea activar y, a continuación, seleccione **Activar**.

3. Siga el paso apropiado:

- Si un mensaje de advertencia le pide que confirme que desea activar la directiva, seleccione **Aceptar**.
- Si aparece un mensaje de advertencia que contiene detalles sobre la política:
 - i. Revise los detalles para asegurarse de que la política gestionaría los datos según lo esperado.
 - ii. Si la regla predeterminada almacena objetos durante un número limitado de días, revise el diagrama de retención y, a continuación, escriba ese número de días en el cuadro de texto.
 - iii. Si la regla predeterminada almacena objetos para siempre, pero una o más reglas tienen retención limitada, escriba **sí** en el cuadro de texto.
- iv. Seleccione **Activar política**.

Activar varias políticas

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



Cuando hay varias etiquetas en uso, si los inquilinos reasignan frecuentemente las etiquetas de política a los buckets, el rendimiento de los grid puede verse afectado. Si tiene inquilinos que no son de confianza, considere la posibilidad de usar solo la etiqueta predeterminada.

1. Selecciona **ILM > Etiquetas de política**.

2. Seleccione **Crear**.

3. En el cuadro de diálogo Crear etiqueta de política, escriba un nombre de etiqueta y, opcionalmente, una descripción para la etiqueta.



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

4. Seleccione **Crear etiqueta**.

5. En la tabla de etiquetas de políticas de ILM, use el menú desplegable para seleccionar una política y asignarla.

6. Si aparecen advertencias en la columna Limitaciones de política, seleccione **Ver detalles de política** para revisar la política.

7. Asegúrese de que cada política gestionara los datos según lo previsto.
8. Selecciona **Activar políticas asignadas**. O bien, seleccione **Borrar cambios** para eliminar la asignación de la política.
9. En el cuadro de diálogo Activar políticas con nuevas etiquetas, revise las descripciones de cómo gestionarán los objetos cada etiqueta, política y regla. Realice los cambios necesarios para garantizar que las políticas gestionen los objetos según lo esperado.
10. Cuando esté seguro de que desea activar las políticas, escriba **sí** en el cuadro de texto y, a continuación, seleccione **Activar políticas**.

Información relacionada

["Ejemplo 6: Cambiar una política de ILM"](#)

Ejemplo de simulaciones de políticas de ILM

Los ejemplos de simulaciones de políticas de ILM ofrecen directrices para estructurar y modificar simulaciones para su entorno.

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

En este ejemplo se describe cómo verificar reglas al simular una política.

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.

Después de simular la política, confirme que cada objeto ha coincidido con la regla correcta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Object	Version ID	Rule matched	Previous match	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	X
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	X
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	X

En este ejemplo:

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

bucket-a.

- 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.
- 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: Reordenar reglas al simular una política de ILM

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 de dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.

Pasos

1. Despues 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, que muestran la Havok.png El objeto coincide con la regla **PNgs**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNgs	—	X

Sin embargo, Havok.png Estaba destinado a probar la regla **X-MEN**.

3. Para resolver el problema, vuelva a ordenar las reglas.
 - a. Seleccione **Finish** para cerrar la ventana Simulate ILM Policy.
 - 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 coincide muestra que la Havok.png

Ahora Object coincide con la regla de metadatos X-men, según lo esperado. La columna Coincidencia anterior muestra que la regla NGs coincide con el objeto en la simulación anterior.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X

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

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.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

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. Seleccione **Finalizar** para cerrar el diálogo de políticas de simulación. En la página de detalles de la política, seleccione **Diagrama de retención**. A continuación, seleccione **Expandir todo** o **Ver detalles** para cada regla según sea necesario.
2. Revise la cuenta de arrendatario de la regla, el tiempo de referencia y los criterios de filtrado.
- Como ejemplo, supongamos que los metadatos para la regla X-men se ingresaron como “x-men01” en lugar de “x-men”.
3. Para resolver el error, corrija la regla de la siguiente manera:
 - Si la regla forma parte de la política, puede clonar la regla o eliminar la regla de la política y, a continuación, editarla.
 - Si la regla forma parte de la política activa, debe clonar esa regla. No puede editar ni eliminar una regla de la política activa.
4. Vuelva a ejecutar la simulación.

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.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	X

Gestione etiquetas de políticas de ILM

Puede ver detalles de etiqueta de política de ILM, editar una etiqueta o quitar una etiqueta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la ["permisos de acceso requeridos"](#).

Vea los detalles de la etiqueta de la política de ILM

Para ver los detalles de una etiqueta:

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

Editar la etiqueta de política de ILM

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

Para editar la descripción de una etiqueta existente:

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

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

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

Quite la etiqueta de política de ILM

Al eliminar una etiqueta de política, se aplicará la política por defecto a todos los depósitos asignados a esa etiqueta.

Para eliminar una etiqueta:

1. Selecciona **ILM > Etiquetas de política**.
 2. Seccione la casilla de verificación para la etiqueta y luego seleccione * Eliminar *. Se muestra un cuadro de diálogo de confirmación.
- También puede seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta, y puede seleccionar **Eliminar** en esa página.
3. Seccione **Sí** para eliminar la etiqueta.

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.

Antes de empezar

- 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. Seccione **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. Seccione **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:
 - Identificador de objeto (UUID)

- nombre del objeto
- nombre del contenedor
- Tipo de resultado (objeto, marcador de borrado, cubo S3 o contenedor Swift)
- Nombre o ID de cuenta de inquilino
- el tamaño lógico del objeto
- fecha y hora de creación del objeto por primera vez
- fecha y hora de la última modificación del 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 al 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.



La siguiente captura de pantalla es un ejemplo. Los resultados variarán en función de la versión de StorageGRID.

System Metadata

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

Replicated Copies

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

Raw Metadata

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 ORLM puede proporcionarle más información sobre el estado del proceso de evaluación de ILM, pero no puede proporcionar información sobre la corrección de la ubicación de los datos de objetos ni 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 LA API DE REST DE S3"
 - "Use la API DE REST de Swift"

Funciona con políticas de ILM y reglas de ILM

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "[permisos de acceso específicos](#)".

Vea las políticas de ILM

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

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



Si ve los detalles de una política cuyo estado se ha editado o eliminado, aparecerá un mensaje en el que se explica que está viendo la versión de la política que estaba activa para el intervalo de tiempo especificado y que se ha editado o suprimido desde entonces.

Editar una política de ILM

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

Para editar una política:

1. Seleccione **ILM > políticas**.
2. Seleccione la casilla de verificación de la política que desea editar y, a continuación, seleccione **Editar**.
3. Edite la política siguiendo las instrucciones de "[Crear políticas de ILM](#)".
4. Simule la política antes de volver a activarla.



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.

Clonar una política de ILM

Para clonar una política de ILM:

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

3. Cree una nueva política que empiece por la política que ha clonado siguiendo las instrucciones de ["Crear políticas de ILM"](#).



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.

Quitar una política de ILM

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

1. Seleccione **ILM > políticas**.
2. Seleccione la casilla de verificación para la política inactiva que desea eliminar.
3. Seleccione **Quitar**.

Vea los detalles de las reglas de ILM

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

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

2 copies 2 data centers

Compliant: No
Ingest behavior: Strict
Reference time: Noncurrent time

[Clone](#) [Edit](#) [Remove](#)

[Rule detail](#) [Used in policies](#)

Time period and placements

[Retention diagram](#) [Placement instructions](#)

Sort placements by [Time period](#) [Storage pool](#)

● Replicated copy ● Erasure-coded (EC) copy

Rule analysis: • Objects processed by this rule will not be deleted by ILM.

Reference time: Noncurrent time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Data Center 1

EC 2+1 - Data Center 1

Duration

Forever

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

Clonar una regla de ILM

Puede clonar una regla existente si desea crear una nueva regla que utilice algunos de los valores de la regla existente. Si necesita editar una regla que se utiliza en cualquier política, clone la regla en su lugar y realice cambios en el clon. Después de realizar cambios en el clon, puede eliminar la regla original de la política y sustituirla por la versión modificada según sea necesario.



No puede clonar una regla de gestión de la vida útil de la información si se creó con StorageGRID versión 10,2 o anterior.

Pasos

1. Selecciona **ILM > Reglas**.
2. Seleccione la casilla de verificación para la regla que desea clonar y luego seleccione **Clonar**. Como alternativa, seleccione el nombre de la regla y, a continuación, seleccione **Clonar** en la página de detalles de la regla.
3. Actualice la regla clonada siguiendo los pasos para [Editar una regla de ILM](#) y.. ["Usar filtros avanzados en reglas de ILM"](#).

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

Editar una regla de ILM

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

No puede editar una regla si se utiliza en alguna política de ILM. En cambio, puedes hacerlo [clonar la regla](#) y realice los cambios necesarios en la copia clonada.



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.

Pasos

1. Selecciona **ILM > Reglas**.
2. Confirme que la regla que desea editar no se utiliza en ninguna política de ILM.
3. Si la regla que desea editar no está en uso, seleccione la casilla de verificación de la regla y seleccione * Acciones * > * Editar . **Alternativamente, seleccione el nombre de la regla y luego seleccione *Editar** en la página de detalles de la regla.
4. Complete los pasos del asistente Edit ILM Rule. Según sea necesario, siga los pasos de ["Creación de una regla de ILM"](#) y.. ["Usar filtros avanzados en reglas de ILM"](#).

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

Quite una regla de ILM

Para que la lista de reglas de ILM actuales sea gestionable, elimine las reglas de ILM que probablemente no use.

Pasos

Para eliminar una regla de ILM utilizada actualmente en una política activa:

1. Clone la política.
2. Quite la regla de ILM del clon de políticas.
3. Guarde, simule y active la nueva directiva para asegurarse de que los objetos están protegidos como se espera.
4. Vaya a los pasos para eliminar una regla de ILM utilizada actualmente en una política inactiva.

Para eliminar una regla de ILM utilizada actualmente en una política inactiva:

1. Seleccione la política inactiva.
2. Quite la regla de ILM de la política o. [elimine la política](#).
3. Vaya a los pasos para eliminar una regla de ILM que no está en uso actualmente.

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

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

Ver las métricas de ILM

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

Pasos

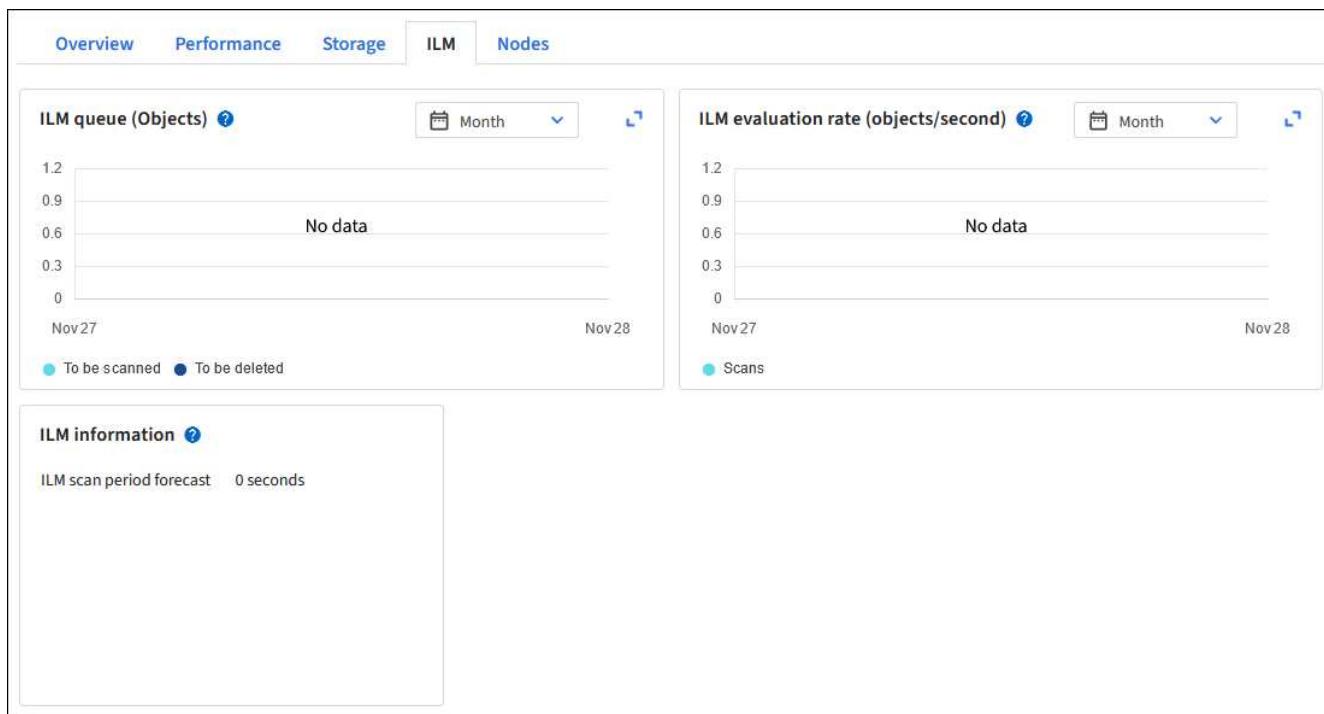
1. Selecciona **Dashboard > ILM**.



Como la consola se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervise las métricas en la pestaña ILM.

Puede seleccionar el signo de interrogación Para ver una descripción de los elementos en la pestaña ILM.



Utilice el bloqueo de objetos de S3

Gestione objetos con S3 Object Lock

Como administrador de grid, puede habilitar el bloqueo de objetos de S3 GB en su sistema StorageGRID e implementar una política de gestión del ciclo de vida de la información conforme a la normativa para garantizar que los objetos de bloques de S3 específicos no se eliminan ni se sobrescriban durante un período de tiempo determinado.

¿Qué es el bloqueo de objetos de S3?

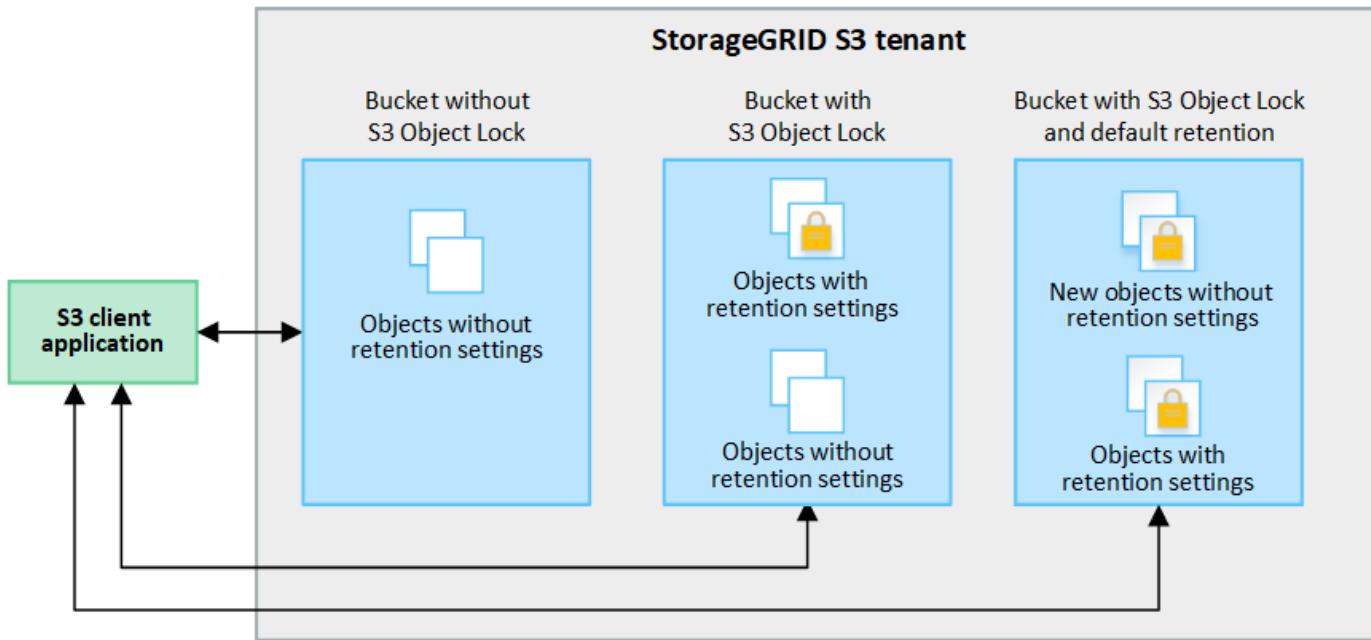
La función StorageGRID S3 Object Lock es una solución de protección de objetos equivalente a S3 Object Lock en Amazon simple Storage Service (Amazon S3).

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 bucket tiene S3 Object Lock habilitado, se requiere el control de versiones de bucket y se habilita automáticamente.

Si un bucket tiene S3 Object Lock habilitado, las aplicaciones cliente S3 pueden especificar, de manera opcional, la configuración de retención para cualquier versión de objeto guardada en ese bucket.

Además, un bloque que tiene S3 Object Lock habilitado puede tener opcionalmente un modo de retención y un período de retención predeterminados. La configuración predeterminada se aplica solo a los objetos que se agregan al depósito sin su propia configuración de retención.

StorageGRID with S3 Object Lock setting enabled



Modos de retención

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

- En modo de cumplimiento:
 - El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.
 - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
 - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
- En modo de gobierno:
 - Los usuarios con permiso especial pueden utilizar un encabezado de omisión en las solicitudes para modificar ciertos valores de retención.
 - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden utilizar la aplicación cliente S3 para especificar opcionalmente los siguientes valores de retención para cada objeto que se agregue al depósito:

- **Modo de retención:** Ya sea cumplimiento o gobierno.
- **Retain-until-date:** Si la fecha de retención de una versión de objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **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.



Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener más información sobre la configuración del objeto, consulte ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#).

Valor de retención predeterminado para los depósitos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden especificar opcionalmente los siguientes ajustes predeterminados para el bloque:

- **Modo de retención predeterminado:** Ya sea cumplimiento o gobierno.
- **Período de retención predeterminado:** Cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este depósito, a partir del día en que se agregan.

La configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención. Los objetos de cubo existentes no se ven afectados al agregar o cambiar estos valores predeterminados.

Consulte ["Cree un bloque de S3"](#) y ["Actualizar S3 Retención predeterminada de bloqueo de objetos"](#).

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 Bloqueo de objetos de S3 cumple con los requisitos de Amazon S3, deja en obsoletos la característica de cumplimiento de normativas de StorageGRID, que ahora se conoce como "Cumplimiento de normativas heredado".

La configuración de cumplimiento global está anticuada. Si ha habilitado esta configuración con una versión anterior de StorageGRID, la configuración Bloqueo de objetos S3 se activa automáticamente. Puede seguir usando StorageGRID para gestionar la configuración de los buckets compatibles existentes; sin embargo, no puede crear nuevos buckets compatibles. Para obtener más información, consulte ["Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"](#).

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.

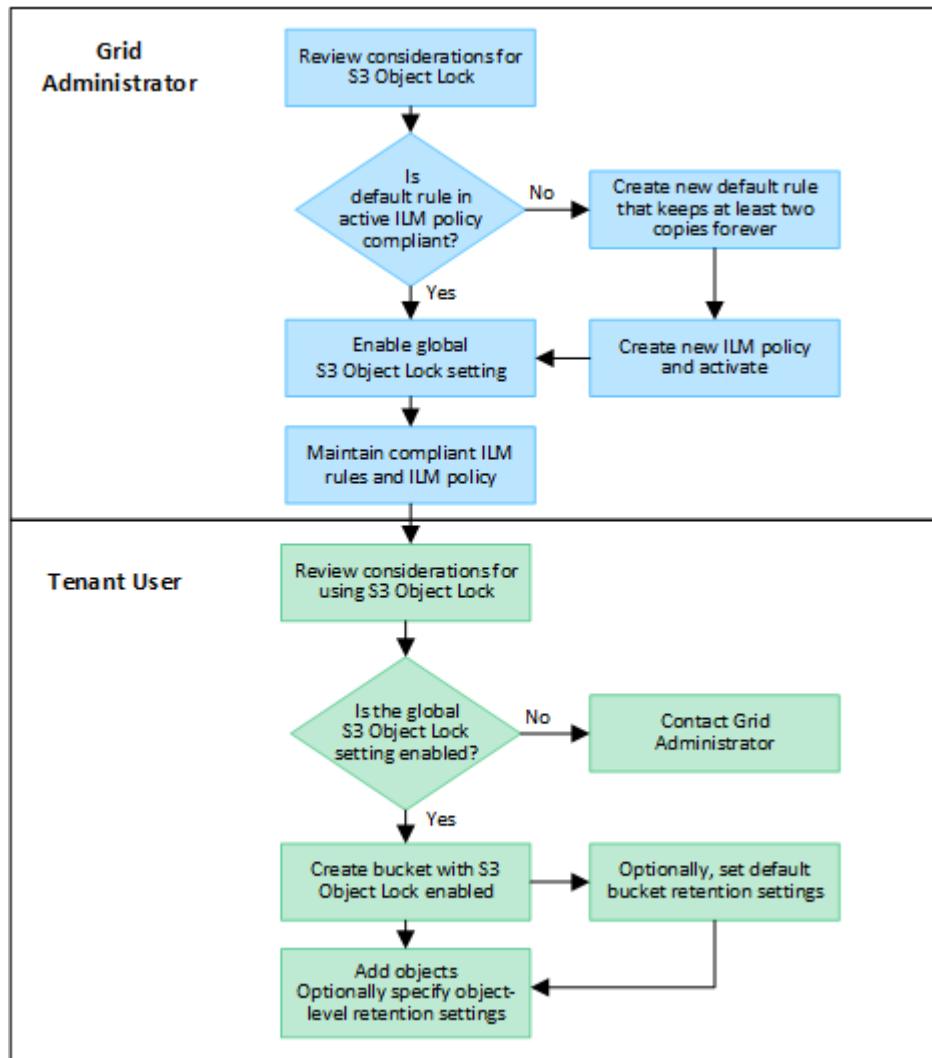
	Bloqueo de objetos de S3	Cumplimiento (heredado)
¿Cómo se habilita la función a nivel global?	En Grid Manager, seleccione CONFIGURACIÓN > sistema > S3 Object Lock .	Ya no es compatible.
¿Cómo se habilita la función para un bloque?	Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo bloque con el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST de S3.	Ya no es compatible.

	Bloqueo de objetos de S3	Cumplimiento (heredado)
¿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
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención hasta la fecha para cada versión de objeto, o pueden establecer un período de retención predeterminado para cada bloque.	Los usuarios deben establecer un período de retención para todo el segmento. El período de retención se aplica a todos los objetos del bloque.
¿Se puede cambiar el período de retención?	<ul style="list-style-type: none"> En el modo de cumplimiento de normativas, se puede aumentar la fecha de retención de una versión de objeto, pero nunca disminuir. En el modo de gobierno, los usuarios con permisos especiales pueden disminuir o incluso eliminar la configuración de retención de un objeto. 	El período de retención de un depósito se puede aumentar, pero nunca disminuir.
¿Dónde se controla la 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?	<ul style="list-style-type: none"> En el modo de cumplimiento, se puede suprimir una versión de objeto después de alcanzar la fecha de retención hasta la fecha, asumiendo que el objeto no está bajo conservación legal. En el modo de gobierno, los usuarios con permisos especiales pueden eliminar un objeto antes de alcanzar su fecha de retención, asumiendo que el objeto no está bajo retención 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 compatible y haga que rija la regla predeterminada en una 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. Opcionalmente, especifique la configuración de retención predeterminada para el bloque. Cualquier configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención.
3. Agregue objetos a esos bloques y, opcionalmente, especifique los períodos de retención a nivel de objeto y la configuración de retención legal.
4. Según sea necesario, actualice la retención predeterminada del depósito o actualice el período de retención o la configuración de retención legal para un objeto individual.

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 S3 Object Lock, no puede desactivar la configuración.
- No puede activar el bloqueo de objetos S3 global a menos que la regla predeterminada en todas las políticas de ILM activas sea *compliant* (es decir, la regla predeterminada debe cumplir con los requisitos de los bloques con bloqueo de objetos S3 habilitado).
- Cuando se habilita la configuración global S3 Object Lock, no se puede crear una nueva política de ILM ni activar una política de ILM existente a menos que la regla predeterminada de la política sea compatible. Una vez habilitada la configuración global S3 Object Lock, las reglas de ILM y las páginas de políticas de ILM indican qué reglas de ILM cumplen.

Requisitos para las reglas de ILM que cumplen con las normativas

Si desea habilitar la configuración global Bloqueo de objetos S3, debe asegurarse de que la regla predeterminada de todas las políticas de ILM activas 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 la nube.
- 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 ingestión** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación debe ser “Para siempre”.

Requisitos para las políticas de ILM

Cuando se habilita la configuración global Bloqueo de objetos S3, las políticas de ILM activas e inactivas pueden incluir reglas que cumplen y no cumplen.

- La regla predeterminada de una política de ILM activa o inactiva debe cumplir.
- Las reglas no compatibles solo se aplican a objetos de los depósitos que no tienen activado el bloqueo de objetos S3 o que no tienen activada la función de cumplimiento de normativas 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 los depósitos que no tienen activado el bloqueo de objetos S3 o el cumplimiento de normativas heredado porque almacena una sola 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.
- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No puede activar el bloqueo de objetos S3 para un depósito existente.
- Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque. No puede desactivar el bloqueo de objetos de S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención y un período de retención predeterminados para cada bloque mediante el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST S3. La configuración de retención predeterminada del depósito se aplica solo a los nuevos objetos agregados al depósito que no tienen su propia configuración de retención. Puede anular esta configuración predeterminada especificando un modo de retención y Retain-until-date para cada versión del objeto cuando se cargue.
- Se admite la configuración de ciclo de vida de bloques para los bloques con S3 Object Lock habilitado.
- 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, puede especificar la configuración de retención predeterminada para el bloque, o bien puede especificar la configuración de retención para cada versión de objeto. La configuración de retención a nivel de objeto se puede especificar mediante la aplicación cliente S3 o la API DE REST S3.

- 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 depósito con S3 Object Lock habilitado pasa por las siguientes etapas:

1. Procesamiento de objetos

Cuando se agrega una versión de objeto al depósito que tiene S3 Object Lock habilitado, la configuración de retención se aplica de la siguiente manera:

- Si se especifica la configuración de retención para el objeto, se aplica la configuración de nivel de objeto. Se ignoran todos los valores predeterminados de los depósitos.
- Si no se especifica ninguna configuración de retención para el objeto, se aplica la configuración de bloque predeterminada, si existe.
- Si no se especifica ninguna configuración de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

Si se aplica una configuración de retención, tanto el objeto como cualquier metadatos definidos por el usuario S3 se protegen.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. El número y el tipo exactos de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas conformes a la normativa de las políticas de ILM activas. Si se puede eliminar un objeto protegido antes de alcanzar su fecha de retención hasta la fecha, depende de su modo de retención.

- Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Información relacionada

- ["Cree un bloque de S3"](#)
- ["Actualizar S3 Retención predeterminada de bloqueo de objetos"](#)
- ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)
- ["Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos 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.

Antes de empezar

- Usted tiene la ["Permiso de 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 comprende las consideraciones.
- Ha confirmado que la regla predeterminada de la política de ILM activa cumple con las normativas. Consulte "[Cree una regla de ILM predeterminada](#)" para obtener más detalles.

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 habilitada esta configuración, no se puede desactivar.



La configuración de cumplimiento global está anticuada. Si ha habilitado esta configuración con una versión anterior de StorageGRID, la configuración Bloqueo de objetos S3 se activa automáticamente. Puede seguir usando StorageGRID para gestionar la configuración de los buckets compatibles existentes; sin embargo, no puede crear nuevos buckets compatibles. Para obtener más información, 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.

2. Seleccione **Activar el bloqueo de objetos S3**.

3. Seleccione **aplicar**.

Aparece un cuadro de diálogo de confirmación que le recuerda que no puede desactivar el bloqueo de objetos S3 después de que esté habilitado.

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, S3 Object Lock ahora está habilitado para toda la cuadrícula y no se puede deshabilitar.
- Si la regla predeterminada no es compatible, aparece un error. Debe crear y activar una nueva política de ILM que incluya una regla de cumplimiento como regla predeterminada. Seleccione **OK**. A continuación, cree una nueva política, simule y actívela. Consulte "[Cree una política de ILM](#)" si desea obtener instrucciones.

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 porque no hay disponibles un sitio de centro de datos o varios nodos de almacenamiento, devuelve un error:

```
503: Service Unavailable  
Unable to update compliance settings because the settings can't be  
consistently applied on enough storage services. Contact your grid  
administrator for assistance.
```

Para resolver este error, siga estos pasos:

1. 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 LA API DE REST DE 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 política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Regla ILM 1 Por ejemplo 1: Copiar datos de objetos en dos sitios

Este ejemplo de regla ILM copia datos de objetos en pools de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Pools de almacenamiento in situ	Dos pools de almacenamiento, cada uno de los cuales contiene sitios diferentes, denominados Sitio 1 y Sitio 2.
Nombre de regla	Dos copias Dos sitios

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingestión
Ubicaciones	En el día 0 hasta siempre, conserve una copia replicada en el sitio 1 y una copia replicada en el sitio 2.

La sección de análisis de reglas del diagrama de retención indica lo siguiente:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- ILM no eliminará los objetos procesados por esta regla.

The screenshot shows the StorageGRID rule configuration interface. At the top, it says "Reference time" with a dropdown set to "Ingest time". Below this is the "Time period and placements" section, which includes a "Sort by start date" button. It contains two time period definitions: "Time period 1" (From Day 0 to forever) and "Store objects by replicating 1 copies at Site 1" and "and store objects by replicating 1 copies at Site 2". There is also an "Add other type or location" link. Below this is an "Add another time period" link. The "Retention diagram" section shows a timeline from "Day 0 - forever" to "Duration" and "Forever". It displays two horizontal bars: "1 replicated copy - Site 1" and "1 replicated copy - Site 2", both extending from Day 0 to Forever. A legend indicates that blue represents "Replicated copy". Rule analysis details are listed as follows:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Regla de ILM 2 Por ejemplo 1: Perfil de código de borrado con coincidencia de bloques

En esta regla de ILM de ejemplo se 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
Pool de almacenamiento con múltiples sitios	<ul style="list-style-type: none"> • Un pool de almacenamiento en tres sitios (sitios 1, 2, 3) • Utilice un esquema de codificación de borrado de 6+3
Nombre de regla	S3 registros financieros del bloque

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingestión
Ubicaciones	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.

Time period and placements Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store forever

Store objects by erasure coding using 6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Duration

Forever

Política de ILM, por ejemplo 1

En la práctica, la mayoría de las políticas de ILM son sencillas, a pesar de que el sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas.

Una política de ILM típica para un grid de varios sitios podría incluir reglas de ILM como las siguientes:

- Durante la ingestión, almacene todos los objetos que pertenecen al bloque de S3 denominado `finance-records` en un pool de almacenamiento que contiene tres sitios. Use el código de borrado `6+3`.
- Si un objeto no coincide con la primera regla de ILM, utilice la regla de ILM predeterminada de la política, dos copias dos centros de datos, para almacenar una copia de ese objeto en el sitio 1 y una copia en el sitio 2.

Información relacionada

- ["Políticas de ILM: Información general"](#)
- ["Crear políticas de ILM"](#)

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 política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

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 use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Definición de regla	Valor de ejemplo
Nombre de regla	Objetos sólo EC > 1 MB
Tiempo de referencia	Tiempo de ingestión
Filtro avanzado para Tamaño de objeto	Tamaño de objeto superior a 1 MB
Ubicaciones	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones

Filter group 1 Objects with all of following metadata will be evaluated by this rule: X

Object size	greater than	1	MB	X
-------------	--------------	---	----	---

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 ingestión
Filtro avanzado para Tamaño de objeto	Ninguno
Ubicaciones	En el día 0 hasta siempre, conserve una copia replicada en el sitio 1 y una copia replicada en el sitio 2.

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 para asegurarse de que las imágenes de más de 1 MB tengan un código de borrado y que dos copias estén hechas 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 política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

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 use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Definición de regla	Valor de ejemplo
Nombre de regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingestión
Filtro avanzado para Tamaño de objeto	Tamaño de objeto superior a 1 MB
Filtros avanzados para Clave	<ul style="list-style-type: none">Termina en .jpgTermina en .png
Ubicaciones	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

Object size greater than 1 MB

and Key ends with .jpg

or Filter group 2 Objects with all of following metadata will be evaluated by this rule:

Object size greater than 1 MB

and Key ends with .png

Debido a que esta regla se configura como la primera regla de la directiva, la instrucción de colocación de codificación de borrado solo se aplica a los archivos .jpg y .png que sean mayores de 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 ingestión
Filtros avanzados para Clave	<ul style="list-style-type: none"> Termina en .jpg Termina en .png
Ubicaciones	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 bucket de S3 con el control de versiones habilitado, puede gestionar las versiones de objetos no corrientes incluyendo reglas en su política de ILM que utilicen la

hora no corriente como tiempo de referencia.



Si especifica un tiempo de retención limitado para los objetos, esos objetos se suprimirán permanentemente después de alcanzar el período de tiempo. Asegúrese de comprender cuánto tiempo se retendrán los objetos.

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 política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.



Para realizar la simulación de política de ILM en una versión no actual de un objeto, debe conocer el UUID o CBID de la versión del objeto. Para encontrar el UUID y CBID, utilice "[búsqueda de metadatos de objetos](#)" mientras el objeto sigue siendo actual.

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 sitios 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 compuesto por diferentes centros de datos, denominados Sitio 1, Sitio 2 y Sitio 3.
Nombre de regla	Tres copias diez años
Tiempo de referencia	Tiempo de ingestión
Ubicaciones	El día 0, conserve tres copias replicadas durante 10 años (3.652 días), una en el sitio 1, una en el sitio 2 y otra en el sitio 3. 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.

Para crear una regla que utilice el tiempo no corriente como tiempo de referencia, seleccione **Sí** para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores (en bloques S3 con control de versiones activado)? En el paso 1 (introduzca detalles) del asistente Create an ILM Rule. Cuando selecciona **Sí**, *Tiempo no corriente* se selecciona automáticamente para el tiempo de referencia y no puede seleccionar un tiempo de

referencia diferente.

1 Enter details — 2 Define placements — 3 Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts [?](#) Select tenant accounts

Bucket name [?](#) matches all [▼](#)

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? [?](#)

No Yes

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 diferentes centros de datos, Sitio 1 y Sitio 2.
Nombre de regla	Versiones no corrientes: Dos copias dos años
Tiempo de referencia	Hora no corriente Seleccionado automáticamente cuando selecciona Sí para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores (en cubos S3 con control de versiones activado)? En el asistente Create an ILM Rule.
Ubicaciones	El día 0 relativo a 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 del objeto no corriente durante 2 años (730 días), una en el sitio 1 y otra en el sitio 2. 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 distinta a la versión actual, las reglas que utilizan una hora no corriente como tiempo de referencia deben aparecer en la política de ILM antes de las reglas que se aplican a la versión del objeto actual.

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 hora no corriente deben aparecer en la política antes de las reglas que se aplican a la versión del objeto actual. De lo contrario, las versiones del objeto no corriente nunca coincidirán con la regla de hora no corriente.

- Al ingerir, cree tres copias replicadas y almacene una copia en cada uno de tres sitios. 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).
- La versión actual del objeto coincidiría con la segunda regla. Cuando la versión actual del objeto se ha almacenado durante 10 años, el proceso de ILM añade un marcador de eliminación como la versión actual del objeto y hace que la versión del objeto anterior sea «no actual». La próxima vez que se produzca una evaluación de ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en el sitio 3 se purga y las dos copias en el sitio 1 y el sitio 2 se almacenan durante 2 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 política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Información relacionada

- ["Opciones de procesamiento"](#)
- ["Create ILM rule: Seleccione el comportamiento de 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
Filtro avanzado	La restricción de ubicación es igual a eu-west-3
Pools de almacenamiento	Sitio 1 (París)
Nombre de regla	Ingesta estricta para garantizar el centro de datos París
Tiempo de referencia	Tiempo de ingestión
Ubicaciones	El día 0, mantenga dos copias replicadas para siempre en el sitio 1 (París)
Comportamiento de ingestión	Estricto. Utilice siempre las colocaciones de esta regla durante el procesamiento. La ingestión falla si no es posible almacenar dos copias del objeto en el centro de datos de París.

Strict ingest to guarantee Paris data center

Compliant: Yes

Used in active policy: No

Used in proposed policy: No

Ingest behavior: Strict

Reference time: Ingest time

[Clone](#) [Edit](#) [Remove](#)

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

[Retention diagram](#) [Placement instructions](#)

Sort placements by [Time period](#) [Storage pool](#) Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: **Ingest time** Ingest behavior: **Strict**

Day 0	Day 0 - forever	2 replicated copies - Site 1	Forever
Duration			

Regla 2 de ILM, por ejemplo 5: Ingesta equilibrada de otros objetos

Esta regla de ILM de ejemplo utiliza el comportamiento de ingestión 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 cumplir 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
Filtro avanzado	<i>No especificado</i>
Pools de almacenamiento	Sitio 1 (París) y Sitio 2 (EE.UU.)
Nombre de regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingestión
Ubicaciones	Desde el día 0, mantenga dos copias replicadas para siempre en dos centros de datos
Comportamiento de ingestión	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. Realice copias provisionales en cualquier ubicación disponible si la instrucción de colocación no se puede satisfacer.

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 ingestión falla.

- Todos los demás objetos coinciden con la segunda regla, incluidos los objetos que pertenecen al arrendatario de París y que no tienen la región del 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

Si es necesario cambiar su protección de datos o añadir nuevos sitios, puede crear y activar una nueva política de ILM.

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 agregado un nuevo sitio StorageGRID en una ampliación y se debe implementar una nueva política de gestión del ciclo de vida de la información activa para almacenar los datos en el nuevo sitio. Para implementar una nueva política activa, primero ["crear una política"](#). Después, debes hacerlo ["simular"](#) y después ["activar"](#) la nueva política.

 Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Cómo el cambio de una política de ILM afecta al rendimiento

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.

Para garantizar que una nueva política de ILM no afecte a la ubicación de los objetos existentes replicados y codificados de borrado, puede hacerlo ["Cree una regla de ILM con un filtro de tiempo de ingestión"](#). Por ejemplo, **tiempo de ingestión es el o posterior <date and time>**, de modo que la nueva regla se aplica solo a los objetos ingeridos en o después de la fecha y hora especificadas.

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 código de borrado diferente a los objetos existentes con código de borrado.

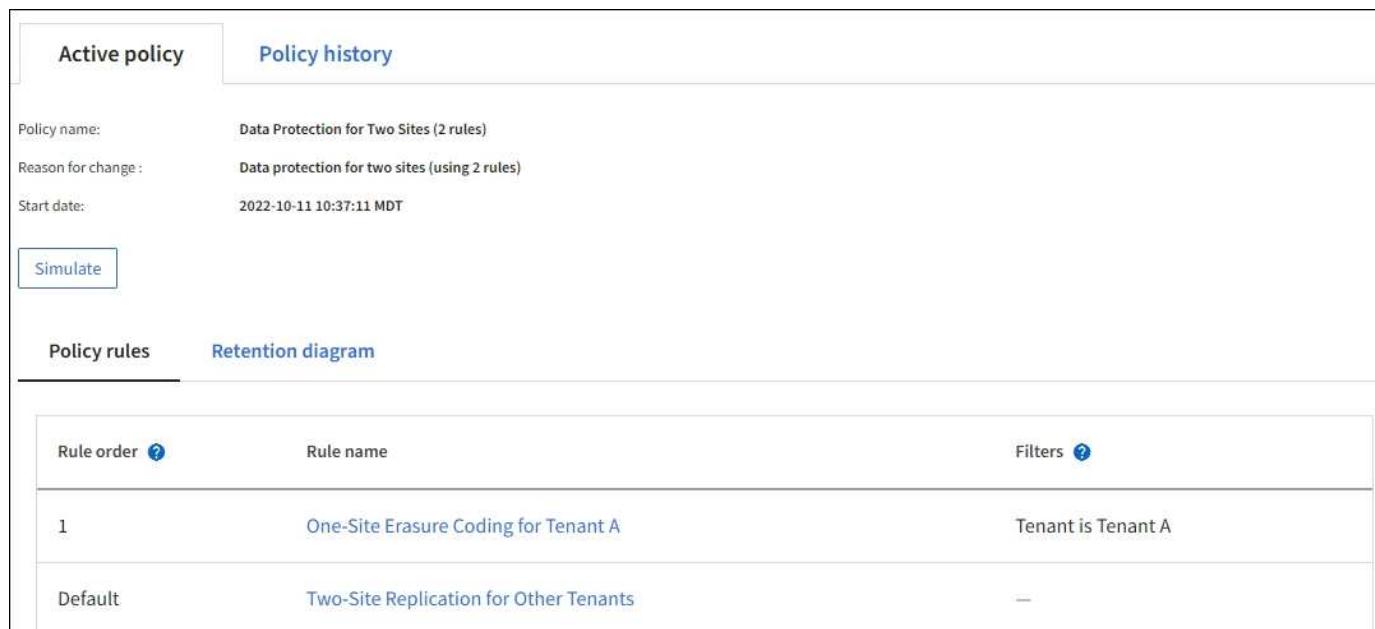


StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

- 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.

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.



The screenshot shows the 'Active policy' tab selected in the top navigation bar. Below it, the 'Policy history' tab is visible. The policy details are as follows:

- Policy name: Data Protection for Two Sites (2 rules)
- Reason for change: Data protection for two sites (using 2 rules)
- Start date: 2022-10-11 10:37:11 MDT

Below the details is a 'Simulate' button. The 'Policy rules' tab is selected, showing the following rules:

Rule order	Rule name	Filters
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

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.

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	Inquilino A
Pool de almacenamiento	Sitio 1
Ubicaciones	Código de borrado 2+1 en el Sitio 1 desde el día 0 hasta 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	Sitio 1 y sitio 2

Definición de regla	Valor de ejemplo
Ubicaciones	Dos copias replicadas desde el día 0 hasta siempre: Una copia en el sitio 1 y una copia en el sitio 2.

Política de ILM por ejemplo 6: Protección de datos en tres sitios

En este ejemplo, la política de ILM se está reemplazando por una nueva política para un sistema StorageGRID de tres sitios.

Después de realizar una expansión para agregar el nuevo sitio, el administrador de grid creó dos nuevos pools de almacenamiento: Un pool de almacenamiento para el sitio 3 y un pool de almacenamiento que contiene los tres sitios (no el mismo que el pool de almacenamiento predeterminado de todos los nodos de almacenamiento). A continuación, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM, que ha sido diseñada para proteger los datos de 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	Todos los sitios 3 (incluye el sitio 1, el sitio 2 y el sitio 3)
Ubicaciones	Código de borrado 2+1 en todos los sitios 3 desde el día 0 hasta 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	Sitio 1, Sitio 2 y Sitio 3
Ubicaciones	Tres copias replicadas desde el día 0 hasta siempre: Una copia en el sitio 1, una copia en el sitio 2 y una copia en el sitio 3.

Activar la política de ILM por ejemplo 6

Al activar una nueva política de ILM, los objetos existentes se pueden mover a ubicaciones nuevas o se

pueden crear copias de objetos nuevas para los objetos existentes, según las instrucciones de ubicación de cualquier regla nueva o actualizada.



Los errores de una 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 actualmente activa en este ejemplo, los objetos que pertenecen al inquilino A se protegen con el código de borrado 2+1 en el sitio 1. En la nueva política de ILM, los objetos pertenecientes al inquilino A se protegerán con el código de borrado 2+1 en los sitios 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. Entonces, cada uno de los tres fragmentos se almacena en un sitio 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 con código de borrado totalmente nuevos en los tres sitios.



Los fragmentos 2+1 existentes en el Sitio 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

Qué ocurre cuando cambian las instrucciones de replicación

En la política de ILM actualmente activa en este ejemplo, los objetos que pertenecen a otros inquilinos se protegen usando dos copias replicadas en los pools de almacenamiento de los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenezcan a otros clientes se protegerán usando tres copias replicadas en pools de almacenamiento de los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Cuando cualquier inquilino que no sea el inquilino A procesa un objeto nuevo, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Como las copias de objetos existentes en el Sitio 1 y el Sitio 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 sitio 3.

Impacto en el rendimiento de la activación de esta política

Cuando se activa la política de ILM en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles superiores a los normales de recursos de grid para crear

nuevos fragmentos con código de borrado para los objetos existentes del inquilino A y nuevas copias replicadas en el sitio 3 para los objetos existentes de otros inquilinos.

Como resultado del cambio 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 utilizar el filtro avanzado de tiempo de procesamiento en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de procesamiento en 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 bloqueo 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 política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

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
<code>retain-until-date</code>	<p>“2030-12-30T23:59:59Z” (30 de diciembre de 2030)</p> <p>Cada versión de objeto tiene su propia <code>retain-until-date</code> ajuste. Este ajuste se puede aumentar, pero no disminuir.</p>
<code>legal hold</code>	<p>APAGADO (no vigente)</p> <p>Se puede colocar o levantar una retención legal en cualquier versión del objeto en cualquier momento durante el período de retención. Si un objeto está sujeto a una conservación legal, dicho objeto no se puede eliminar ni siquiera si el <code>retain-until-date</code> se ha alcanzado.</p>

Regla de ILM 1 para S3 Object Lock Ejemplo: Perfil de codificación 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 código de borrado para almacenar el objeto en los nodos de almacenamiento en tres sitios de centros de datos mediante un perfil de código de borrado 6+3. Esta regla satisface los requisitos de los buckets con S3 Object Lock activado: Se mantiene una copia en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando el tiempo de ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla compatible: Objetos EC en el depósito de registros bancarios - Banco de ABC
Cuenta de inquilino	Banco de ABC
Nombre del bloque	<code>bank-records</code>
Filtro avanzado	<p>Tamaño de objeto (MB) mayor que 1</p> <p>Nota: este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menores.</p>

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 almacenar para siempre

Definición de regla	Valor de ejemplo
Perfil de código de borrado	<ul style="list-style-type: none"> 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: Use Cloud Storage Pool
Cuentas de inquilino	No especificado
Nombre del bloque	No se especifica, pero solo se aplica a los depósitos que no tienen S3 Object Lock (o la función de cumplimiento de normativas heredada) activada.
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingestión
Ubicaciones	<ul style="list-style-type: none"> 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

Definición de regla	Valor de ejemplo
Cuenta de inquilino	No especificado
Nombre del bloque	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingestión
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 política.

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.

Simule la política

Después de agregar reglas a la política, elegir una regla compatible predeterminada y organizar las demás reglas, debe simular la política probando objetos del depósito con S3 Object Lock activado y desde otros depósitos. 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.

Ejemplo 8: Prioridades para el ciclo de vida del bloque de S3 y política de ILM

Según la configuración del ciclo de vida, los objetos siguen los ajustes de retención del ciclo de vida de bloques de S3 o una política de ILM.

Ejemplo de ciclo de vida del bloque que tiene prioridad sobre la política de ILM

Política de ILM

- Regla basada en referencia de tiempo no corriente: En el día 0, mantenga X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminado): En el día 0, mantenga X copias durante 50 días

Ciclo de vida del cucharón

- Filter: {Prefix: "docs/"}, Expiration: Days: 100, NoncurrentVersionExpiration: Days: 5

Resultado

- Se ingiere un objeto denominado «docs/text». Coincide con el filtro de ciclo de vida del cucharón del prefijo «docs/».
 - Transcurridos 100 días, se crea un marcador de borrado y los documentos/texto dejan de ser actuales.
 - Transcurridos 5 días, se elimina el término «docs/text» durante un total de 105 días desde la ingesta.
- Se ingiere un objeto llamado «vídeo/película». No coincide con el filtro y utiliza la política de retención de ILM.
 - Despues de 50 días, se crea un marcador de borrado y el mensaje «vídeo o película» deja de ser actual.
 - Transcurridos 20 días, se eliminará el «vídeo/película» durante un total de 70 días desde la ingesta.

Ejemplo de ciclo de vida del segmento que se mantiene implícitamente para siempre

Política de ILM

- Regla basada en referencia de tiempo no corriente: En el día 0, mantenga X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminado): En el día 0, mantenga X copias durante 50 días

Ciclo de vida del cucharón

- Filter: {Prefix: "docs/"}, Expiration: ExpiredObjectDeleteMarker: true

Resultado

- Se ingiere un objeto denominado «docs/text». Coincide con el filtro de ciclo de vida del cucharón del prefijo «docs/».

La `Expiration` la acción solo se aplica a los marcadores de borrado caducados, lo que implica mantener todo lo demás para siempre (empezando por «docs/»).

Los marcadores de borrado que comienzan con «docs/» se eliminan cuando caducan.

- Se ingiere un objeto llamado «vídeo/película». No coincide con el filtro y utiliza la política de retención de ILM.
 - Después de 50 días, se crea un marcador de borrado y el mensaje «vídeo o película» deja de ser actual.
 - Transcurridos 20 días, se eliminará el «vídeo/película» durante un total de 70 días desde la ingesta.

Ejemplo de uso del ciclo de vida de bloque para duplicar ILM y borrar los marcadores de eliminación vencidos

Política de ILM

- Regla basada en referencia de tiempo no corriente: En el día 0, mantenga X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminado): En el día 0, mantenga X copias durante 50 días

Ciclo de vida del cucharón

- `Filter: {}, Expiration: Days: 50, NoncurrentVersionExpiration: Days: 20`

Resultado

- La política de ILM se duplica en el ciclo de vida del bloque.
- Se ha ingerido un objeto. Ningún filtro significa que el ciclo de vida del bloque se aplica a todos los objetos y anula la configuración de retención de ILM.
 - Después de 50 días, se crea un marcador de borrado y el objeto pasa a ser no actual.
 - Una vez transcurridos 20 días, un total de 70 días desde la ingesta, el objeto no actual se elimina y el marcador de borrado pasa a caducar.
 - Transcurridos 30 días, un total de 100 días desde la ingesta, se elimina el marcador de borrado caducado.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.