Gestión de bloques de S3

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Gestión de bloques de S3

Si usa un inquilino de S3 con los permisos adecuados, puede crear, ver y eliminar bloques de S3, actualizar la configuración de nivel de coherencia, configurar el uso compartido de recursos de origen cruzado (CORS), habilitar y deshabilitar las opciones de actualización del tiempo de acceso anterior y gestionar servicios de plataforma de S3.

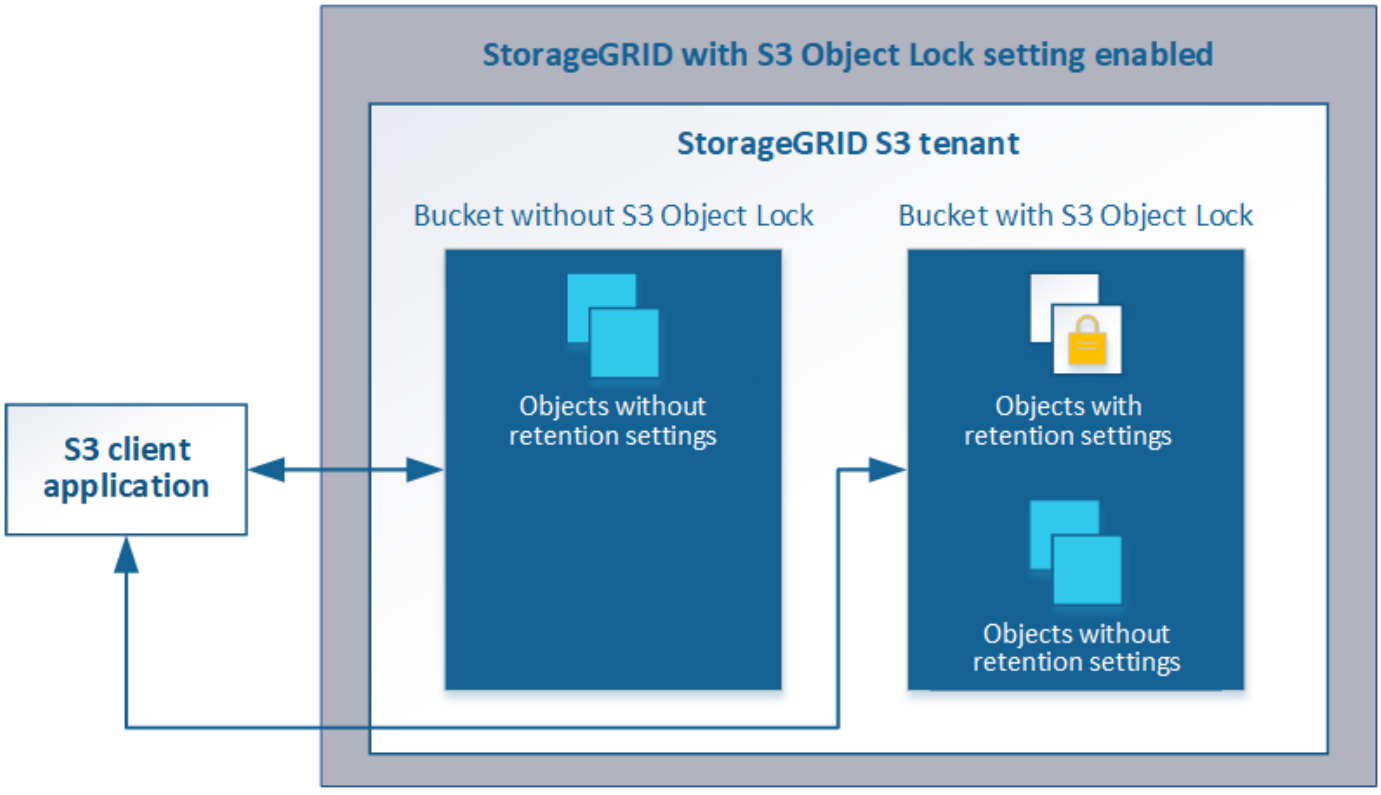
Uso del bloqueo de objetos de S3

Puede usar la función de bloqueo de objetos S3 en StorageGRID si los objetos deben cumplir los requisitos normativos de retención.

¿Qué es el bloqueo de objetos de S3?

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

Tal y como se muestra en la figura, cuando se habilita la opción global de bloqueo de objetos de S3 para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear bloques con o sin la función de bloqueo de objetos de S3 habilitada. Si un bloque tiene habilitada la función S3 Object Lock, las aplicaciones cliente S3 pueden especificar, opcionalmente, la configuración de retención para cualquier versión del objeto en ese bloque. Una versión de objeto debe tener la configuración de retención especificada para estar protegida por S3 Object Lock.



La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de

retención o eliminar objetos protegidos.

Si un bloque tiene habilitado el bloqueo de objetos S3, la aplicación cliente S3 puede especificar, de manera opcional, la siguiente configuración de retención a nivel de objeto al crear o actualizar un objeto:

- **Retener-hasta-fecha**: Si la fecha retener-hasta-fecha de una versión de objeto es en el futuro, el objeto puede ser recuperado, pero no puede ser modificado o eliminado. Según sea necesario, se puede aumentar la fecha de retención hasta de un objeto, pero esta fecha no se puede disminuir.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente. La retención legal es independiente de la retención hasta la fecha.

Para obtener información detallada sobre estos ajustes, vaya a "'uso del bloqueo de objetos S3'" en "Operaciones y limitaciones compatibles con la API REST de S3".

Gestión de bloques que cumplen con las normativas heredadas

La función de bloqueo de objetos S3 sustituye la función Compliance disponible en versiones anteriores de StorageGRID. Si ha creado cubos compatibles con una versión anterior de StorageGRID, puede seguir gestionando la configuración de estos bloques; sin embargo, ya no puede crear nuevos bloques compatibles. Para obtener instrucciones, consulte el artículo de la base de conocimientos de NetApp.

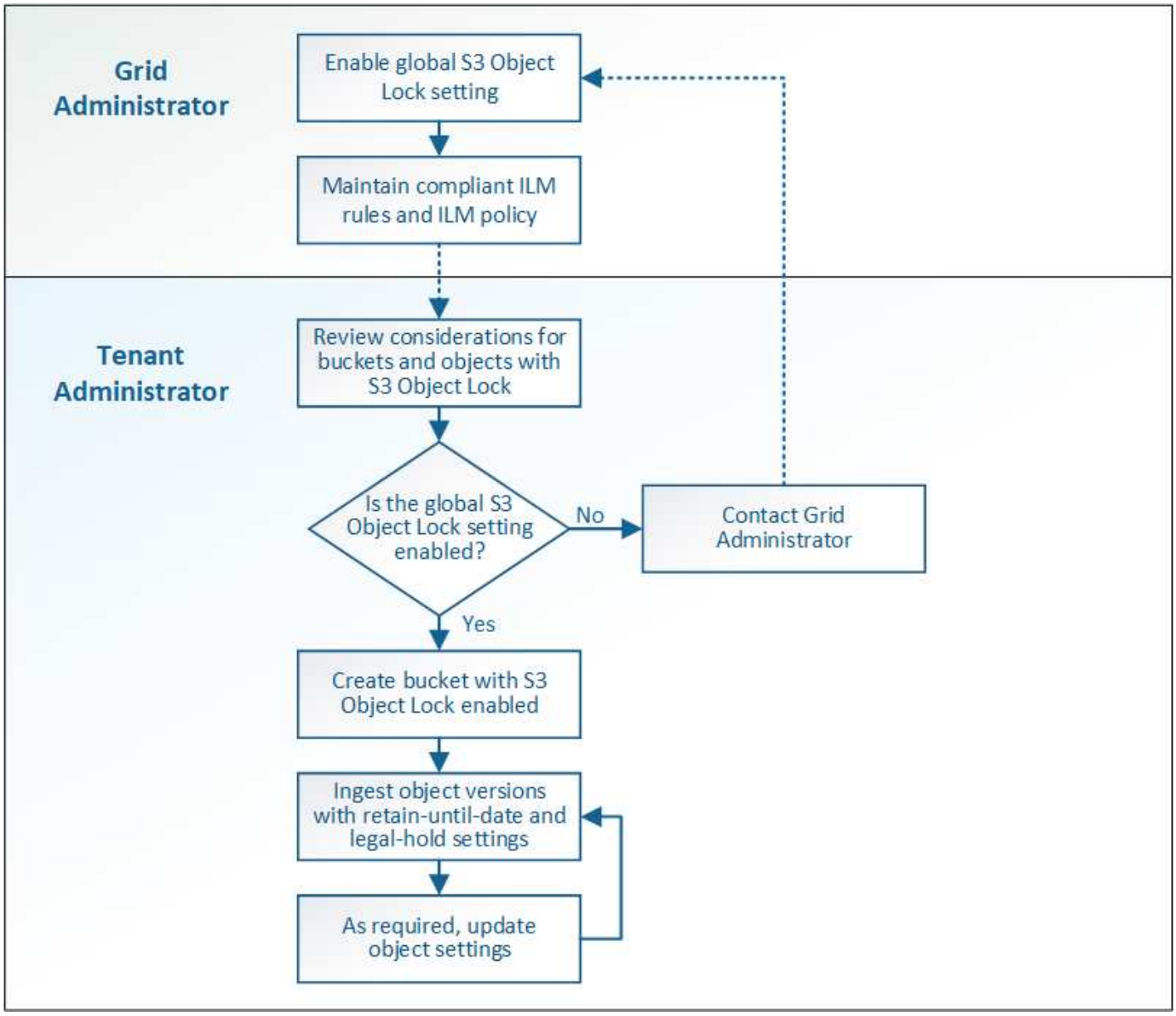
"Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Flujo de trabajo de bloqueo de objetos de S3

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar la función de bloqueo de objetos de S3 en StorageGRID.

Para poder crear bloques con el bloqueo de objetos S3 habilitado, el administrador de grid debe habilitar el valor global de bloqueo de objetos S3 para todo el sistema StorageGRID. El administrador del grid también debe asegurarse de que la política de gestión del ciclo de vida de la información (ILM) sea « conforme»; debe cumplir los requisitos de los bloques con la función S3 Object Lock habilitada. Para obtener más información, póngase en contacto con el administrador de grid o consulte las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Una vez que se habilita la opción global de bloqueo de objetos S3, se pueden crear bloques con el bloqueo de objetos S3 habilitado. Posteriormente, puede usar la aplicación cliente S3 para especificar opcionalmente la configuración de retención para cada versión del objeto.



Información relacionada

"Gestión de objetos con ILM"

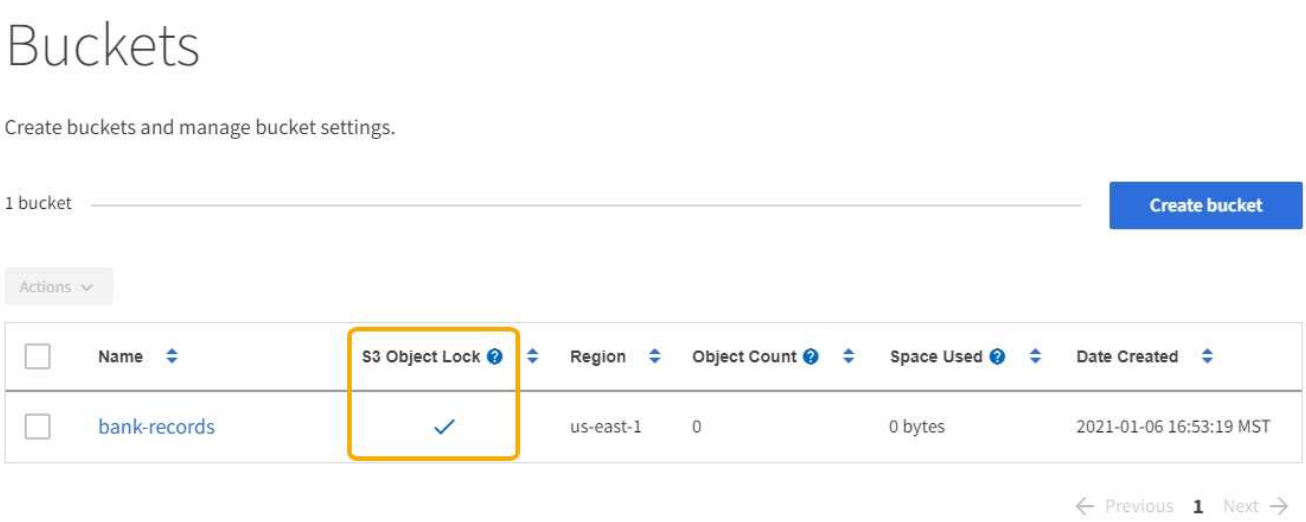
Requisitos para el bloqueo de objetos de S3

Antes de habilitar S3 Object Lock para un bloque, revise los requisitos para los bloques y objetos de S3 Object Lock y el ciclo de vida de los objetos en bloques con S3 Object Lock habilitado.

Requisitos para bloques con bloqueo de objetos de S3 habilitado

- Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede usar el administrador de inquilinos, la API de gestión de inquilinos o la API REST de S3 para crear bloques con el bloqueo de objetos S3 habilitado.

  Este ejemplo del Administrador de inquilinos muestra un bloque con el bloqueo de objetos S3 habilitado.



- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No es posible habilitar el bloqueo de objetos de S3 para un bloque existente.
- Se requiere el versionado de bloques con S3 Object Lock. Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque.
- Después de crear un bloque con el bloqueo de objetos S3 habilitado, no se puede deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones de ese bloque.
- Un bloque StorageGRID con el bloqueo de objetos S3 habilitado no tiene un período de retención predeterminado. En su lugar, la aplicación cliente S3 puede especificar opcionalmente una fecha de retención y una configuración de conservación legal para cada versión del objeto que se agrega a ese bloque.
- Se admite la configuración del ciclo de vida de bloques para los bloques del ciclo de vida de objetos S3.
- La replicación de CloudMirror no es compatible para bloques con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en bloques con S3 Object Lock habilitado

- La aplicación cliente S3 debe especificar la configuración de retención de cada objeto que tenga que protegerse mediante el bloqueo de objetos S3.
- Puede aumentar la fecha de retención hasta una versión de objeto, pero nunca puede disminuir este valor.
- Si recibe una notificación de una acción legal pendiente o una investigación normativa, puede conservar la información relevante colocando una retención legal en una versión del objeto. Cuando una versión de objeto se encuentra bajo una retención legal, ese objeto no se puede eliminar de StorageGRID, aunque haya alcanzado su fecha de retención. Tan pronto como se levante la retención legal, la versión del objeto se puede eliminar si se ha alcanzado la fecha de retención.
- El bloqueo de objetos de S3 requiere el uso de bloques con versiones. La configuración de retención se aplica a versiones individuales de objetos. Una versión de objeto puede tener una configuración de retención hasta fecha y una retención legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta fecha o de retención legal para un objeto, sólo se protege la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en bloques con S3 Object Lock habilitado

Cada objeto que se guarda en un bloque con el bloqueo de objetos S3 habilitado atraviesa tres etapas:

1. **Procesamiento de objetos**

- Al añadir una versión de objeto a un bloque con el bloqueo de objetos S3 habilitado, la aplicación cliente S3 puede especificar, de manera opcional, la configuración de retención del objeto (retener hasta la fecha, la conservación legal o ambos). A continuación, StorageGRID genera metadatos para ese objeto, que incluye un identificador de objeto (UUID) único y la fecha y la hora de procesamiento.
- Después de procesar una versión de objeto con configuración de retención, sus datos y los metadatos definidos por el usuario de S3 no se pueden modificar.
- StorageGRID almacena los metadatos del objeto de forma independiente de los datos del objeto. Mantiene tres copias de todos los metadatos de objetos en cada sitio.

2. **Retención de objetos**
   - StorageGRID almacena varias copias del objeto. El número y el tipo exactos de copias y las ubicaciones del almacenamiento se determinan según las reglas conformes de la política de ILM activa.
3. **Eliminación de objetos**
   - Un objeto se puede eliminar cuando se alcanza su fecha de retención.
   - No se puede eliminar un objeto que se encuentra bajo una retención legal.

Crear un bloque de S3

Puede usar el administrador de inquilinos para crear bloques S3 para los datos de objetos. Al crear un bloque, debe especificar el nombre y la región del bloque. Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, de manera opcional, puede habilitar el bloqueo de objetos S3 para el bloque.

Lo que necesitará

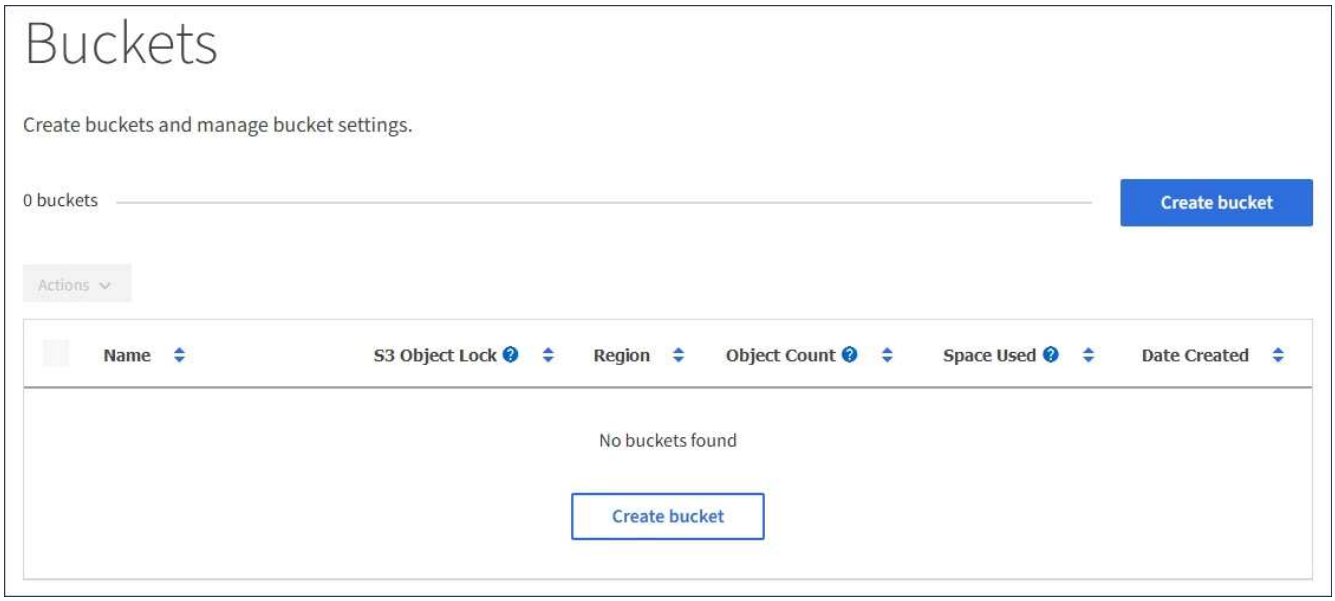
- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Si planea crear un bloque con bloqueo de objetos S3, la configuración global de bloqueo de objetos S3 debe haber estado habilitada para el sistema StorageGRID y debe haber revisado los requisitos para los bloques y objetos de bloqueo de objetos S3.

  "Uso del bloqueo de objetos de S3"

Pasos

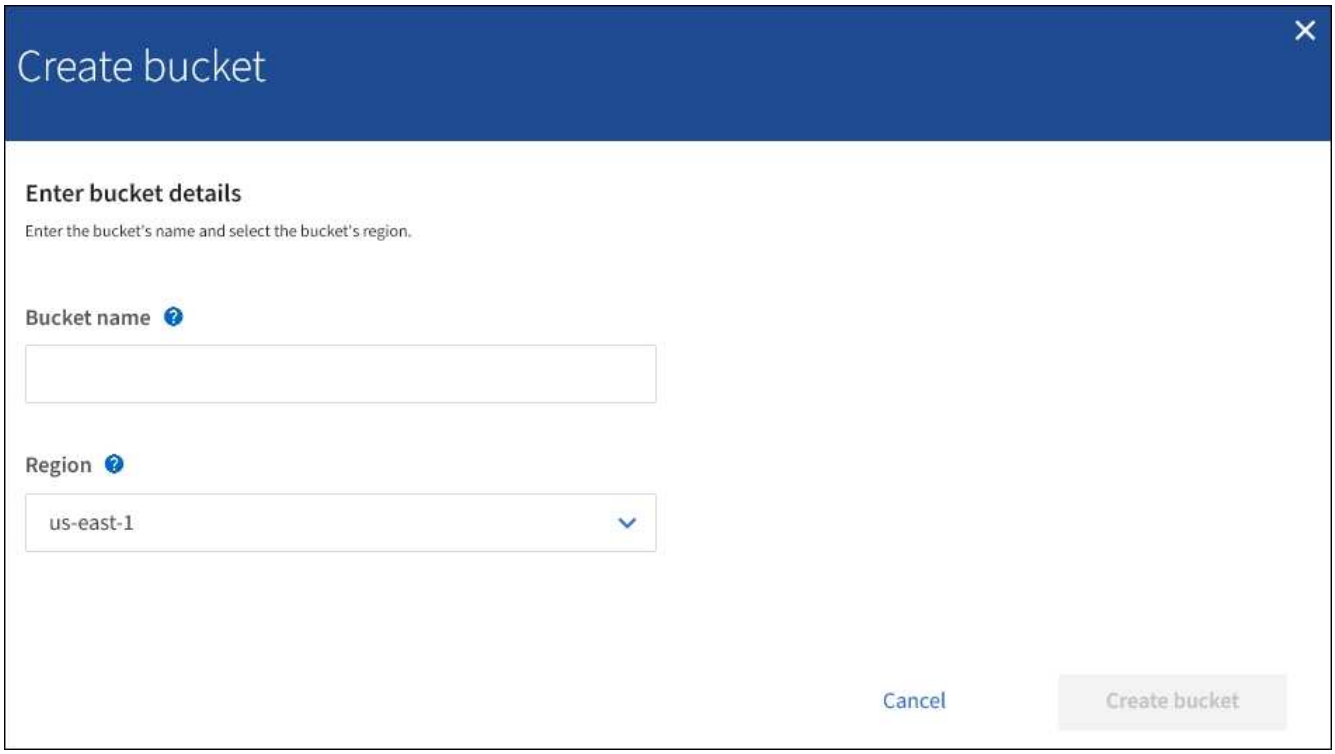
1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

   Aparece la página Cuchos y muestra todos los cestillos que ya se han creado.



2. Seleccione **Crear cucharón**.

   Se mostrará el asistente Create bucket.



> Si la opción de configuración global de bloqueo de objetos S3 está habilitada, Create bucket incluye un segundo paso para la gestión del bloqueo de objetos S3 para el bloque.

3. Introduzca un nombre único para el bloque.

> No se puede cambiar el nombre del bloque después de crear el bloque.

Los nombres de los bloques deben cumplir con las siguientes reglas:

- Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino).
- Debe ser compatible con DNS.
- Debe incluir al menos 3 y no más de 63 caracteres.
- Puede ser una serie de una o más etiquetas, con etiquetas adyacentes separadas por un punto. Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones.
- No debe ser una dirección IP con formato de texto.
- No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor.

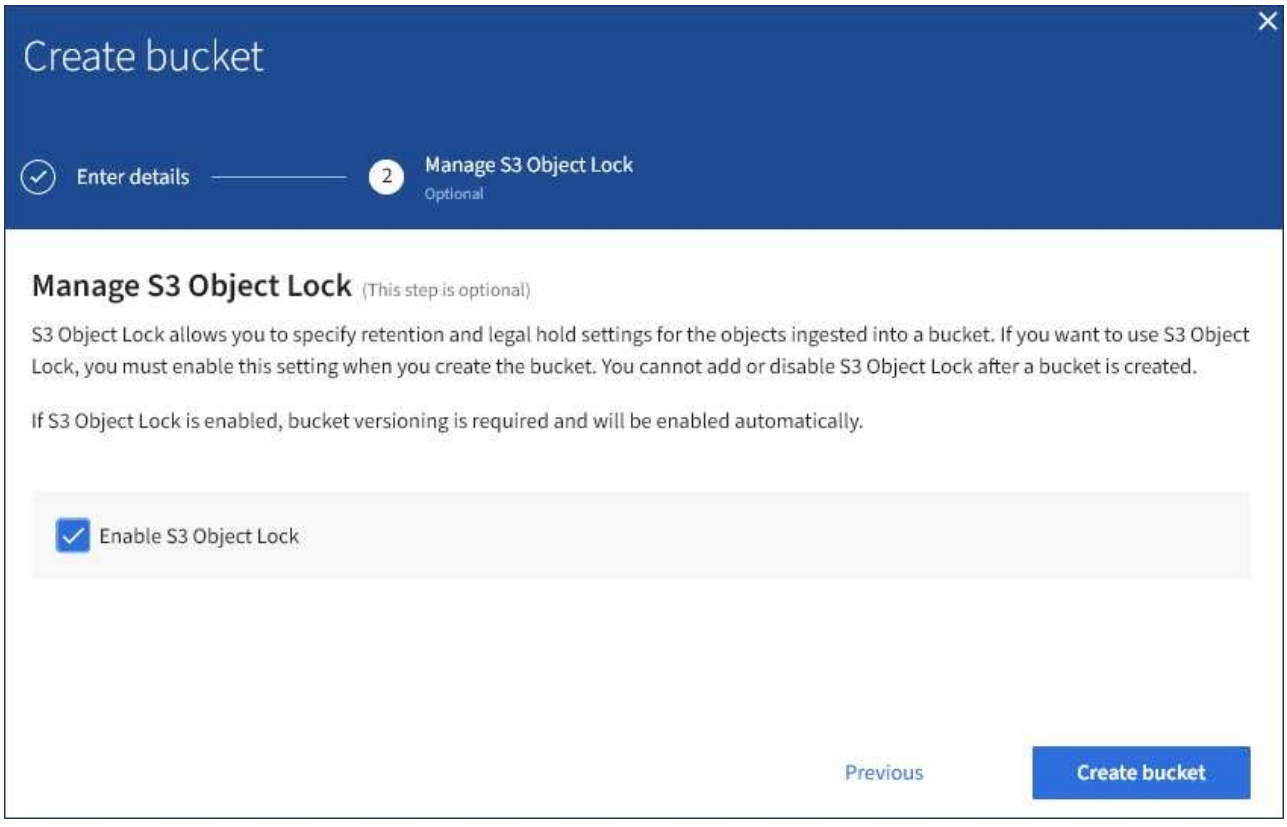
> Para obtener más información, consulte la documentación de Amazon Web Services (AWS).

4. Seleccione la región para este segmento.

   El administrador de StorageGRID gestiona las regiones disponibles. La región de un bloque puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los bloques se crean en la `us-east-1` región.

> No se puede cambiar la región después de crear el bloque.

5. Seleccione **Crear cucharón** o **continuar**.
   - Si el valor global de bloqueo de objetos S3 no está habilitado, seleccione **Crear bloque**. El cucharón se crea y se agrega a la tabla de la página Cuches.
   - Si el valor global de bloqueo de objetos S3 está activado, seleccione **continuar**. Paso 2, se muestra Manage S3 Object Lock.



6. De manera opcional, seleccione la casilla de comprobación para habilitar S3 Object Lock para este bloque.

   El bloqueo de objetos S3 debe estar habilitado para el bloque antes de que una aplicación cliente S3 pueda especificar la configuración de retención legal y hasta la fecha para los objetos agregados al bloque.

   > No se puede habilitar o deshabilitar S3 Object Lock después de crear el bloque.

   > Si habilita S3 Object Lock para un bloque, el control de versiones de bloques se habilita automáticamente.

7. Seleccione **Crear cucharón**.

   El cucharón se crea y se agrega a la tabla de la página Cuches.

Información relacionada

"Gestión de objetos con ILM"

"API de gestión de inquilinos"

"Use S3"

Ver los detalles de bloques de S3

Puede ver una lista de las configuraciones de bloques y bloques en su cuenta de inquilino.

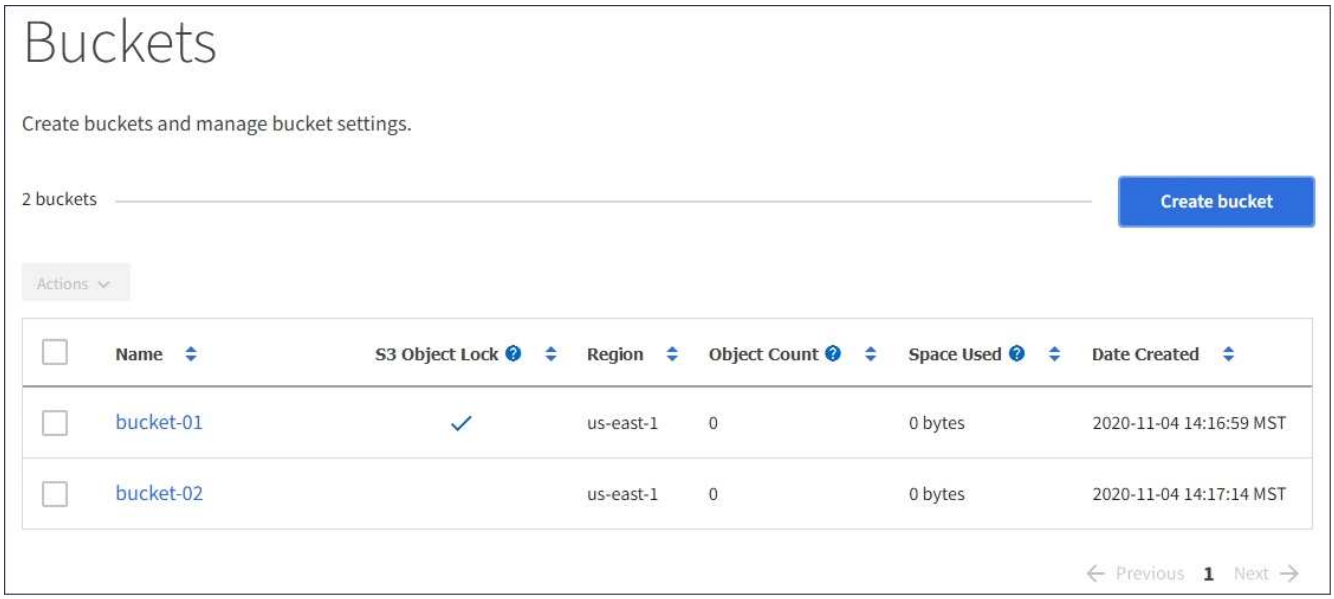
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

   Aparece la página Cuchos y enumera todos los cucharones de la cuenta de arrendatario.



2. Revisar la información de cada bloque.

   Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder por la lista.

   - Nombre: Nombre único del bloque, que no se puede cambiar.
   - S3 Object Lock: Si está habilitado el bloqueo de objetos de S3 para este bloque.

     Esta columna no se muestra si la configuración global de bloqueo de objetos S3 está deshabilitada. Esta columna también muestra información para todos los segmentos compatibles anteriores.

   - Región: La región del cucharón, que no se puede cambiar.
   - Recuento de objetos: El número de objetos de este bloque.
   - Espacio utilizado: Tamaño lógico de todos los objetos de este bloque. El tamaño lógico no incluye el espacio real necesario para las copias replicadas o con código de borrado o para los metadatos de objetos.
   - Fecha de creación: La fecha y la hora en que se creó el segmento.

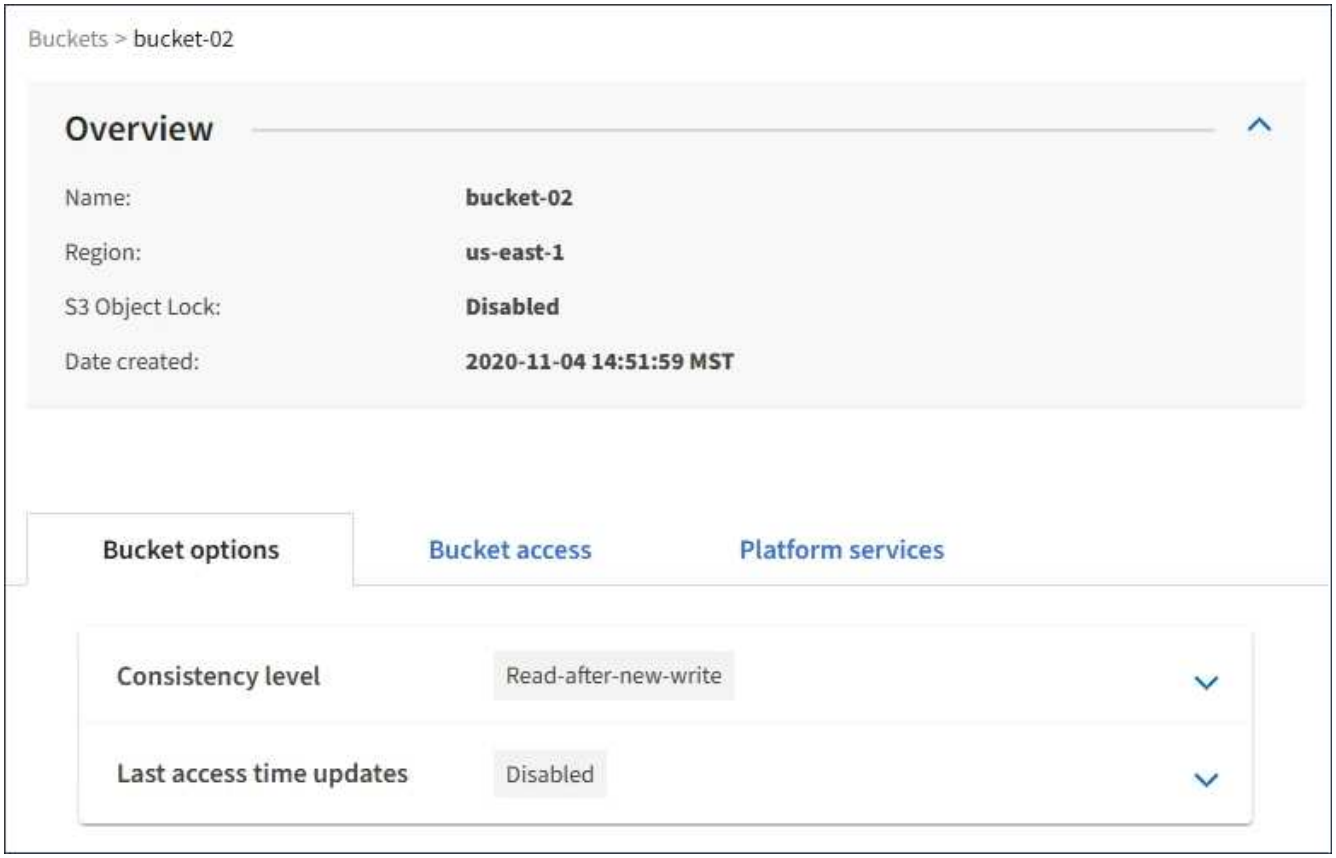
   > Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo.

3. Para ver y gestionar la configuración de un bloque, seleccione el nombre del bloque.

   Aparece la página de detalles bucket.

   Esta página le permite ver y editar la configuración para las opciones de bloque, el acceso a bloque y los servicios de plataforma.

   Consulte las instrucciones para configurar cada ajuste o servicio de plataforma.



Información relacionada

"Cambiar el nivel de coherencia"

"Habilitar o deshabilitar las actualizaciones de la hora del último acceso"

"Configuración de uso compartido de recursos de origen cruzado (CORS)"

"Configurar la replicación de CloudMirror"

"Configuración de notificaciones de eventos"

"Configurar el servicio de integración de búsqueda"

Cambiar el nivel de coherencia

Si usa un inquilino de S3, puede usar el administrador de inquilinos o la API de gestión de inquilinos para cambiar el control de coherencia para las operaciones realizadas en los objetos en los bloques S3.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El nivel de coherencia establece una compensación entre la disponibilidad de los objetos y la coherencia de

dichos objetos en los diferentes nodos y sitios de almacenamiento. En general, debe utilizar el nivel de consistencia de **lectura tras escritura nueva** para sus cucharones. Si el nivel de consistencia de **lectura tras escritura nueva** no cumple los requisitos de la aplicación cliente, puede cambiar el nivel de consistencia estableciendo el nivel de consistencia de la cuchara o utilizando la `Consistency-Control` encabezado. La `Consistency-Control` el encabezado anula el nivel de consistencia del cucharón.

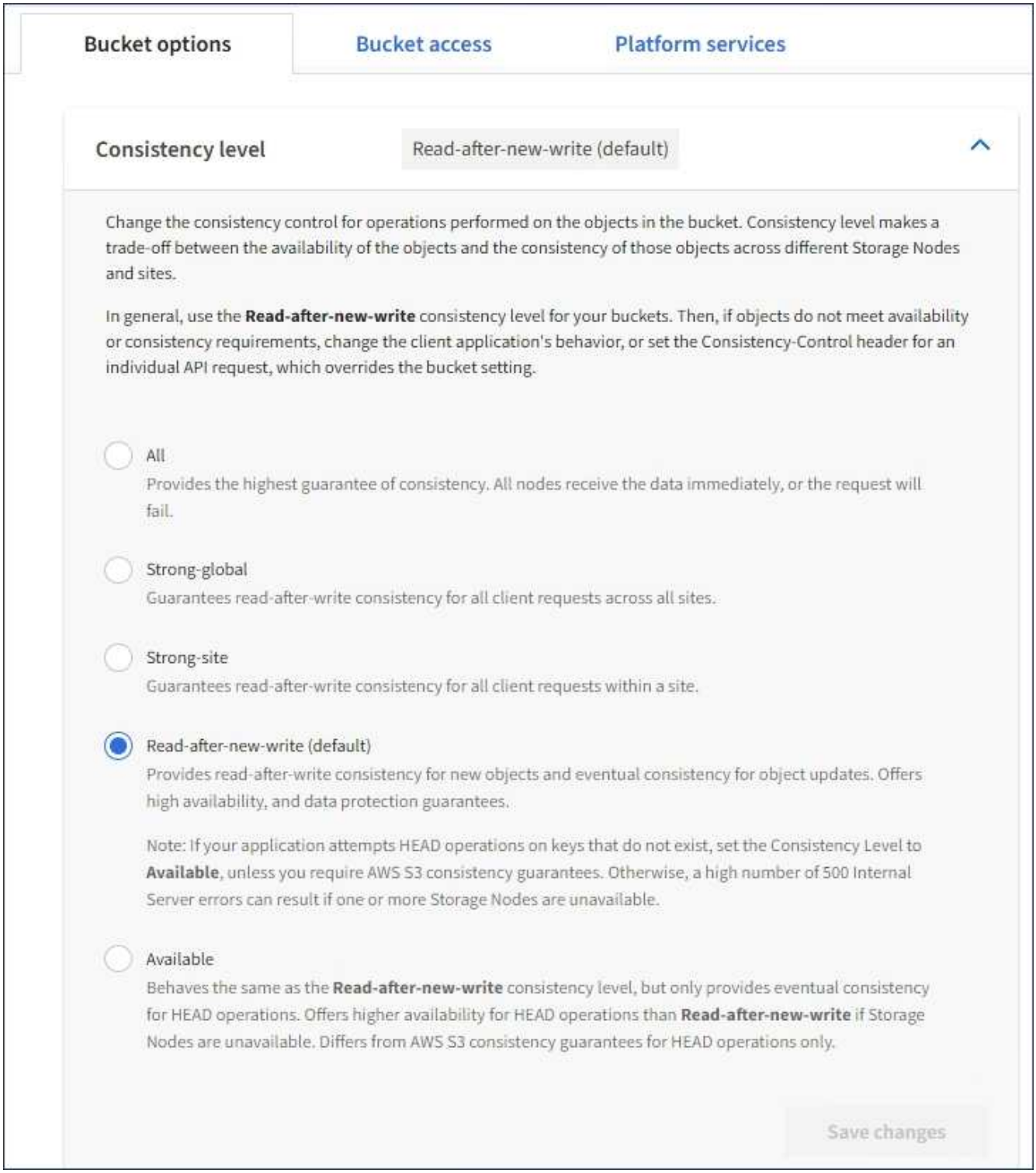
> Cuando se cambia el nivel de consistencia de un cubo, solo se garantiza que los objetos que se ingieren después del cambio alcancen el nivel revisado.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque** > **nivel de coherencia**.



4. Seleccione un nivel de coherencia para las operaciones realizadas en los objetos de este bloque.

Nivel de coherencia	Descripción
Todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.

Nivel de coherencia	Descripción
Fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
Sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
Read-after-new-write (predeterminado)	Proporciona coherencia de lectura tras escritura para los objetos nuevos y consistencia final para las actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Coincide con las garantías de coherencia de Amazon S3. **Nota:** Si su aplicación intenta realizar operaciones HEAD en claves que no existen, establezca el nivel de consistencia en **disponible**, a menos que necesite garantías de consistencia de Amazon S3. De lo contrario, un número elevado de 500 errores internos del servidor pueden producirse si uno o más nodos de almacenamiento no están disponibles.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia de **lectura tras escritura nueva**, pero sólo proporciona consistencia eventual para las operaciones DE CABEZAL. Ofrece una mayor disponibilidad para operaciones CON CABEZAL que **lectura tras escritura nueva** si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

5. Seleccione **Guardar cambios**.

Información relacionada

"Permisos de gestión de inquilinos"

Habilitar o deshabilitar las actualizaciones de la hora del último acceso

Cuando los administradores de grid crean las reglas de gestión del ciclo de vida de la información (ILM) para un sistema StorageGRID, puede especificar si desea mover ese objeto a una ubicación de almacenamiento diferente. Si usa un inquilino de S3, puede aprovechar esas reglas al habilitar actualizaciones en la última hora de acceso para los objetos de un bloque de S3.

Estas instrucciones sólo se aplican a los sistemas StorageGRID que incluyen al menos una regla de ILM que utiliza la opción **última hora de acceso** en sus instrucciones de colocación. Puede ignorar estas instrucciones si el sistema StorageGRID no incluye dicha regla.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Last Access Time es una de las opciones disponibles para la instrucción de colocación **Reference Time** para una regla de ILM. Si se establece el tiempo de referencia de una regla en tiempo de último acceso, los administradores de la cuadrícula pueden especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento en función de cuándo se recuperaron por última vez esos objetos (se leen o se visualizan).

Por ejemplo, para asegurarse de que los objetos que se ven recientemente permanecen en un almacenamiento más rápido, el administrador de grid puede crear una regla de ILM que especifique lo siguiente:

- Los objetos que se han recuperado durante el último mes deben permanecer en los nodos de almacenamiento local.
- Los objetos que no se han recuperado en el último mes deben moverse a una ubicación externa.

> Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

De forma predeterminada, las actualizaciones de la hora del último acceso están desactivadas. Si el sistema StorageGRID incluye una regla de ILM que utiliza la opción **Hora de último acceso** y desea que esta opción se aplique a los objetos de este bloque, debe habilitar las actualizaciones para el último tiempo de acceso para los bloques S3 especificados en esa regla.

> La actualización del último tiempo de acceso cuando se recupera un objeto puede reducir el rendimiento de la StorageGRID, especialmente en objetos pequeños.

El impacto en el rendimiento se produce con las actualizaciones del último tiempo de acceso porque StorageGRID debe realizar estos pasos adicionales cada vez que se recuperan los objetos:

- Actualice los objetos con nuevas marcas de tiempo
- Añada los objetos a la cola de ILM para poder reevaluarlos según las reglas y políticas actuales de ILM

La tabla resume el comportamiento aplicado a todos los objetos del bloque cuando la hora de último acceso está desactivada o habilitada.

Tipo de solicitud	Comportamiento si la hora del último acceso está desactivada (valor predeterminado)		Comportamiento si la hora del último acceso está activada	
	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	No	Sí	Sí

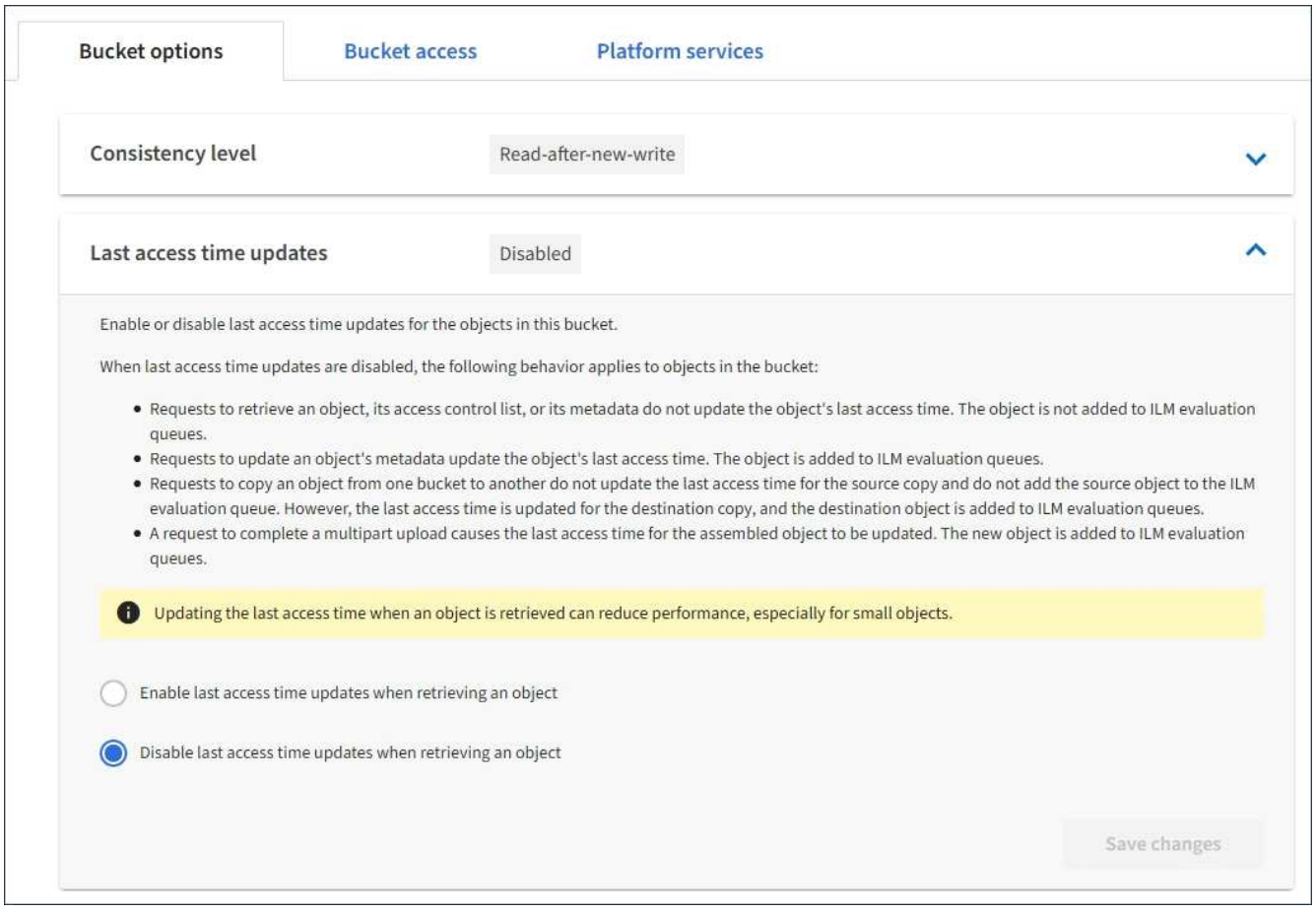
Solicitud para actualizar los metadatos de un objeto	Sí	Sí	Sí	Sí
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque** > **actualizaciones del último tiempo de acceso**.
4. Seleccione el botón de opción adecuado para activar o desactivar las actualizaciones de la hora del último acceso.



5. Seleccione **Guardar cambios**.

Información relacionada

"Permisos de gestión de inquilinos"

"Gestión de objetos con ILM"

Configuración de uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bloque de S3 si desea que dicho bloque y los objetos de ese bloque sean accesibles a las aplicaciones web de otros dominios.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite que las aplicaciones web de cliente de un dominio accedan a los recursos de un dominio diferente. Por ejemplo, supongamos que se utiliza un bloque de S3 llamado `Images` para almacenar gráficos. Configurando CORS para `Images` bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web `http://www.example.com`.

Pasos

1. Utilice un editor de texto para crear el XML necesario para habilitar CORS.

   Este ejemplo muestra el XML utilizado para habilitar CORS para un bloque de S3. Este XML permite a cualquier dominio enviar solicitudes GET al bloque, pero sólo permite el `http://www.example.com` Dominio para enviar solicitudes DE PUBLICACIÓN Y ELIMINACIÓN. Se permiten todos los encabezados de las solicitudes.

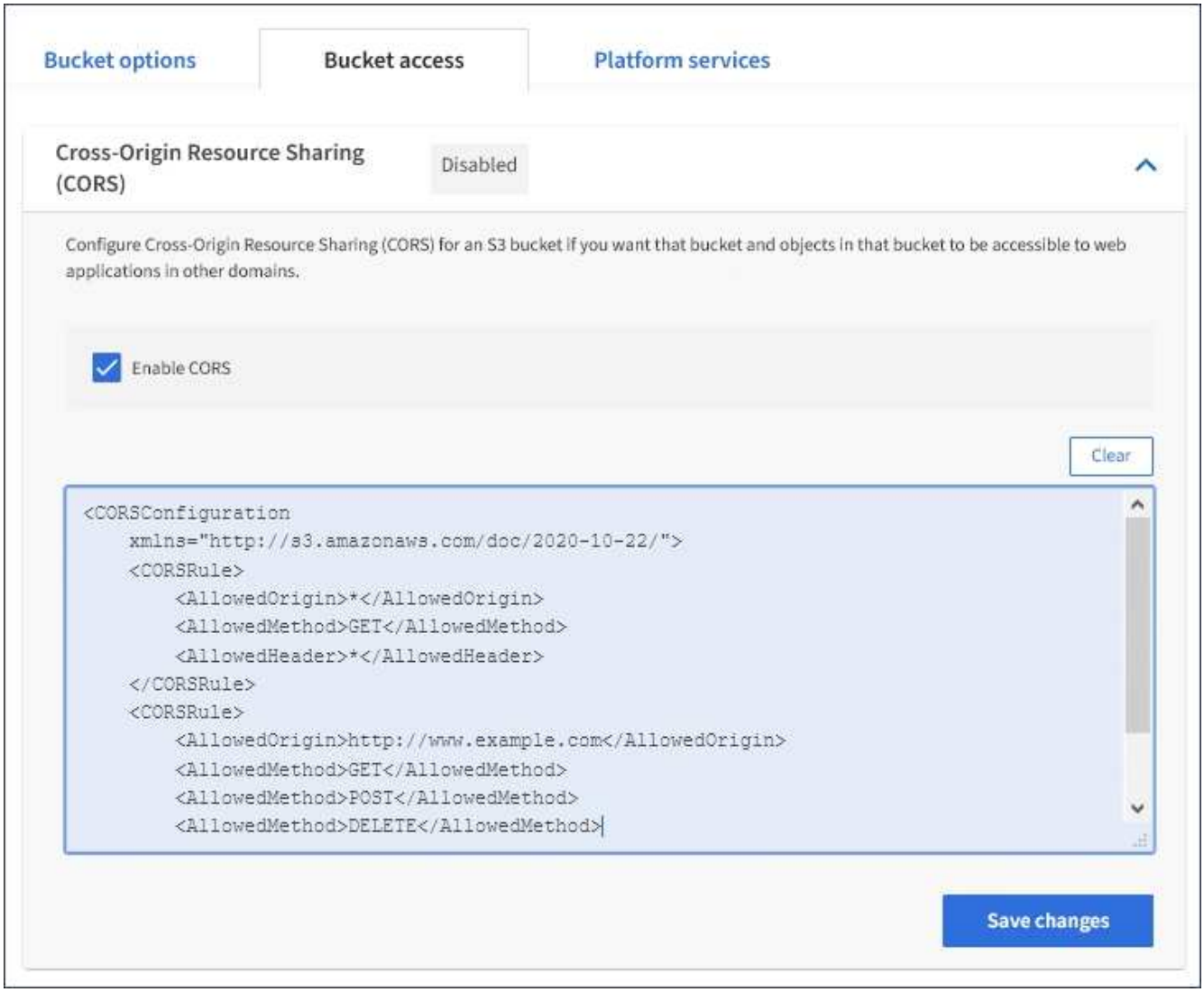
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Para obtener más información acerca del XML de configuración de CORS, consulte "Documentación de Amazon Web Services (AWS): Guía para desarrolladores de Amazon simple Storage Service".

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

4. Seleccione **acceso a bloque** > **uso compartido de recursos de origen cruzado (CORS)**.
5. Seleccione la casilla de verificación **Activar CORS**.
6. Pegue el XML de configuración de CORS en el cuadro de texto y seleccione **Guardar cambios**.



7. Para modificar la configuración de CORS para el bloque, actualice el XML de configuración de CORS en el cuadro de texto o seleccione **Borrar** para volver a empezar. A continuación, seleccione **Guardar cambios**.
8. Para desactivar CORS para el cucharón, desactive la casilla de verificación **Activar CORS** y, a continuación, seleccione **Guardar cambios**.

Eliminar un bloque de S3

Puede usar el administrador de inquilinos para eliminar un bloque de S3 que esté vacío.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un bloque de S3 mediante el administrador de inquilinos. También se pueden eliminar bloques S3 con la API de gestión de inquilinos o la API DE REST de S3.

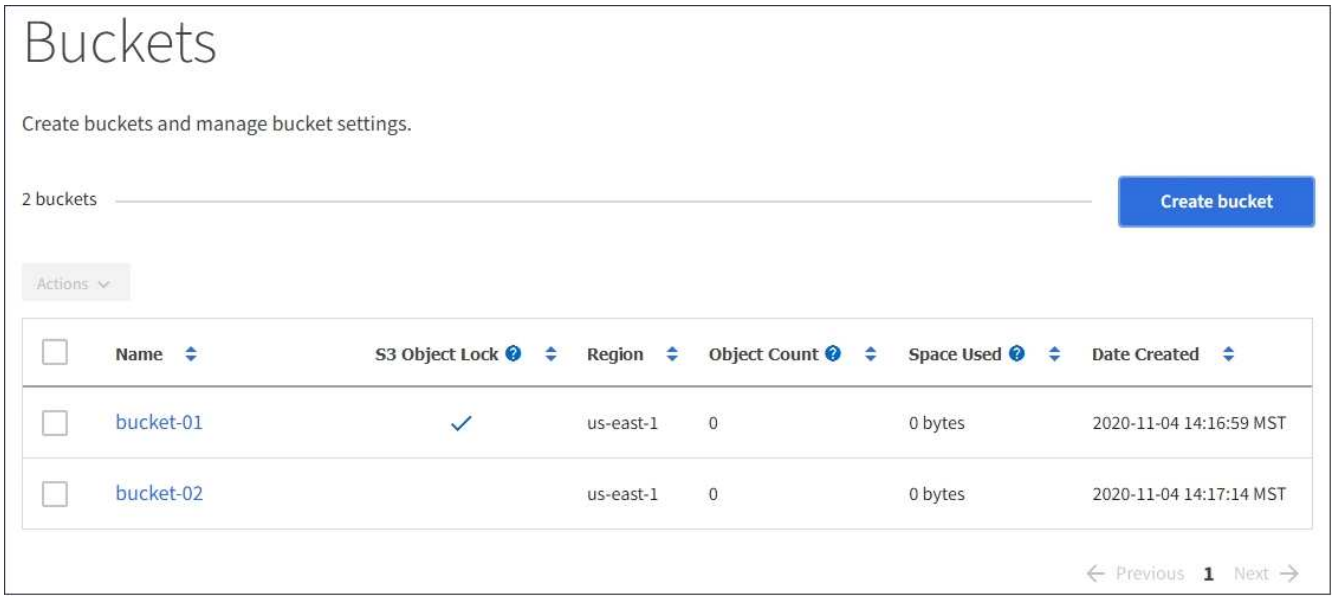
No puede eliminar un bloque de S3 si contiene objetos o versiones de objetos no actuales. Para obtener información sobre cómo se eliminan los objetos con versiones S3, consulte las instrucciones para gestionar

objetos con gestión del ciclo de vida de la información.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

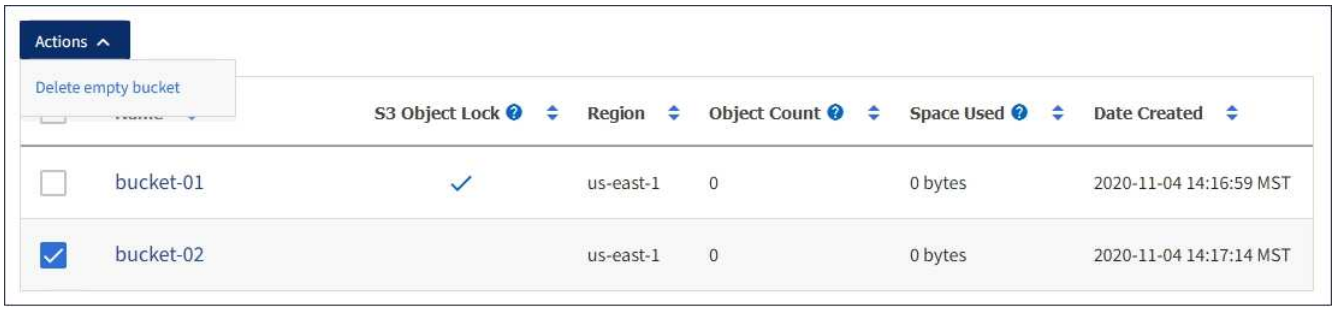
   Aparece la página Buckets y muestra todos los bloques S3 existentes.



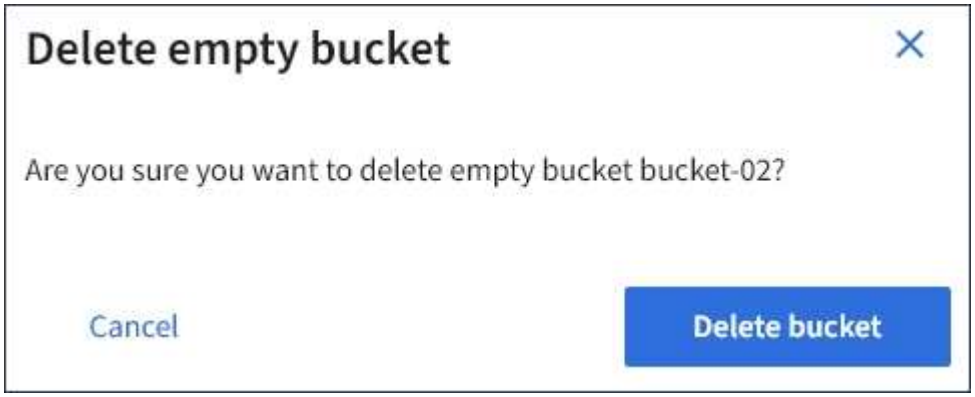
2. Seleccione la casilla de verificación para el segmento vacío que desea eliminar.

   El menú acciones está activado.

3. En el menú acciones, seleccione **Eliminar segmento vacío**.



   Aparecerá un mensaje de confirmación.



4. Si está seguro de que desea eliminar el bloque, seleccione **Eliminar bloque**.

   StorageGRID confirma que el cucharón está vacío y, a continuación, elimina el cucharón. Esta operación puede llevar algunos minutos.

   Si el segmento no está vacío, aparece un mensaje de error. Debe eliminar todos los objetos antes de poder eliminar el bloque.

Información relacionada

"Gestión de objetos con ILM"