



Usa S3 Object Lock

StorageGRID software

NetApp
July 23, 2026

Tabla de contenidos

- Usa S3 Object Lock 1
 - Cómo S3 Object Lock protege los objetos en StorageGRID 1
 - ¿Qué es S3 Object Lock? 1
 - Comparación entre S3 Object Lock y Compliance tradicional 2
 - Flujo de trabajo de S3 Object Lock en StorageGRID 4
 - Requisitos de S3 Object Lock en StorageGRID 5
 - Requisitos para usar la configuración global de S3 Object Lock 5
 - Requisitos para reglas de ILM compatibles 5
 - Requisitos para las políticas de ILM 5
 - Requisitos para los buckets con S3 Object Lock activado 6
 - Requisitos para los objetos en buckets con S3 Object Lock activado 6
 - Ciclo de vida de los objetos en los buckets con S3 Object Lock activado 6
 - Habilita el bloqueo de objetos S3 a nivel global en StorageGRID 7
 - Resuelve errores de consistencia al actualizar la configuración de S3 Object Lock o legacy Compliance en StorageGRID 8

Usa S3 Object Lock

Cómo S3 Object Lock protege los objetos en StorageGRID

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

¿Qué es S3 Object Lock?

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

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

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

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

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

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

Modos de retención

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

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

Configuración de retención para las versiones de los objetos

Si se crea un depósito con S3 Object Lock activado, los usuarios pueden usar la aplicación cliente de S3 para especificar de forma opcional los siguientes parámetros de retención para cada objeto que se añada al depósito:

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



`${post_edited_translations.segment}`

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

`${post_edited_translations.segment}`

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

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

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

Consulta ["Crear un depósito de S3"](#) y ["Actualizar la retención predeterminada de S3 Object Lock"](#).

Comparación entre S3 Object Lock y Compliance tradicional

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



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

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

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

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

Flujo de trabajo de S3 Object Lock en StorageGRID

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



`#{post_edited_translations.segment}`

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

Administrador de grid

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

Usuario arrendatario

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

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

Requisitos de S3 Object Lock en StorageGRID

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

Requisitos para usar la configuración global de S3 Object Lock

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

Requisitos para reglas de ILM compatibles

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

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

Requisitos para las políticas de ILM

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

- La regla predeterminada en una política de ILM activa o inactiva debe ser compatible.
- Las reglas de incumplimiento solo se aplican a los objetos en los buckets que no tienen habilitado S3 Object Lock o que no tienen habilitada la función de cumplimiento heredada.
- Las reglas de cumplimiento pueden aplicarse a los objetos de cualquier bucket; no es necesario que el bucket tenga activado S3 Object Lock ni el cumplimiento heredado.

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

Requisitos para los buckets con S3 Object Lock activado

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

Requisitos para los objetos en buckets con S3 Object Lock activado

- Para proteger una versión de un objeto, puedes especificar ajustes de retención predeterminados para el bucket, o puedes especificar ajustes de retención para cada versión del objeto. Los ajustes de retención a nivel de objeto se pueden especificar usando la aplicación cliente de S3 o la API de REST de S3.
- Los ajustes de retención se aplican a las versiones individuales de los objetos. Una versión de un objeto puede tener tanto una configuración de «retención hasta una fecha» como una de «retención legal», una de ellas pero no la otra, o ninguna de las dos. Al especificar una configuración de «retención hasta una fecha» o de «retención legal» para un objeto, solo se protege la versión especificada en la solicitud. Puedes crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en los buckets con S3 Object Lock activado

Cada objeto que se guarda en un bucket con S3 Object Lock activado pasa por estas etapas:

1. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- Si especificas la configuración de retención para el objeto, se aplica la configuración a nivel de objeto. Se ignora cualquier configuración predeterminada del bucket.

- Si no se especifican ajustes de retención para el objeto, se aplican los ajustes predeterminados del bucket, si existen.
- Si no se especifican ajustes de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

Si se aplican los parámetros de retención, quedan protegidos tanto el objeto como cualquier metadato definido por el usuario en S3.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el periodo de retención especificado. El número exacto y el tipo de copias de objeto y las ubicaciones de almacenamiento se determinan por las reglas de cumplimiento en las políticas de ILM activas. Si un objeto protegido puede eliminarse antes de que se alcance su fecha de retención depende de su modo de retención.

- `${post_edited_translations.segment}`

Información relacionada

- ["Crear un depósito de S3"](#)
- ["Actualizar la retención predeterminada de S3 Object Lock"](#)
- ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)
- ["Ejemplo 7: política de ILM compatible con S3 Object Lock"](#)

Habilita el bloqueo de objetos S3 a nivel global en StorageGRID

Si una cuenta de inquilino de S3 debe cumplir con los requisitos normativos a la hora de guardar datos de objetos, debes habilitar S3 Object Lock para todo tu sistema StorageGRID. Al habilitar la configuración global de S3 Object Lock, cualquier usuario de inquilino de S3 podrá crear y gestionar buckets y objetos con S3 Object Lock.

Antes de empezar

- Tienes el ["Permiso de acceso raíz"](#).
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Has revisado el flujo de trabajo de S3 Object Lock y entiendes las consideraciones.
- Has confirmado que la regla predeterminada de la política de ILM activa cumple con los requisitos. Consulta ["Crear una regla de ILM predeterminada"](#) para más detalles.

Acerca de esta tarea

El administrador de grid debe activar la configuración global de S3 Object Lock para permitir que los usuarios inquilinos creen nuevos buckets con S3 Object Lock activado. Una vez activada esta configuración, no se puede desactivar.

Revisa la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de S3 Object Lock. Cuando habilitas esta configuración, los ajustes de S3 Object Lock por inquilino dependen de la versión de StorageGRID vigente en el momento en que se creó el inquilino.



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

Pasos

1. Selecciona **Configuración > Sistema > S3 Object Lock**.

Aparece la página «Configuración de S3 Object Lock».

2. Selecciona **Habilitar bloqueo de objetos S3**.

3. Selecciona **Aplicar**.

Aparece un cuadro de diálogo de confirmación que te recuerda que no puedes desactivar S3 Object Lock después de que se haya activado.

4. Si estás seguro de que quieres activar de forma permanente S3 Object Lock para todo tu sistema, selecciona **OK**.

Cuando seleccionas **OK**:

- Si la regla predeterminada de la política de ILM activa cumple con los requisitos, S3 Object Lock queda habilitado para toda la grid y no se puede desactivar.
- Si la regla predeterminada no cumple los requisitos, aparece un error. Debes crear y activar una nueva política de ILM que incluya una regla que cumpla los requisitos como regla predeterminada. Selecciona **OK**. Luego, crea una nueva política, simúlala y actívala. Consulta ["Crear política de ILM"](#) para ver las instrucciones.

Resuelve errores de consistencia al actualizar la configuración de S3 Object Lock o legacy Compliance en StorageGRID

Si un centro de datos o varios nodos de almacenamiento de una misma ubicación dejan de estar disponibles, es posible que tengas que ayudar a los usuarios de S3 a aplicar cambios en la configuración de S3 Object Lock o en la configuración de cumplimiento heredada.

Los usuarios de un inquilino que tengan buckets con S3 Object Lock (o Compliance heredado) activado pueden cambiar ciertos ajustes. Por ejemplo, un usuario de un inquilino que use S3 Object Lock podría necesitar poner una versión de un objeto bajo retención legal.

Cuando un usuario de un inquilino actualiza la configuración de un bucket de S3 o la versión de un objeto, StorageGRID intenta actualizar inmediatamente los metadatos del bucket o del objeto en toda la grid. Si el sistema no puede actualizar los metadatos porque un data center o varios Storage Nodes no están disponibles, devuelve un error:

503: Service Unavailable

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

Para solucionar este error, sigue estos pasos:

1. Intenta que todos los nodos de almacenamiento o sitios vuelvan a estar disponibles lo antes posible.
2. Si no puedes poner a disposición un número suficiente de nodos de almacenamiento en cada sitio, ponte en contacto con el soporte técnico, que te ayudará a recuperar los nodos y a garantizar que los cambios se apliquen de forma coherente en toda la grid.
3. Una vez resuelto el problema subyacente, recuerda al usuario del tenant que vuelva a intentar aplicar los cambios de configuración.

Información relacionada

- ["Utiliza una cuenta de inquilino"](#)
- ["Usa la API de REST de S3"](#)
- ["Recuperar y mantener"](#)

Información de copyright

Copyright © 2026 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.