Cómo StorageGRID implementa la API DE REST de S3

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-115/s3/conflicting-client-requests.html on April 11, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Cómo StorageGRID implementa la API DE REST de S3

Una aplicación cliente puede utilizar llamadas API DE REST de S3 para conectarse a StorageGRID y crear, eliminar y modificar bloques, así como almacenar y recuperar objetos.

- "Solicitudes de clientes en conflicto"
- "Controles de consistencia"
- "Cómo gestionan las reglas de ILM de StorageGRID los objetos"
- "Control de versiones de objetos"
- "Recomendaciones para implementar la API REST de S3"

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como una escritura de dos clientes en la misma clave, se resuelven en base a «'últimas ventas conseguidas'».

El plazo para la evaluación de «'últimos logros'» se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 inician una operación.

Controles de consistencia

Los controles de consistencia proporcionan una compensación entre la disponibilidad de los objetos y la consistencia de dichos objetos en diferentes nodos y sitios de almacenamiento, según lo requiera su aplicación.

De forma predeterminada, StorageGRID garantiza la coherencia de lectura tras escritura de los objetos recién creados. Cualquier OBTENER después de un PUESTO completado correctamente podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones son coherentes en la actualidad. Por lo general, las sobrescrituras tardan segundos o minutos en propagarse, pero pueden tardar hasta 15 días.

Si desea realizar operaciones de objetos en un nivel de coherencia diferente, puede especificar un control de coherencia para cada bloque o para cada operación de API.

Controles de consistencia

El control de consistencia afecta a cómo los metadatos que utiliza StorageGRID para realizar un seguimiento de los objetos se distribuyen entre los nodos y, por lo tanto, la disponibilidad de los objetos para las solicitudes del cliente.

Puede establecer el control de coherencia de un bloque o una operación API en uno de los siguientes valores:

Control de consistencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
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.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Coincide con las garantías de coherencia de Amazon S3. **Nota:** Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores de Internal Server si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, establezca el control de coherencia en "'Available'" a menos que necesite garantías de coherencia similares a las de Amazon S3.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia "read-after-new-write", pero sólo proporciona consistencia eventual para las operaciones DE CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

Utilizando los controles de coherencia "ad-after-new-write" y "available"

Cuando una OPERACIÓN DE CABEZA u OBTIENE utiliza el control de consistencia «read-after-new-write» o UNA operación GET utiliza el control de consistencia «'available'», StorageGRID realiza la búsqueda en varios pasos, de la siguiente manera:

- Primero busca el objeto con una baja consistencia.
- Si esa búsqueda falla, repite la búsqueda en el siguiente nivel de consistencia hasta alcanzar el nivel de consistencia más alto, "'all,'", lo que requiere que todas las copias de los metadatos del objeto estén disponibles.

Si una operación HEAD o GET utiliza el control de consistencia «read-after-new-write» pero el objeto no existe, la búsqueda de objetos siempre alcanzará el nivel de consistencia «'all'». Debido a que este nivel de consistencia requiere que todas las copias de los metadatos del objeto estén disponibles, puede recibir un

número elevado de 500 errores de servidor interno si uno o más nodos de almacenamiento no están disponibles.

A menos que necesite garantías de coherencia similares a las de Amazon S3, puede evitar estos errores en operaciones CON CABEZAL estableciendo el control de coherencia en "'disponible'". Cuando una operación DE CABEZAL utiliza el control de consistencia "'disponible'", StorageGRID proporciona únicamente consistencia eventual. No vuelve a intentar una operación fallida hasta que alcanza el nivel de consistencia "'all'", por lo que no requiere que todas las copias de los metadatos del objeto estén disponibles.

Especifique el control de consistencia para una operación API

Para configurar el control de coherencia para una operación de API individual, deben ser compatibles los controles de coherencia para la operación y debe especificar el control de coherencia en el encabezado de la solicitud. En este ejemplo se establece el control de coherencia en «punto de referencia» para una operación GET Object.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

Debe usar el mismo control de coherencia para las operaciones PUT Object y GET Object.

Especificar el control de consistencia de un bloque

Para establecer el control de consistencia para el bloque, puede utilizar StorageGRID la solicitud de consistencia PUT Bucket y LA solicitud DE consistencia GET Bucket. También puede usar el Administrador de inquilinos o la API de gestión de inquilinos.

Cuando configure los controles de coherencia para un cucharón, tenga en cuenta lo siguiente:

- La configuración del control de coherencia para un bloque determina el control de coherencia que se utiliza para las operaciones de S3 realizadas en los objetos del bloque o en la configuración de bloques. No afecta a las operaciones del propio cucharón.
- El control de coherencia de una operación API individual anula el control de coherencia del bloque.
- En general, los cucharones deben utilizar el control de coherencia predeterminado, «entre una y otra escritura». Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de la aplicación, si es posible. O bien, configure el cliente para especificar el control de consistencia de cada solicitud API. Establecer el control de consistencia a nivel de cucharón únicamente como último recurso.

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

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

Por ejemplo, el control de consistencia usado cuando se almacena un objeto afecta a la colocación inicial de los metadatos de objetos, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta a la colocación inicial de las copias de objetos. Dado que StorageGRID requiere acceso tanto a los

metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

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

- **Estricto**: Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **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.
- **Commit doble**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

> Antes de seleccionar el comportamiento de procesamiento de una regla de ILM, lea la descripción completa de estos ajustes en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

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

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

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

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

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

Si en su lugar ha utilizado la misma regla de ILM y el nivel de coherencia de «un sitio común», puede que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en la ubicación remota, pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

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

Información relacionada

"Gestión de objetos con ILM"

"OBTENGA la solicitud de consistencia de bloque"

"PONER solicitud de consistencia de bloque"

Cómo gestionan las reglas de ILM de StorageGRID los objetos

El administrador de grid crea reglas de gestión del ciclo de vida de la información (ILM) para gestionar los datos de los objetos que se ingieren en el sistema StorageGRID desde aplicaciones cliente de la API REST S3. A continuación, estas reglas se añaden a la política de ILM para determinar cómo y dónde se almacenan los datos de objetos con el tiempo.

La configuración de ILM determina los siguientes aspectos de un objeto:

- **Geografía**

  La ubicación de los datos de un objeto, ya sea en el sistema StorageGRID (pool de almacenamiento) o en un pool de almacenamiento en el cloud.

- **Grado de almacenamiento**

  El tipo de almacenamiento utilizado para almacenar datos de objetos, como la tecnología flash o el disco giratorio.

- **Protección contra pérdidas**

  Cuántas copias se hacen y los tipos de copias que se crean: Replicación, codificación de borrado o ambos.

- **Retención**

  Los cambios se producen a lo largo del tiempo en el modo en que se gestionan los datos de un objeto, dónde se almacenan y cómo se protegen de pérdidas.

- **Protección durante la ingesta**

  El método utilizado para proteger los datos de objetos durante el procesamiento: Colocación síncrona (utilizando las opciones equilibradas o estrictas para el comportamiento de ingesta) o creación de copias provisionales (mediante la opción Dual Commit).

Las reglas de ILM pueden filtrar y seleccionar objetos. Para los objetos ingeridos mediante S3, las reglas de ILM pueden filtrar objetos en función de los siguientes metadatos:

- Cuenta de inquilino
- Nombre del bloque
- Tiempo de ingesta
- Clave
- Hora del último acceso

De forma predeterminada, las actualizaciones del último tiempo de acceso se deshabilitan para todos los bloques S3. Si el sistema StorageGRID incluye una regla de ILM que usa la opción Last Access Time, debe habilitar las actualizaciones a la hora del último acceso para los bloques S3 especificados en esa regla. Puede habilitar las actualizaciones de la última hora de acceso mediante LA solicitud DE LA última hora de acceso DE PUT Bucket, la casilla de verificación **S3** > **Cuchos** > **Configurar la última hora de acceso** en el Administrador de inquilinos o mediante la API de administración de inquilinos. Al habilitar las actualizaciones del último tiempo de acceso, tenga en cuenta que el rendimiento de StorageGRID puede reducirse, especialmente en sistemas con objetos pequeños.

- Restricción de ubicaciones
- Tamaño del objeto
- Metadatos del usuario
- Etiqueta de objeto

Para obtener más información sobre ILM, consulte las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Información relacionada

"Usar una cuenta de inquilino"

"Gestión de objetos con ILM"

"PUT Bucket última solicitud de tiempo de acceso"

Control de versiones de objetos

Puede utilizar el control de versiones para conservar varias versiones de un objeto, lo que protege contra la eliminación accidental de objetos y le permite recuperar y restaurar versiones anteriores de un objeto.

El sistema StorageGRID implementa versiones con compatibilidad para la mayoría de las funciones y con algunas limitaciones. StorageGRID admite hasta 1,000 versiones de cada objeto.

El control de versiones de objetos puede combinarse con la gestión del ciclo de vida de la información (ILM) de StorageGRID o con la configuración del ciclo de vida de bloques de S3. Debe habilitar explícitamente el control de versiones para cada segmento a fin de activar esta funcionalidad para el bloque. A cada objeto de su bloque se le asigna un ID de versión, que genera el sistema StorageGRID.

No se admite el uso de la autenticación multifactor (MFA).

El control de versiones solo se puede habilitar en bloques creados con StorageGRID versión 10.3 o posterior.

ILM y versiones

Las políticas de ILM se aplican a cada versión de un objeto. Un proceso de análisis de ILM analiza continuamente todos los objetos y los vuelve a evaluar en relación con la política actual de ILM. Todos los cambios realizados en las políticas de ILM se aplican a todos los objetos procesados anteriormente. Esto incluye versiones que se han ingerido previamente si la versión está activada. El análisis de ILM aplica nuevos cambios de ILM a los objetos procesados previamente.

En el caso de objetos S3 en bloques habilitados para versionado, la compatibilidad con versionado le permite crear reglas de ILM que usen hora no corriente como tiempo de referencia. Cuando se actualiza un objeto, sus versiones anteriores se vuelven no actuales. El uso de un filtro de tiempo no actual permite crear políticas que reduzcan el impacto en el almacenamiento de las versiones anteriores de objetos.

> Cuando se carga una nueva versión de un objeto mediante una operación de carga de varias partes, la hora no actual de la versión original del objeto se refleja cuando se creó la carga de varias partes para la nueva versión, no cuando se completó la carga de varias partes. En casos limitados, la hora no actual de la versión original puede ser horas o días antes de la hora de la versión actual.

Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información para ver un ejemplo de política de ILM para objetos con versiones de S3.

Información relacionada

"Gestión de objetos con ILM"

Recomendaciones para implementar la API REST de S3

Debe seguir estas recomendaciones al implementar la API DE REST de S3 para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si su aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe utilizar el control de consistencia "'disponible'". Por ejemplo, debe utilizar el control de coherencia "'disponible'" si su aplicación dirige una ubicación antes DE PONERLA en práctica.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba un número elevado de 500 errores internos de Server si uno o más nodos de almacenamiento no están disponibles.

Puede establecer el control de consistencia "'Available'" para cada bloque mediante LA solicitud DE consistencia PUT Bucket, o bien puede especificar el control de consistencia en el encabezado de solicitud para una operación de API individual.

Recomendaciones para las claves de objeto

En el caso de los bloques creados en StorageGRID 11.4 o posterior, ya no es necesario restringir los nombres de claves de objetos para cumplir con las prácticas recomendadas de rendimiento. Por ejemplo, ahora puede utilizar valores aleatorios para los primeros cuatro caracteres de nombres de claves de objeto.

Para los bloques que se crearon en las versiones anteriores a StorageGRID 11.4, siga estas recomendaciones para los nombres de claves de objetos:

- No debe utilizar valores aleatorios como los primeros cuatro caracteres de claves de objeto. Esto contrasta con la anterior recomendación de AWS para prefijos clave. En su lugar, debe utilizar prefijos no aleatorios y no únicos, como `image`.
- Si sigue la recomendación anterior de AWS de utilizar caracteres aleatorios y únicos en prefijos clave, debe anteponer las claves de objeto con un nombre de directorio. Es decir, utilice este formato:

```
mybucket/mydir/f8e3-image3132.jpg
```

En lugar de este formato:

```
mybucket/f8e3-image3132.jpg
```

Recomendaciones para «lecturas de rango»

Si se selecciona la opción **Compress Stored Objects** (**Configuración** > **Opciones de cuadrícula**), las aplicaciones cliente S3 deberían evitar realizar operaciones GET Object que especifiquen un intervalo de bytes que se devolverán. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos para acceder a los bytes solicitados. LAS operaciones GET Object que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es muy ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

> Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Información relacionada

"Controles de consistencia"

"PONER solicitud de consistencia de bloque"

"Administre StorageGRID"

Información de copyright

Copyright © 2024 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.