# Come StorageGRID implementa l'API REST S3

StorageGRID

NetApp
April 10, 2024

# Sommario

Come StorageGRID implementa l'API REST S3 . . . . . 1
Richieste client in conflitto . . . . . 1
Controlli di coerenza . . . . . 1
Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID . . . . . 4
Versione degli oggetti . . . . . 5
Raccomandazioni per l'implementazione dell'API REST S3 . . . . . 6

# Come StorageGRID implementa l’API REST S3

Un’applicazione client può utilizzare le chiamate API REST S3 per connettersi a StorageGRID per creare, eliminare e modificare i bucket, oltre che per memorizzare e recuperare oggetti.

## Richieste client in conflitto

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite".

La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un’operazione.

## Controlli di coerenza

I controlli di coerenza forniscono un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage, come richiesto dall’applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET che segue UN PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

Se si desidera eseguire operazioni a oggetti a un livello di coerenza diverso, è possibile specificare un controllo di coerenza per ciascun bucket o per ciascuna operazione API.

### Controlli di coerenza

Il controllo della coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tenere traccia degli oggetti vengono distribuiti tra i nodi e, di conseguenza, sulla disponibilità degli oggetti per le richieste dei client.

È possibile impostare il controllo di coerenza per un bucket o un’operazione API su uno dei seguenti valori:

- **All**: Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non avrà esito positivo.
- **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all’interno di un sito.
- **Read-after-new-write**: (Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

## Utilizzare i controlli di coerenza “read-after-new-write” e “available”

Quando un’operazione HEAD o GET utilizza il controllo di coerenza “read-after-new-write”, StorageGRID esegue la ricerca in più passaggi, come segue:

- Per prima cosa, cerca l’oggetto utilizzando una bassa coerenza.
- Se la ricerca non riesce, ripete la ricerca al livello di coerenza successivo fino a raggiungere un livello di coerenza equivalente al comportamento per un livello globale-forte.

Se un’operazione HEAD o GET utilizza il controllo di coerenza “read-after-new-write” ma l’oggetto non esiste, la ricerca dell’oggetto raggiungerà sempre un livello di coerenza equivalente al comportamento per strong-Global. Poiché questo livello di coerenza richiede la disponibilità di più copie dei metadati dell’oggetto in ciascun sito, è possibile ricevere un numero elevato di errori 500 interni del server se due o più nodi di storage nello stesso sito non sono disponibili.

A meno che non necessiti di garanzie di coerenza simili a Amazon S3, puoi evitare questi errori per LE operazioni HEAD and GET impostando il controllo di coerenza su “Available”. Quando un’operazione HEAD o GET utilizza il controllo di coerenza “Available”, StorageGRID fornisce solo la coerenza finale. Non riprova un’operazione non riuscita a livelli di coerenza crescenti, quindi non richiede la disponibilità di più copie dei metadati dell’oggetto.

## Specificare il controllo di coerenza per il funzionamento API

Per impostare il controllo di coerenza per una singola operazione API, i controlli di coerenza devono essere supportati per l’operazione e occorre specificare il controllo di coerenza nell’intestazione della richiesta. Questo esempio imposta il controllo di coerenza su “strong-site” per un’operazione GET Object.

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

> È necessario utilizzare lo stesso controllo di coerenza per le operazioni PUT object e GET object.

## Specificare il controllo di coerenza per il bucket

Per impostare il controllo di coerenza per il bucket, è possibile utilizzare la richiesta di coerenza PUT bucket StorageGRID e LA richiesta di coerenza GET bucket. In alternativa, puoi utilizzare l’API di gestione tenant o tenant Manager.

Quando si impostano i controlli di coerenza per un bucket, tenere presente quanto segue:

- L’impostazione del controllo di coerenza per un bucket determina quale controllo di coerenza viene utilizzato per le operazioni S3 eseguite sugli oggetti nel bucket o sulla configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- Il controllo di coerenza per una singola operazione API sovrascrive il controllo di coerenza per il bucket.
- In generale, i bucket devono utilizzare il controllo di coerenza predefinito, “read-after-new-write”. Se le richieste non funzionano correttamente, modificare il comportamento del client dell’applicazione, se

possibile. In alternativa, configurare il client per specificare il controllo di coerenza per ogni richiesta API. Impostare il controllo di coerenza a livello di bucket solo come ultima risorsa.

## Come interagiscono i controlli di coerenza e le regole ILM per influire sulla protezione dei dati

La scelta del controllo di coerenza e la regola ILM influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il controllo di coerenza utilizzato quando un oggetto viene memorizzato influisce sul posizionamento iniziale dei metadati dell'oggetto, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie dell'oggetto. Poiché StorageGRID richiede l'accesso sia ai metadati di un oggetto che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Strict**: Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.
- **Balanced**: StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Doppio commit**: StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.

> Prima di selezionare il comportamento di acquisizione per una regola ILM, leggere la descrizione completa di queste impostazioni in Gestire gli oggetti con ILM.

## Esempio di come il controllo di coerenza e la regola ILM possono interagire

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di coerenza:

- **ILM rule**: Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **Livello di coerenza**: "strong-Global" (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece sono state utilizzate la stessa regola ILM e il livello di coerenza "strong-site", il client potrebbe ricevere un messaggio di successo dopo la replica dei dati dell'oggetto nel sito remoto, ma prima della distribuzione dei metadati dell'oggetto. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interconnessione tra i livelli di coerenza e le regole ILM può essere complessa. Contattare NetApp per assistenza.

**Informazioni correlate**

OTTIENI una richiesta di coerenza bucket

INSERIRE la richiesta di coerenza del bucket

# Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID

L'amministratore del grid crea regole ILM (Information Lifecycle Management) per gestire i dati degli oggetti acquisiti nel sistema StorageGRID dalle applicazioni client API REST S3. Queste regole vengono quindi aggiunte al criterio ILM per determinare come e dove i dati degli oggetti vengono memorizzati nel tempo.

Le impostazioni ILM determinano i seguenti aspetti di un oggetto:

- **Geografia**

  La posizione dei dati di un oggetto, all'interno del sistema StorageGRID (pool di storage) o in un pool di storage cloud.

- **Grado di storage**

  Il tipo di storage utilizzato per memorizzare i dati dell'oggetto, ad esempio flash o disco rotante.

- **Protezione contro le perdite**

  Quante copie vengono eseguite e i tipi di copie create: Replica, erasure coding o entrambe.

- **Conservazione**

  Il cambia nel tempo in base alla modalità di gestione dei dati di un oggetto, alla posizione in cui sono memorizzati e al modo in cui sono protetti dalla perdita.

- **Protezione durante l'acquisizione**

  Metodo utilizzato per proteggere i dati degli oggetti durante l'acquisizione: Posizionamento sincrono (utilizzando le opzioni bilanciate o rigide per il comportamento di Ingest) o creazione di copie intermedie (utilizzando l'opzione Dual Commit).

Le regole ILM possono filtrare e selezionare gli oggetti. Per gli oggetti acquisiti tramite S3, le regole ILM possono filtrare gli oggetti in base ai seguenti metadati:

- Account tenant
- Nome bucket
- Tempo di acquisizione
- Chiave
- Ora ultimo accesso

> Per impostazione predefinita, gli aggiornamenti dell'ultimo tempo di accesso sono disattivati per tutti i bucket S3. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione ultimo tempo di accesso, è necessario abilitare gli aggiornamenti per l'ultimo tempo di accesso per i bucket S3 specificati in tale regola. È possibile attivare gli ultimi aggiornamenti del tempo di accesso utilizzando LA richiesta PUT Bucket Last Access Time (INSERISCI ultima ora di accesso bucket), la casella di controllo **S3** > **Bucket** > **Configure Last Access Time** (Configura ultima ora di accesso) in Tenant Manager o l'API di gestione tenant. Quando si abilitando gli ultimi aggiornamenti del tempo di accesso, tenere presente che le prestazioni di StorageGRID potrebbero essere ridotte, soprattutto nei sistemi con oggetti di piccole dimensioni.

- Vincolo di posizione
- Dimensione oggetto
- Metadati dell'utente
- Tag oggetto

Per ulteriori informazioni su ILM, vedere le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

**Informazioni correlate**

USA account tenant

Gestire gli oggetti con ILM

METTI richiesta dell'ultimo tempo di accesso al bucket

# Versione degli oggetti

È possibile utilizzare il controllo delle versioni per conservare più versioni di un oggetto, che protegge dall'eliminazione accidentale di oggetti e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con il supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 1,000 versioni di ciascun oggetto.

La versione degli oggetti può essere combinata con la gestione del ciclo di vita delle informazioni di StorageGRID (ILM) o con la configurazione del ciclo di vita del bucket S3. Per attivare questa funzionalità per il bucket, è necessario abilitare esplicitamente il controllo delle versioni per ciascun bucket. A ciascun oggetto del bucket viene assegnato un ID di versione, generato dal sistema StorageGRID.

L'utilizzo dell'autenticazione MFA (multi-factor Authentication) Delete non è supportato.

> Il controllo delle versioni può essere attivato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

## ILM e versione

I criteri ILM vengono applicati a ogni versione di un oggetto. Un processo di scansione ILM esegue una scansione continua di tutti gli oggetti e li rivaluti in base al criterio ILM corrente. Qualsiasi modifica apportata ai criteri ILM viene applicata a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente ingerite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche

ILM agli oggetti acquisiti in precedenza.

Per gli oggetti S3 nei bucket abilitati per il controllo delle versioni, il supporto delle versioni consente di creare regole ILM che utilizzano l'ora non corrente come tempo di riferimento. Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro orario non corrente consente di creare policy che riducono l'impatto sullo storage delle versioni precedenti degli oggetti.

> Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, l'ora non corrente per la versione originale dell'oggetto si riflette quando il caricamento multiparte è stato creato per la nuova versione, non quando il caricamento multiparte è stato completato. In casi limitati, il tempo non corrente per la versione originale potrebbe essere di ore o giorni prima del tempo per la versione corrente.

Vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni per un esempio di policy ILM per gli oggetti con versione S3.

**Informazioni correlate**

Gestire gli oggetti con ILM

# Raccomandazioni per l'implementazione dell'API REST S3

Seguire questi consigli quando si implementa l'API REST S3 per l'utilizzo con StorageGRID.

## Raccomandazioni per la gestione di oggetti inesistenti

Se l'applicazione verifica regolarmente l'esistenza di un oggetto in un percorso in cui non si prevede l'effettiva esistenza dell'oggetto, utilizzare il controllo di coerenza "Available". Ad esempio, è necessario utilizzare il controllo di coerenza "Available" se l'applicazione dirige una posizione prima DI INSERIRVI.

In caso contrario, se l'operazione HEAD non trova l'oggetto, potrebbe essere visualizzato un numero elevato di errori 500 nel server interno se uno o più nodi di storage non sono disponibili.

È possibile impostare il controllo di coerenza "Available" per ciascun bucket utilizzando LA richiesta di coerenza PUT bucket oppure specificare il controllo di coerenza nell'intestazione della richiesta per una singola operazione API.

## Raccomandazioni per le chiavi a oggetti

Per i bucket creati in StorageGRID 11.4 o versioni successive, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. Ad esempio, è ora possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi oggetto.

Per i bucket creati in release precedenti a StorageGRID 11.4, continuare a seguire questi consigli per i nomi delle chiavi degli oggetti:

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Si consiglia invece di utilizzare prefissi non casuali e non univoci, ad esempio `image`.
- Se si segue la precedente raccomandazione AWS per utilizzare caratteri casuali e univoci nei prefissi delle chiavi, è necessario anteporre le chiavi oggetto a un nome di directory. Ovvero, utilizzare questo formato:

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

Invece di questo formato:

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

## Raccomandazioni per “range reads”

Se l’opzione **compress stored objects** è selezionata (**CONFIGURATION** > **System** > **Grid options**), le applicazioni client S3 dovrebbero evitare di eseguire operazioni GET object che specificano un intervallo di byte da restituire. Queste operazioni “range Read” sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è molto inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client possono scadere.

> Se è necessario comprimere gli oggetti e l’applicazione client deve utilizzare le letture dell’intervallo, aumentare il timeout di lettura per l’applicazione.

**Informazioni correlate**

- Controlli di coerenza
- INSERIRE la richiesta di coerenza del bucket
- Amministrare StorageGRID