



# **Come StorageGRID implementa l'API REST S3**

StorageGRID 11.7

NetApp  
April 12, 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
  - Utilizzare l'API REST S3 per configurare il blocco oggetti S3 ..... 6
  - Creare la configurazione del ciclo di vita S3 ..... 12
  - Raccomandazioni per l'implementazione dell'API REST S3 ..... 16

# Come StorageGRID implementa l'API REST S3

## 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:

- **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.
- **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.



Prima di selezionare il comportamento di acquisizione per una regola ILM, leggere la descrizione completa di queste impostazioni nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

## 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

"Gestire gli oggetti con ILM"

"COERENZA del bucket"

"METTI la 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 dell'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. Utilizza LA richiesta PUT bucket Last access time, il tenant manager (vedere ["Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso"](#)) 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 dell'oggetto
- Metadati dell'utente
- Tag oggetto

#### Informazioni correlate

["Utilizzare un account tenant"](#)

["Gestire gli oggetti con ILM"](#)

["TEMPO ULTIMO accesso 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 "ora non corrente" come ora di riferimento (selezionare **Sì** per la domanda, "applicare questa regola solo alle versioni di oggetti precedenti?" poll ["Fase 1 della creazione guidata di una regola ILM"](#)).

Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro "Noncurrent Time" 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 ["Regole e criteri ILM per gli oggetti con versione S3 \(esempio 4\)"](#).

## Utilizzare l'API REST S3 per configurare il blocco oggetti S3

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato. È possibile specificare la conservazione predefinita per ogni bucket o impostazioni di conservazione per ciascuna versione dell'oggetto.

### Come attivare il blocco oggetti S3 per un bucket

Se l'impostazione globale di blocco oggetti S3 è attivata per il sistema StorageGRID, è possibile attivare il blocco oggetti S3 quando si crea ciascun bucket.

S3 Object Lock è un'impostazione permanente che può essere attivata solo quando si crea un bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

Per attivare il blocco oggetti S3 per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager. Vedere ["Creare un bucket S3"](#).
- Creare il bucket utilizzando una richiesta PUT bucket con `x-amz-bucket-object-lock-enabled` intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando viene creato il bucket. Non puoi sospendere il controllo delle versioni per il bucket. Vedere ["Versione degli oggetti"](#).

### Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è attivato per un bucket, è possibile attivare la conservazione predefinita per il bucket e specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito.

#### Modalità di conservazione predefinita

- In modalità COMPLIANCE:
  - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
  - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità GOVERNANCE:



- Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione.
- Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
- Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

## Periodo di conservazione predefinito

Ogni bucket può avere un periodo di conservazione predefinito specificato in anni o giorni.

## Come impostare la conservazione predefinita per un bucket

Per impostare la conservazione predefinita per un bucket, utilizzare uno dei seguenti metodi:

- Gestire le impostazioni del bucket da Tenant Manager. Vedere ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).
- Inviare una richiesta DI configurazione PUT Object Lock per il bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

## PUT Object Lock Configuration (CONFIGURAZIONE blocco oggetto)

La richiesta PUT Object Lock Configuration consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket con S3 Object Lock attivato. È inoltre possibile rimuovere le impostazioni di conservazione predefinite precedentemente configurate.

Quando le nuove versioni degli oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` e `x-amz-object-lock-retain-until-date` non sono specificati. Il periodo di conservazione predefinito viene utilizzato per calcolare il periodo di conservazione fino alla data se `x-amz-object-lock-retain-until-date` non specificato.

Se il periodo di conservazione predefinito viene modificato dopo l'acquisizione di una versione dell'oggetto, la data di conservazione della versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

È necessario disporre di `s3:PutBucketObjectLockConfiguration` autorizzazione, o essere root dell'account, per completare questa operazione.

Il Content-MD5 L'intestazione della richiesta deve essere specificata nella richiesta PUT.

## Esempio di richiesta

Questo esempio attiva il blocco oggetti S3 per un bucket e imposta la modalità di conservazione predefinita su COMPLIANCE e il periodo di conservazione predefinito su 6 anni.

```

PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>

```

## Come determinare la conservazione predefinita per un bucket

Per determinare se S3 Object Lock è attivato per un bucket e per visualizzare la modalità di conservazione e il periodo di conservazione predefiniti, utilizzare uno dei seguenti metodi:

- Visualizza il bucket nel tenant manager. Vedere ["Visualizza i bucket S3"](#).
- Eseguire una richiesta GET Object Lock Configuration.

### OTTIENI configurazione blocco oggetto

La richiesta GET Object Lock Configuration (OTTIENI configurazione blocco oggetto) consente di determinare se S3 Object Lock (blocco oggetto S3) è attivato per un bucket e, se è attivato, di verificare se sono configurate una modalità di conservazione predefinita e un periodo di conservazione per il bucket.

Quando le nuove versioni degli oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` non specificato. Il periodo di conservazione predefinito viene utilizzato per calcolare il periodo di conservazione fino alla data se `x-amz-object-lock-retain-until-date` non specificato.

È necessario disporre di `s3:GetBucketObjectLockConfiguration` autorizzazione, o essere root dell'account, per completare questa operazione.

### Esempio di richiesta

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

### Esempio di risposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

## Come specificare le impostazioni di conservazione per un oggetto

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate utilizzando l'API REST S3. Le impostazioni di conservazione per un oggetto sovrascrivono le impostazioni di conservazione predefinite per il bucket.

È possibile specificare le seguenti impostazioni per ciascun oggetto:

- **Modalità di conservazione:** CONFORMITÀ o GOVERNANCE.
- **Conserva-fino-data:** Una data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da StorageGRID.

- In modalità COMPLIANCE, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. È possibile aumentare la data di conservazione fino alla data prevista, ma non è possibile ridurla o rimuoverla.
- In modalità GOVERNANCE, gli utenti con autorizzazioni speciali possono ignorare l'impostazione di conservazione fino alla data odierna. Possono eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere il mantenimento fino ad oggi.
- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa.

L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla conservazione fino alla data. Se una versione dell'oggetto è sottoposta a blocco legale, nessuno può eliminare tale versione.

Per specificare le impostazioni di blocco oggetti S3 quando si aggiunge una versione di oggetto a un bucket, eseguire un "METTI oggetto", "METTI oggetto - Copia", o "Avvia caricamento multiparte" richiesta.

È possibile utilizzare quanto segue:

- `x-amz-object-lock-mode`, Che può essere COMPLIANCE o GOVERNANCE (sensibile al maiuscolo/minuscolo).



Se si specifica `x-amz-object-lock-mode`, è inoltre necessario specificare `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
  - La data di conservazione deve essere in futuro.
- `x-amz-object-lock-legal-hold`

Se la conservazione legale È ATTIVA (sensibile al maiuscolo/minuscolo), l'oggetto viene collocato sotto una conservazione legale. Se l'opzione Legal Hold è disattivata, non viene effettuata alcuna conservazione a fini giudiziari. Qualsiasi altro valore genera un errore 400 Bad Request (InvalidArgument).

Se si utilizza una di queste intestazioni di richiesta, tenere presente le seguenti restrizioni:

- Il `Content-MD5` l'intestazione della richiesta è obbligatoria, se presente `x-amz-object-lock-*` L'intestazione della richiesta è presente nella richiesta DELL'oggetto PUT. `Content-MD5` Non è richiesto per METTERE oggetto - copiare o avviare caricamento multiparte.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` L'intestazione della richiesta è presente, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta DI oggetti PUT supporta l'utilizzo di `x-amz-storage-class: REDUCED_REDUNDANCY` Per far corrispondere il comportamento di AWS. Tuttavia, quando un oggetto viene acquisito in un bucket con il blocco oggetti S3 attivato, StorageGRID eseguirà sempre un ingest a doppio commit.

- Una risposta successiva ALLA versione DELL'oggetto GET o HEAD includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e. `x-amz-object-lock-legal-hold`, se configurato e se il mittente della richiesta ha il corretto `s3:Get*` permessi.

È possibile utilizzare `s3:object-lock-remaining-retention-days` chiave di condizione dei criteri per limitare i periodi di conservazione minimi e massimi consentiti per gli oggetti.

## Come aggiornare le impostazioni di conservazione per un oggetto

Se è necessario aggiornare le impostazioni di conservazione o conservazione a fini giudiziari per una versione di oggetto esistente, è possibile eseguire le seguenti operazioni di sottorisorsa oggetto:

- `PUT Object legal-hold`

Se IL nuovo valore di conservazione a fini giudiziari è ATTIVO, l'oggetto viene collocato sotto una conservazione a fini giudiziari. Se il valore di conservazione a fini giudiziari è OFF, la conservazione a fini giudiziari viene revocata.

- `PUT Object retention`
  - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (distinzione tra maiuscole e minuscole).
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
  - Se una versione a oggetti ha un valore di conservazione esistente fino alla data odierna, è possibile aumentarlo. Il nuovo valore deve essere in futuro.

## Come utilizzare LA modalità DI GOVERNANCE

Utenti che dispongono di `s3:BypassGovernanceRetention` L'autorizzazione può ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità DI GOVERNANCE. Tutte le operazioni DI eliminazione o CONSERVAZIONE degli oggetti PUT devono includere `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire queste operazioni aggiuntive:

- Eseguire operazioni DI ELIMINAZIONE di oggetti o DI ELIMINAZIONE di oggetti multipli per eliminare una versione di oggetti prima che sia trascorso il periodo di conservazione.

Non è possibile eliminare gli oggetti che si trovano sotto un blocco legale. La sospensione legale deve essere disattivata.

- Eseguire operazioni DI conservazione degli oggetti PUT che modificano la modalità di una versione dell'oggetto da GOVERNANCE a COMPLIANCE prima che sia trascorso il periodo di conservazione dell'oggetto.

Non è mai consentito cambiare la modalità dalla CONFORMITÀ alla GOVERNANCE.

- Eseguire operazioni DI conservazione DEGLI oggetti PUT per aumentare, ridurre o rimuovere il periodo di conservazione di una versione dell'oggetto.

### Informazioni correlate

- ["Gestire gli oggetti con S3 Object Lock"](#)

- ["USA il blocco oggetti S3 per conservare gli oggetti"](#)
- ["Amazon Simple Storage Service User Guide \(Guida utente di Amazon Simple Storage Service\): Utilizzo di S3 Object Lock"](#)

## Creare la configurazione del ciclo di vita S3

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono cancellati dal sistema StorageGRID.

Il semplice esempio di questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando alcuni oggetti vengono cancellati (scaduti) da specifici bucket S3. L'esempio in questa sezione è a solo scopo illustrativo. Per informazioni dettagliate sulla creazione di configurazioni del ciclo di vita S3, vedere ["Amazon Simple Storage Service Developer Guide: Gestione del ciclo di vita degli oggetti"](#). Nota: StorageGRID supporta solo le azioni di scadenza e non le azioni di transizione.

### Che cos'è la configurazione del ciclo di vita

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in specifici bucket S3. Ogni regola specifica quali oggetti sono interessati e quando scadranno (in una data specifica o dopo un certo numero di giorni).

StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:

- Scadenza: Consente di eliminare un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dalla data di acquisizione dell'oggetto.
- NoncurrentVersionExpiration (NoncurrentExpiration versione): Consente di eliminare un oggetto quando viene raggiunto un numero di giorni specificato, a partire da quando l'oggetto è diventato non corrente.
- Filtro (prefisso, tag)
- Stato
- ID

Se si applica una configurazione del ciclo di vita a un bucket, le impostazioni del ciclo di vita del bucket sovrascrivono sempre le impostazioni ILM di StorageGRID. StorageGRID utilizza le impostazioni di scadenza per il bucket, non ILM, per determinare se eliminare o conservare oggetti specifici.

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora applicabili all'oggetto. Oppure, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni di posizionamento ILM per l'oggetto. Per ulteriori informazioni, vedere ["Come ILM opera per tutta la vita di un oggetto"](#).



La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- ELIMINA ciclo di vita bucket
- OTTIENI il ciclo di vita del bucket

- METTI IL ciclo di vita del bucket

## Creare la configurazione del ciclo di vita

Come primo passo nella creazione di una configurazione del ciclo di vita, è possibile creare un file JSON che includa una o più regole. Ad esempio, questo file JSON include tre regole, come segue:

1. La regola 1 si applica solo agli oggetti che corrispondono al prefisso `category1/` e che hanno un `key2` valore di `tag2`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno alla mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2/`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno 100 giorni dopo l'acquisizione.



Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato acquisito. Se la data corrente supera la data di acquisizione più il numero di giorni, alcuni oggetti potrebbero essere rimossi dal bucket non appena viene applicata la configurazione del ciclo di vita.

3. La regola 3 si applica solo agli oggetti che corrispondono al prefisso `category3/`. Il `Expiration` parametro specifica che qualsiasi versione non corrente degli oggetti corrispondenti scadrà 50 giorni dopo che diventeranno non aggiornati.

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```



## Applica la configurazione del ciclo di vita al bucket

Dopo aver creato il file di configurazione del ciclo di vita, lo si applica a un bucket inviando una richiesta DI ciclo di vita PUT bucket.

Questa richiesta applica la configurazione del ciclo di vita nel file di esempio agli oggetti in un bucket denominato `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Per verificare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, emettere una richiesta DI ciclo di vita GET Bucket. Ad esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Una risposta corretta elenca la configurazione del ciclo di vita appena applicata.

## Verificare che la scadenza del ciclo di vita del bucket si applichi all'oggetto

È possibile determinare se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico quando si invia una richiesta DI oggetto PUT, HEAD o GET. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata associata.



Poiché il ciclo di vita del bucket ha la priorità su ILM, il sistema `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere ["Come viene determinata la conservazione degli oggetti"](#).

Ad esempio, questa richiesta DI oggetti PUT è stata emessa il 22 giugno 2020 e inserisce un oggetto in `testbucket` bucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta corretta indica che l'oggetto scadrà tra 100 giorni (01 ottobre 2020) e che corrisponde alla regola 2 della configurazione del ciclo di vita.

```
{
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  ETag: "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Ad esempio, questa richiesta di oggetto HEAD è stata utilizzata per ottenere metadati per lo stesso oggetto nel bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La risposta di successo include i metadati dell'oggetto e indica che l'oggetto scadrà tra 100 giorni e che corrisponde alla regola 2.

```
{
  "AcceptRanges": "bytes",
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```

## 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

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base alla prima volta che il bucket è stato creato.

### Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Utilizzare invece 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, inserire un prefisso tra le chiavi degli oggetti e il nome della directory. Ovvero, utilizzare questo formato:

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

Invece di questo formato:

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

### Bucket creati in StorageGRID 11.4 o versioni successive

Non è necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.



Un'eccezione è rappresentata da un carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto delle performance per questo caso d'utilizzo, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa di simile alla data. Si supponga, ad esempio, che un client S3 scriva in genere 2,000 oggetti al secondo e che il criterio del ciclo di vita di ILM o bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto delle performance, è possibile assegnare un nome alle chiavi utilizzando un modello come questo:

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

## Raccomandazioni per “range reads”

Se il ["opzione globale per comprimere gli oggetti memorizzati"](#) È attivato, 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 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"](#)
- ["METTI la coerenza del bucket"](#)
- ["Amministrare StorageGRID"](#)

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.