



Operazioni sugli oggetti

StorageGRID software

NetApp
December 03, 2025

Sommario

Operazioni sugli oggetti	1
Operazioni sugli oggetti	1
Utilizzare S3 Select	4
Clausole	5
Tipi di dati	5
Operatori	5
Funzioni aggregate	6
Funzioni condizionali	6
Funzioni di conversione	6
Funzioni di data	6
Funzioni stringa	7
Utilizzare la crittografia lato server	7
Utilizzare SSE	7
Utilizzare SSE-C	8
Considerazioni sull'utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)	8
CopiaOggetto	9
Risolvere i conflitti	9
Dimensione dell'oggetto	9
Caratteri UTF-8 nei metadati utente	9
Intestazioni di richiesta supportate	10
Intestazioni di richiesta non supportate	11
Opzioni di classe di archiviazione	11
Utilizzo di x-amz-copy-source in CopyObject	11
Intestazioni di richiesta per la crittografia lato server	12
Controllo delle versioni	13
OttieniOggetto	13
GetObject e oggetti multipart	13
Caratteri UTF-8 nei metadati utente	13
Intestazione della richiesta supportata	13
Intestazione della richiesta non supportata	13
Controllo delle versioni	13
Intestazioni di richiesta per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)	14
Comportamento di GetObject per gli oggetti Cloud Storage Pool	14
GetObject e replicazione tra griglie	15
HeadObject	15
HeadObject e oggetti multiparte	15
Caratteri UTF-8 nei metadati utente	16
Intestazione della richiesta supportata	16
Intestazione della richiesta non supportata	16
Controllo delle versioni	16
Intestazioni di richiesta per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)	16

Risposte HeadObject per gli oggetti Cloud Storage Pool	17
HeadObject e replicazione cross-grid	18
MettiOggetto	19
Risolvere i conflitti	19
Dimensione dell'oggetto	19
Dimensione dei metadati utente	19
Caratteri UTF-8 nei metadati utente	19
Limiti dei tag degli oggetti	19
Proprietà dell'oggetto	20
Intestazioni di richiesta supportate	20
Intestazioni di richiesta non supportate	21
Opzioni di classe di archiviazione	21
Intestazioni di richiesta per la crittografia lato server	23
Controllo delle versioni	23
Calcoli della firma per l'intestazione di autorizzazione	23
Ripristina oggetto	24
Tipo di richiesta supportato	24
Controllo delle versioni	24
Comportamento di RestoreObject sugli oggetti Cloud Storage Pool	24
SelezionaOggettoContenuto	25
Esempio di sintassi della richiesta CSV	26
Esempio di sintassi della richiesta Parquet	27
Esempio di query SQL	27
Esempio di utilizzo di AWS-CLI (CSV)	28
Esempio di utilizzo di AWS-CLI (Parquet)	29

Operazioni sugli oggetti

Operazioni sugli oggetti

Questa sezione descrive come il sistema StorageGRID implementa le operazioni S3 REST API per gli oggetti.

Le seguenti condizioni si applicano a tutte le operazioni sugli oggetti:

- StorageGRID "**valori di coerenza**" sono supportati da tutte le operazioni sugli oggetti, ad eccezione delle seguenti:
 - OttieniOggettoAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelezionaOggettoContenuto
- Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, compresi gli oggetti creati da un utente anonimo o da un altro account.
- Gli oggetti dati acquisiti nel sistema StorageGRID tramite Swift non sono accessibili tramite S3.

La tabella seguente descrive come StorageGRID implementa le operazioni degli oggetti S3 REST API.

Operazione	Implementazione
EliminaOggetto	<p data-bbox="589 163 1484 226">Autenticazione a più fattori (MFA) e intestazione di risposta <code>x-amz-mfa</code> non sono supportati.</p> <p data-bbox="589 264 1484 499">Durante l'elaborazione di una richiesta <code>DeleteObject</code>, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni archiviate. In caso di esito positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e quindi segnala l'esito positivo al client.</p> <p data-bbox="589 537 899 562">Controllo delle versioni</p> <p data-bbox="630 579 1484 783">Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare <code>versionId</code> sottorisorsa. L'utilizzo di questa sottorisorsa elimina definitivamente la versione. Se il <code>versionId</code> corrisponde a un marcatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene restituito impostato su <code>true</code>.</p> <ul data-bbox="654 825 1484 1297" style="list-style-type: none"> • Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket con controllo delle versioni abilitato, si traduce nella generazione di un marcatore di eliminazione. IL <code>versionId</code> per il marcatore di eliminazione viene restituito utilizzando il <code>x-amz-version-id</code> intestazione di risposta e <code>x-amz-delete-marker</code> l'intestazione di risposta viene restituita impostata su <code>true</code>. • Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket con controllo delle versioni sospeso, si traduce nell'eliminazione permanente di una versione 'null' già esistente o di un marcatore di eliminazione 'null' e nella generazione di un nuovo marcatore di eliminazione 'null'. IL <code>x-amz-delete-marker</code> l'intestazione di risposta viene restituita impostata su <code>true</code>. <p data-bbox="678 1335 1369 1398">Nota: in alcuni casi, potrebbero esistere più marcatori di eliminazione per un oggetto.</p> <p data-bbox="589 1451 1442 1545">Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.</p>
EliminaOggetti (in precedenza denominato DELETE Multiple Objects)	<p data-bbox="589 1608 1484 1671">Autenticazione a più fattori (MFA) e intestazione di risposta <code>x-amz-mfa</code> non sono supportati.</p> <p data-bbox="589 1703 1425 1734">È possibile eliminare più oggetti nello stesso messaggio di richiesta.</p> <p data-bbox="589 1770 1442 1864">Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.</p>

Operazione	Implementazione
DeleteObjectTagging	<p>Utilizza il <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un oggetto.</p> <p>Controllo delle versioni</p> <p>Se il <code>versionId</code> Se il parametro di query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.</p>
OttieniOggetto	"OttieniOggetto"
OttieniOggettoAcl	Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, il <code>DisplayName</code> e l'autorizzazione del proprietario dell'oggetto, a indicare che il proprietario ha accesso completo all'oggetto.
OttieniOggettoLegaleHold	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
Ottieni conservazione oggetto	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
OttieniTaggingOggetto	<p>Utilizza il <code>tagging</code> sottorisorsa per restituire tutti i tag per un oggetto.</p> <p>Controllo delle versioni</p> <p>Se il <code>versionId</code> Se il parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag dalla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.</p>
HeadObject	"HeadObject"
Ripristina oggetto	"Ripristina oggetto"
MettiOggetto	"MettiOggetto"
CopiaOggetto (in precedenza denominato PUT Object - Copy)	"CopiaOggetto"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
PutObjectRetention	"Utilizzare l'API REST S3 per configurare S3 Object Lock"

Operazione	Implementazione
PutObjectTagging	<p>Utilizza il <code>tagging</code> sottorisorsa per aggiungere un set di tag a un oggetto esistente.</p> <p>Limiti dei tag degli oggetti</p> <p>Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole.</p> <p>Aggiornamenti dei tag e comportamento di acquisizione</p> <p>Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non reingestisce l'oggetto. Ciò significa che l'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.</p> <p>Ciò significa che se la regola ILM utilizza l'opzione Rigorosa per il comportamento di acquisizione, non viene intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio perché una posizione appena richiesta non è disponibile). L'oggetto aggiornato mantiene la sua posizione attuale finché non sarà possibile il posizionamento richiesto.</p> <p>Risolvere i conflitti</p> <p>Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.</p> <p>Controllo delle versioni</p> <p>Se il <code>versionId</code> Se il parametro <code>query</code> non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.</p>
SelezionaOggettoContenuto	"SelezionaOggettoContenuto"

Utilizzare S3 Select

StorageGRID supporta le seguenti clausole Amazon S3 Select, tipi di dati e operatori per ["Comando SelectObjectContent"](#).



Tutti gli elementi non elencati non sono supportati.

Per la sintassi, vedere ["Seleziona Oggetto Contenuto"](#) . Per ulteriori informazioni su S3 Select, vedere ["Documentazione AWS per S3 Select"](#) .

Solo gli account tenant che hanno abilitato S3 Select possono inviare query SelectObjectContent. Vedi il ["considerazioni e requisiti per l'utilizzo di S3 Select"](#) .

Clausole

- SELEZIONA elenco
- clausola FROM
- clausola WHERE
- Clausola LIMIT

Tipi di dati

- bool
- intero
- corda
- galleggiante
- decimale, numerico
- marca temporale

Operatori

Operatori logici

- E
- NON
- O

Operatori di confronto

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- FRA
- IN

Operatori di corrispondenza di pattern

- COME
- _
- %

Operatori unitari

- È NULLO
- NON È NULLO

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni aggregate

- MEDIA()
- CONTARE(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- CASO
- COALESCERE
- NULLIF

Funzioni di conversione

- CAST (per i tipi di dati supportati)

Funzioni di data

- DATA_AGGIUNGI
- DATE_DIFF
- ESTRARRE
- A_STRINGA
- TO_TIMESTAMP

- UTCNOW

Funzioni stringa

- LUNGHEZZA_CARATTERE, LUNGHEZZA_CARATTERE
- INFERIORE
- SOTTOSTRINGA
- ORDINARE
- SUPERIORE

Utilizzare la crittografia lato server

La crittografia lato server consente di proteggere i dati degli oggetti quando sono inattivi. StorageGRID crittografa i dati durante la scrittura dell'oggetto e li decrittografa quando si accede all'oggetto.

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni reciprocamente esclusive, in base al modo in cui vengono gestite le chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite StorageGRID):** quando si invia una richiesta S3 per archiviare un oggetto, StorageGRID crittografa l'oggetto con una chiave univoca. Quando si invia una richiesta S3 per recuperare l'oggetto, StorageGRID utilizza la chiave memorizzata per decrittografare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente):** quando si invia una richiesta S3 per archiviare un oggetto, si fornisce la propria chiave di crittografia. Quando recuperi un oggetto, fornisci la stessa chiave di crittografia come parte della tua richiesta. Se le due chiavi di crittografia corrispondono, l'oggetto viene decrittografato e vengono restituiti i dati dell'oggetto.

Mentre StorageGRID gestisce tutte le operazioni di crittografia e decrittografia degli oggetti, è necessario gestire le chiavi di crittografia fornite.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente.



Se un oggetto è crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Utilizzare SSE

Per crittografare un oggetto con una chiave univoca gestita da StorageGRID, utilizzare la seguente intestazione di richiesta:

```
x-amz-server-side-encryption
```

L'intestazione della richiesta SSE è supportata dalle seguenti operazioni sugli oggetti:

- "MettiOggetto"
- "CopiaOggetto"

- ["CreaCaricamentoMultiparte"](#)

Utilizzare SSE-C

Per crittografare un oggetto con una chiave univoca gestita da te, puoi utilizzare tre intestazioni di richiesta:

Intestazione della richiesta	Descrizione
x-amz-server-side-encryption-customer-algorithm	Specificare l'algoritmo di crittografia. Il valore dell'intestazione deve essere AES256.
x-amz-server-side-encryption-customer-key	Specificare la chiave di crittografia che verrà utilizzata per crittografare o decrittografare l'oggetto. Il valore della chiave deve essere a 256 bit, codificato in base64.
x-amz-server-side-encryption-customer-key-MD5	Specificare il digest MD5 della chiave di crittografia secondo RFC 1321, utilizzato per garantire che la chiave di crittografia sia stata trasmessa senza errori. Il valore per il digest MD5 deve essere codificato in base64 a 128 bit.

Le intestazioni delle richieste SSE-C sono supportate dalle seguenti operazioni sugli oggetti:

- ["OttieniOggetto"](#)
- ["HeadObject"](#)
- ["MettiOggetto"](#)
- ["CopiaOggetto"](#)
- ["CreaCaricamentoMultiparte"](#)
- ["CaricaParte"](#)
- ["CaricaParteCopia"](#)

Considerazioni sull'utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)

Prima di utilizzare SSE-C, tenere presente quanto segue:

- Devi usare https.



StorageGRID rifiuta qualsiasi richiesta effettuata tramite http quando si utilizza SSE-C. Per motivi di sicurezza, è opportuno considerare compromessa qualsiasi chiave inviata accidentalmente tramite http. Scartare la chiave e ruotarla come appropriato.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire la mappatura delle chiavi di crittografia sugli oggetti. StorageGRID non memorizza le chiavi di crittografia. Sei responsabile del monitoraggio della chiave di crittografia fornita per ciascun oggetto.
- Se il bucket è abilitato al controllo delle versioni, ogni versione dell'oggetto dovrebbe avere la propria chiave di crittografia. Sei responsabile del monitoraggio della chiave di crittografia utilizzata per ogni

versione dell'oggetto.

- Poiché le chiavi di crittografia vengono gestite sul lato client, è necessario gestire anche eventuali misure di sicurezza aggiuntive, come la rotazione delle chiavi, sul lato client.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente.

- Se per il bucket è configurata la replica tra griglie o la replica CloudMirror, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non andrà a buon fine.

Informazioni correlate

["Guida per l'utente di Amazon S3: utilizzo della crittografia lato server con chiavi fornite dal cliente \(SSE-C\)"](#)

CopiaOggetto

È possibile utilizzare la richiesta S3 CopyObject per creare una copia di un oggetto già archiviato in S3. Un'operazione CopyObject equivale all'esecuzione di GetObject seguito da PutObject.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa ["caricamento multiparte"](#). Invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se hai eseguito l'aggiornamento da StorageGRID 11.6 o da una versione precedente, verrà attivato l'avviso S3 PUT Object size too large (Dimensioni oggetto troppo grandi) se tenti di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11.7 o 11.8, in questo caso l'avviso non verrà attivato. Tuttavia, per allinearsi allo standard AWS S3, le future versioni di StorageGRID non supporteranno caricamenti di oggetti di dimensioni superiori a 5 GiB.

Caratteri UTF-8 nei metadati utente

Se una richiesta include valori UTF-8 (non sottoposti a escape) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 sottoposti a escape vengono trattati come caratteri ASCII:

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 con escape.
- StorageGRID non restituisce il `x-amz-missing-meta` intestazione se il valore interpretato del nome o del

valore della chiave include caratteri non stampabili.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- x-amz-meta-, seguito da una coppia nome-valore contenente metadati definiti dall'utente
- x-amz-metadata-directive: Il valore predefinito è COPY , che consente di copiare l'oggetto e i metadati associati.

Puoi specificare REPLACE per sovrascrivere i metadati esistenti durante la copia dell'oggetto o per aggiornare i metadati dell'oggetto.

- x-amz-storage-class
- x-amz-tagging-directive: Il valore predefinito è COPY , che consente di copiare l'oggetto e tutti i tag.

Puoi specificare REPLACE per sovrascrivere i tag esistenti durante la copia dell'oggetto o per aggiornare i tag.

- Intestazioni delle richieste di blocco degli oggetti S3:
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

Se viene effettuata una richiesta senza queste intestazioni, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#) .

- Intestazioni delle richieste SSE:
 - x-amz-copy-source-server-side-encryption-customer-algorithm
 - x-amz-copy-source-server-side-encryption-customer-key
 - x-amz-copy-source-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption
 - x-amz-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption-customer-key
 - x-amz-server-side-encryption-customer-algorithm

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm

Quando si copia un oggetto, se l'oggetto di origine ha un checksum, StorageGRID non copia quel valore di checksum nel nuovo oggetto. Questo comportamento si applica indipendentemente dal fatto che tu provi o meno a utilizzare `x-amz-checksum-algorithm` nella richiesta dell'oggetto.

- x-amz-website-redirect-location

Opzioni di classe di archiviazione

IL `x-amz-storage-class` l'intestazione della richiesta è supportata e influisce sul numero di copie dell'oggetto che StorageGRID crea se la regola ILM corrispondente utilizza il commit doppio o bilanciato ["opzione di ingestione"](#).

- STANDARD

(Predefinito) Specifica un'operazione di acquisizione a doppio commit quando la regola ILM utilizza l'opzione Doppio commit o quando l'opzione Bilanciato ricorre alla creazione di copie provvisorie.

- REDUCED_REDUNDANCY

Specifica un'operazione di acquisizione con commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ricorre alla creazione di copie provvisorie.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, REDUCED_REDUNDANCY l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, REDUCED_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di x-amz-copy-source in CopyObject

Se il bucket di origine e la chiave, specificati in `x-amz-copy-source` intestazione, sono diversi dal bucket di destinazione e dalla chiave, una copia dei dati dell'oggetto sorgente viene scritta nella destinazione.

Se la sorgente e la destinazione corrispondono, e il `x-amz-metadata-directive` l'intestazione è specificata come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non reingerisce l'oggetto. Ciò ha due importanti conseguenze:

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la crittografia di un oggetto esistente sul posto. Se fornisci il `x-amz-server-side-encryption` intestazione o il `x-amz-server-side-encryption-customer-algorithm` intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented`.
- L'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.

Ciò significa che se la regola ILM utilizza l'opzione Rigorosa per il comportamento di acquisizione, non viene intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio perché una posizione appena richiesta non è disponibile). L'oggetto aggiornato mantiene la sua posizione attuale finché non sarà possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se tu [utilizzare la crittografia lato server](#), le intestazioni di richiesta fornite dipendono dal fatto che l'oggetto di origine sia crittografato e dal fatto che si intenda crittografare l'oggetto di destinazione.

- Se l'oggetto sorgente è crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta CopyObject, in modo che l'oggetto possa essere decrittografato e quindi copiato:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Specifica la chiave di crittografia fornita al momento della creazione dell'oggetto sorgente.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 fornito quando hai creato l'oggetto sorgente.
- Se desideri crittografare l'oggetto di destinazione (la copia) con una chiave univoca che fornisci e gestisci, includi le seguenti tre intestazioni:
 - `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-server-side-encryption-customer-key`: Specificare una nuova chiave di crittografia per l'oggetto di destinazione.
 - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della nuova chiave di crittografia.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per ["utilizzando la crittografia lato server"](#).

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da StorageGRID (SSE), includere questa intestazione nella richiesta CopyObject:

- `x-amz-server-side-encryption`



IL `server-side-encryption` il valore dell'oggetto non può essere aggiornato. Invece, fai una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive: REPLACE`.

Controllo delle versioni

Se il bucket di origine è sottoposto a versioning, è possibile utilizzare `x-amz-copy-source` intestazione per copiare l'ultima versione di un oggetto. Per copiare una versione specifica di un oggetto, è necessario specificare esplicitamente la versione da copiare utilizzando `versionId` sottorisorsa. Se il bucket di destinazione è sottoposto a versioning, la versione generata viene restituita nel `x-amz-version-id` intestazione di risposta. Se il controllo delle versioni è sospeso per il bucket di destinazione, allora `x-amz-version-id` restituisce un valore "null".

OttieniOggetto

È possibile utilizzare la richiesta S3 `GetObject` per recuperare un oggetto da un bucket S3.

GetObject e oggetti multipart

Puoi usare il `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multipart o segmentato. IL `x-amz-mp-parts-count` l'elemento di risposta indica quante parti ha l'oggetto.

Puoi impostare `partNumber` a 1 sia per gli oggetti segmentati/multipart che per gli oggetti non segmentati/non multipart; tuttavia, il `x-amz-mp-parts-count` l'elemento response viene restituito solo per oggetti segmentati o multipart.

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le richieste GET per un oggetto con caratteri UTF-8 sfuggiti nei metadati definiti dall'utente non restituiscono `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione della richiesta supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`: Specificare `ENABLED`

IL Range l'intestazione non è supportata con `x-amz-checksum-mode` per `GetObject`. Quando includi Range nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore di checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented` :

- `x-amz-website-redirect-location`

Controllo delle versioni

Se un `versionId` Se la sottorisorsa non è specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "Non trovato" con `x-amz-delete-marker` intestazione di risposta impostata su `true`

Intestazioni di richiesta per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre le intestazioni se l'oggetto è crittografato con una chiave univoca da te fornita.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256 .
- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 della chiave di crittografia dell'oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in ["Utilizzare la crittografia lato server"](#) .

Comportamento di GetObject per gli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un ["Pool di archiviazione cloud"](#) , il comportamento di una richiesta GetObject dipende dallo stato dell'oggetto. Vedere ["HeadObject"](#) per maggiori dettagli.



Se un oggetto è archiviato in un Cloud Storage Pool e una o più copie dell'oggetto esistono anche sulla griglia, le richieste GetObject tenteranno di recuperare i dati dalla griglia prima di recuperarli dal Cloud Storage Pool.

Stato dell'oggetto	Comportamento di GetObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	200 OK Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	200 OK Viene recuperata una copia dell'oggetto.
Oggetto passato a uno stato non recuperabile	403 Forbidden , InvalidObjectState Utilizzare un "Ripristina oggetto" richiesta di ripristinare l'oggetto a uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden , InvalidObjectState Attendi il completamento della richiesta RestoreObject.

Stato dell'oggetto	Comportamento di GetObject
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Viene recuperata una copia dell'oggetto.

Oggetti multiparte o segmentati in un pool di archiviazione cloud

Se hai caricato un oggetto multiparte o se StorageGRID ha suddiviso un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel Cloud Storage Pool campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta GetObject potrebbe restituire in modo errato 200 OK quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

In questi casi:

- La richiesta GetObject potrebbe restituire alcuni dati ma interrompersi a metà del trasferimento.
- Una successiva richiesta GetObject potrebbe restituire 403 Forbidden .

GetObject e replicazione tra griglie

Se stai usando "federazione di rete" E "replicazione cross-grid" è abilitato per un bucket, il client S3 può verificare lo stato di replicazione di un oggetto emettendo una richiesta GetObject. La risposta include StorageGRID-specifico x-ntap-sg-cgr-replication-status intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	<ul style="list-style-type: none"> • COMPLETO: La replica è riuscita. • IN ATTESA: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta il x-amz-replication-status intestazione.

HeadObject

È possibile utilizzare la richiesta S3 HeadObject per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto è archiviato in un Cloud Storage Pool, è possibile utilizzare HeadObject per determinare lo stato di transizione dell'oggetto.

HeadObject e oggetti multiparte

Puoi usare il partNumber parametro di richiesta per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. IL x-amz-mp-parts-count l'elemento di risposta indica quante parti ha l'oggetto.

Puoi impostare `partNumber` a 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, il `x-amz-mp-parts-count` l'elemento response viene restituito solo per oggetti segmentati o multiparte.

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le richieste HEAD per un oggetto con caratteri UTF-8 sfuggiti nei metadati definiti dall'utente non restituiscono `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione della richiesta supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`

IL `partNumber` parametro e Range l'intestazione non è supportata con `x-amz-checksum-mode` per `HeadObject`. Quando li includi nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore di checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Controllo delle versioni

Se un `versionId` Se la sottorisorsa non è specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "Non trovato" con `x-amz-delete-marker` intestazione di risposta impostata su `true`.

Intestazioni di richiesta per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre queste intestazioni se l'oggetto è crittografato con una chiave univoca da te fornita.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 della chiave di crittografia dell'oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in ["Utilizzare la crittografia lato server"](#).

Risposte HeadObject per gli oggetti Cloud Storage Pool

Se l'oggetto è memorizzato in un ["Pool di archiviazione cloud"](#) , vengono restituite le seguenti intestazioni di risposta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Le intestazioni di risposta forniscono informazioni sullo stato di un oggetto mentre viene spostato in un Cloud Storage Pool, facoltativamente portato a uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta a HeadObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	200 OK(Non viene restituita alcuna intestazione di risposta speciale.)
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Finché l'oggetto non viene portato in uno stato non recuperabile, il valore per <code>expiry-date</code> è ambientato in un lontano futuro. Il momento esatto della transizione non è controllato dal sistema StorageGRID .
L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche sulla griglia	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Il valore per <code>expiry-date</code> è ambientato in un lontano futuro. Nota: se la copia sulla griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario emettere un "Ripristina oggetto" richiedere di ripristinare la copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.

Stato dell'oggetto	Risposta a HeadObject
L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia sulla griglia	200 OK x-amz-storage-class: GLACIER
Oggetto in fase di ripristino da uno stato non recuperabile	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" IL expiry-date indica quando l'oggetto nel Cloud Storage Pool tornerà a uno stato non recuperabile.

Oggetti multiparte o segmentati in Cloud Storage Pool

Se hai caricato un oggetto multiparte o se StorageGRID ha suddiviso un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel Cloud Storage Pool campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire in modo errato x-amz-restore: ongoing-request="false" quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

HeadObject e replicazione cross-grid

Se stai usando ["federazione di rete"](#) E ["replicazione cross-grid"](#) è abilitato per un bucket, il client S3 può verificare lo stato di replicazione di un oggetto inviando una richiesta HeadObject. La risposta include StorageGRID-specifico x-ntap-sg-cgr-replication-status intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	<ul style="list-style-type: none"> • COMPLETO: La replica è riuscita. • IN ATTESA: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA: L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta il `x-amz-replication-status` intestazione.

MettiOggetto

È possibile utilizzare la richiesta S3 PutObject per aggiungere un oggetto a un bucket.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa ["caricamento multiparte"](#). Invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se hai eseguito l'aggiornamento da StorageGRID 11.6 o da una versione precedente, verrà attivato l'avviso S3 PUT Object size too large (Dimensioni oggetto troppo grandi) se tenti di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11.7 o 11.8, in questo caso l'avviso non verrà attivato. Tuttavia, per allinearsi allo standard AWS S3, le future versioni di StorageGRID non supporteranno carichi di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati utente

Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione di richiesta PUT a 2 KB. StorageGRID limita i metadati utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata sommando il numero di byte nella codifica UTF-8 di ciascuna chiave e valore.

Caratteri UTF-8 nei metadati utente

Se una richiesta include valori UTF-8 (non sottoposti a escape) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 sottoposti a escape vengono trattati come caratteri ASCII:

- Le richieste PutObject, CopyObject, GetObject e HeadObject hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 con escape.
- StorageGRID non restituisce il `x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Limiti dei tag degli oggetti

Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode

e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole.

Proprietà dell'oggetto

In StorageGRID, tutti gli oggetti sono di proprietà dell'account proprietario del bucket, compresi gli oggetti creati da un account non proprietario o da un utente anonimo.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Cache-Control
- Content-Disposition
- Content-Encoding

Quando specifichi `aws-chunked` per `Content-Encoding` StorageGRID non verifica i seguenti elementi:

- StorageGRID non verifica il `chunk-signature` rispetto ai dati in blocco.
- StorageGRID non verifica il valore fornito per `x-amz-decoded-content-length` contro l'oggetto.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codifica di trasferimento in blocchi è supportata se `aws-chunked` viene utilizzata anche la firma del payload.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

```
x-amz-meta-name: value
```

Se si desidera utilizzare l'opzione **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando è stato creato l'oggetto. Per esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi a partire dal 1° gennaio 1970.



Una regola ILM non può utilizzare sia un **orario di creazione definito dall'utente** per l'orario di riferimento sia l'opzione di acquisizione bilanciata o rigorosa. Viene restituito un errore quando viene creata la regola ILM.

- `x-amz-tagging`
- Intestazioni di richiesta di blocco degli oggetti S3
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

Se viene effettuata una richiesta senza queste intestazioni, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#).

- Intestazioni delle richieste SSE:
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

Vedere [Intestazioni di richiesta per la crittografia lato server](#)

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

IL `x-amz-website-redirect-location` intestazione ritorna `XNotImplemented`.

Opzioni di classe di archiviazione

IL `x-amz-storage-class` è supportata l'intestazione della richiesta. Il valore inviato per `x-amz-storage-class` influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto archiviate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza l'opzione di ingestione rigorosa, `x-amz-storage-class` l'intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class` :

- **STANDARD(Predefinito)**
 - **Doppio commit:** se la regola ILM specifica l'opzione Doppio commit per Comportamento di acquisizione, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita a un diverso nodo di archiviazione (doppio commit). Quando l'ILM viene valutato, StorageGRID determina se queste copie provvisorie iniziali soddisfano le istruzioni di posizionamento nella regola. In caso contrario, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e le copie provvisorie iniziali potrebbero dover essere eliminate.
 - **Bilanciato:** se la regola ILM specifica l'opzione Bilanciato e StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola, StorageGRID effettua due copie provvisorie su nodi di archiviazione diversi.

Se StorageGRID può creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), `x-amz-storage-class` l'intestazione non ha alcun effetto.

- **REDUCED_REDUNDANCY**
 - **Doppio commit:** se la regola ILM specifica l'opzione Doppio commit per Comportamento di acquisizione, StorageGRID crea una singola copia provvisoria durante l'acquisizione dell'oggetto (singolo commit).
 - **Bilanciato:** se la regola ILM specifica l'opzione Bilanciato, StorageGRID esegue una singola copia provvisoria solo se il sistema non riesce a eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. IL `REDUCED_REDUNDANCY` L'opzione è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia extra dell'oggetto per ogni operazione di acquisizione.

Utilizzando il `REDUCED_REDUNDANCY` questa opzione non è consigliata in altre circostanze.

`REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, si potrebbero perdere dati se la singola copia viene inizialmente archiviata su un nodo di archiviazione che si guasta prima che possa aver luogo la valutazione ILM.



Disporre di una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Specificando `REDUCED_REDUNDANCY` influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto effettuate quando l'oggetto viene valutato dai criteri ILM attivi e non determina l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID .



Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme `legacy`, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto con la crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID.

- `x-amz-server-side-encryption`

Quando il `x-amz-server-side-encryption` l'intestazione non è inclusa nella richiesta `PutObject`, la griglia ["impostazione di crittografia degli oggetti memorizzati"](#) viene omesso dalla risposta `PutObject`.

- **SSE-C**: utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256 .

- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo oggetto.

- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per ["utilizzando la crittografia lato server"](#) .



Se un oggetto è crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Controllo delle versioni

Se il controllo delle versioni è abilitato per un bucket, univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene restituito anche nella risposta utilizzando il `x-amz-version-id` intestazione di risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, questa verrà sovrascritta.

Calcoli della firma per l'intestazione di autorizzazione

Quando si utilizza il `Authorization` intestazione per autenticare le richieste, StorageGRID differisce da AWS nei seguenti modi:

- StorageGRID non richiede `host` intestazioni da includere all'interno `CanonicalHeaders` .
- StorageGRID non richiede `Content-Type` da includere all'interno `CanonicalHeaders` .
- StorageGRID non richiede `x-amz-*` intestazioni da includere all'interno `CanonicalHeaders` .



Come buona pratica generale, includi sempre queste intestazioni all'interno `CanonicalHeaders` per garantire che siano verificati; tuttavia, se si escludono queste intestazioni, `StorageGRID` non restituisce un errore.

Per i dettagli, fare riferimento a ["Calcoli della firma per l'intestazione di autorizzazione: trasferimento del payload in un singolo blocco \(AWS Signature versione 4\)"](#).

Informazioni correlate

- ["Gestire gli oggetti con ILM"](#)
- ["Riferimento API di Amazon Simple Storage Service: PutObject"](#)

Ripristina oggetto

È possibile utilizzare la richiesta `S3 RestoreObject` per ripristinare un oggetto archiviato in un `Cloud Storage Pool`.

Tipo di richiesta supportato

`StorageGRID` supporta solo le richieste `RestoreObject` per ripristinare un oggetto. Non supporta il `SELECT` tipo di restauro. Seleziona le richieste di ritorno `XNotImplemented`.

Controllo delle versioni

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket con versione. Se non specifichi `versionId`, viene ripristinata la versione più recente dell'oggetto.

Comportamento di `RestoreObject` sugli oggetti `Cloud Storage Pool`

Se un oggetto è stato memorizzato in un ["Pool di archiviazione cloud"](#), una richiesta `RestoreObject` ha il seguente comportamento, in base allo stato dell'oggetto. Vedere ["HeadObject"](#) per maggiori dettagli.



Se un oggetto è archiviato in un `Cloud Storage Pool` e sulla griglia sono presenti anche una o più copie dell'oggetto, non è necessario ripristinare l'oggetto inviando una richiesta `RestoreObject`. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta `GetObject`.

Stato dell'oggetto	Comportamento di <code>RestoreObject</code>
Oggetto inserito in <code>StorageGRID</code> ma non ancora valutato da ILM oppure l'oggetto non si trova in un <code>Cloud Storage Pool</code>	403 Forbidden, InvalidObjectState
Oggetto nel <code>Cloud Storage Pool</code> ma non ancora trasferito a uno stato non recuperabile	200 OK Non vengono apportate modifiche. Nota: prima che un oggetto sia passato a uno stato non recuperabile, non è possibile modificarne lo stato. <code>expiry-date</code> .

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto passato a uno stato non recuperabile	<p>`202 Accepted` Ripristina una copia recuperabile dell'oggetto nel Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto torna a uno stato non recuperabile.</p> <p>Facoltativamente, utilizzare il <code>Tier</code> elemento di richiesta per determinare quanto tempo impiegherà il processo di ripristino per essere completato (<code>Expedited</code>, <code>Standard</code>, <code>On Bulk</code>). Se non specifichi <code>Tier</code>, il <code>Standard</code> viene utilizzato il livello.</p> <p>Importante: se un oggetto è stato trasferito a S3 Glacier Deep Archive o il pool di archiviazione cloud utilizza l'archiviazione BLOB di Azure, non è possibile ripristinarlo utilizzando <code>Expedited</code> livello. Viene restituito il seguente errore <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class</code>.</p>
Oggetto in fase di ripristino da uno stato non recuperabile	<code>409 Conflict, RestoreAlreadyInProgress</code>
Oggetto completamente ripristinato nel Cloud Storage Pool	<p><code>200 OK</code></p> <p>Nota: se un oggetto è stato ripristinato in uno stato recuperabile, è possibile modificarne lo stato <code>expiry-date</code> rimettendo la richiesta <code>RestoreObject</code> con un nuovo valore per <code>Days</code>. La data di ripristino viene aggiornata in base al momento della richiesta.</p>

Selezione Oggetto Contenuto

È possibile utilizzare la richiesta S3 `SelectObjectContent` per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL.

Per maggiori informazioni vedere ["Riferimento API di Amazon Simple Storage Service: SelectObjectContent"](#).

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 `Select`.
- Hai `s3:GetObject` autorizzazione per l'oggetto che si desidera interrogare.
- L'oggetto che si desidera interrogare deve essere in uno dei seguenti formati:
 - **CSV.** Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
 - **Parquet.** Requisiti aggiuntivi per gli oggetti Parquet:
 - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
 - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.

- Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.
- La lunghezza massima dell'espressione SQL è di 256 KB.
- Ogni record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi della richiesta CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Esempio di sintassi della richiesta Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Esempio di query SQL

Questa query ricava il nome dello stato, la popolazione del 2010, la popolazione stimata del 2015 e la percentuale di variazione dai dati del censimento degli Stati Uniti. I record nel file che non sono stati vengono ignorati.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Le prime righe del file da interrogare, SUB-EST2020_ALL.csv, assomiglia a questo:

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Esempio di utilizzo di AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Le prime righe del file di output, changes.csv, assomiglia a questo:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Esempio di utilizzo di AWS-CLI (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV": {}}' changes.csv
```

Le prime righe del file di output, changes.csv, hanno questo aspetto:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Informazioni sul copyright

Copyright © 2025 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.