



# **Operazioni sugli oggetti**

## StorageGRID

NetApp  
October 03, 2025

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-116/s3/using-s3-object-lock.html> on October 03, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Sommario

Operazioni sugli oggetti .....	1
USA blocco oggetti S3 .....	5
Attiva il blocco oggetti S3 per il bucket .....	5
Determinare se il blocco oggetti S3 è attivato per il bucket .....	5
Creare un oggetto con le impostazioni di blocco oggetti S3 .....	5
Aggiornare le impostazioni di blocco oggetti S3 .....	6
USA S3 Select .....	7
Clausole .....	7
Tipi di dati .....	7
Operatori .....	8
Funzioni di aggregazione .....	8
Funzioni condizionali .....	9
Funzioni di conversione .....	9
Funzioni di data .....	9
Funzioni di stringa .....	9
Utilizzare la crittografia lato server .....	9
Utilizzare SSE .....	10
Utilizzare SSE-C .....	10
Considerazioni sull'utilizzo della crittografia lato server con le chiavi fornite dal cliente (SSE-C) .....	11
OTTIENI oggetto .....	12
OTTIENI oggetti oggetto e multipart .....	12
Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C) .....	12
UTF-8 caratteri nei metadati dell'utente .....	12
Intestazione della richiesta non supportata .....	12
Versione .....	12
Comportamento di GET Object per gli oggetti Cloud Storage Pool .....	13
Oggetti multipart o segmentati in un pool di storage cloud .....	13
Oggetto TESTA .....	14
OGGETTI TESTA e multipart .....	14
Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C) .....	14
UTF-8 caratteri nei metadati dell'utente .....	14
Intestazione della richiesta non supportata .....	14
Intestazioni di risposta per gli oggetti del Cloud Storage Pool .....	15
Oggetti multipart o segmentati nel Cloud Storage Pool .....	16
Versione .....	16
RIPRISTINO POST-oggetto .....	16
Tipo di richiesta supportato .....	17
Versione .....	17
Comportamento del ripristino degli oggetti POST sugli oggetti del Cloud Storage Pool .....	17
METTI oggetto .....	18
Risolvi i conflitti .....	18

Dimensione dell'oggetto . . . . .	19
Dimensione dei metadati dell'utente . . . . .	19
UTF-8 caratteri nei metadati dell'utente . . . . .	19
Limiti tag oggetto . . . . .	19
Proprietà degli oggetti . . . . .	19
Intestazioni di richiesta supportate . . . . .	19
Intestazioni di richiesta non supportate . . . . .	21
Opzioni di classe storage . . . . .	21
Intestazioni di richiesta per la crittografia lato server . . . . .	22
Versione . . . . .	22
<b>METTI oggetto - Copia</b> . . . . .	23
Risvolvi i conflitti . . . . .	23
Dimensione dell'oggetto . . . . .	23
UTF-8 caratteri nei metadati dell'utente . . . . .	23
Intestazioni di richiesta supportate . . . . .	23
Intestazioni di richiesta non supportate . . . . .	25
Opzioni di classe storage . . . . .	25
Utilizzo di x-amz-copy-source in PUT Object - Copy . . . . .	25
Intestazioni di richiesta per la crittografia lato server . . . . .	26
Versione . . . . .	26
<b>SelectObjectContent</b> . . . . .	27
Esempio di sintassi della richiesta . . . . .	27
Esempio di query SQL . . . . .	28
Esempio di utilizzo di AWS-CLI . . . . .	29

# Operazioni sugli oggetti

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

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

- StorageGRID [controlli di coerenza](#) sono supportate da tutte le operazioni sugli oggetti, ad eccezione di quanto segue:
  - GET Object ACL (OTTIENI ACL oggetto)
  - OPTIONS /
  - METTERE in attesa legale l'oggetto
  - METTI la conservazione degli oggetti
  - SELEZIONARE il contenuto dell'oggetto
- 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.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.
- Non è possibile accedere agli oggetti dati acquisiti nel sistema StorageGRID tramite Swift tramite S3.

Nella tabella seguente viene descritto il modo in cui StorageGRID implementa le operazioni degli oggetti API REST S3.

Operazione	Implementazione
ELIMINA oggetto	<p>Autenticazione multifattore (MFA) e intestazione della risposta <code>x-amz-mfa</code> non sono supportati.</p> <p>Durante l'elaborazione di una richiesta DI ELIMINAZIONE degli oggetti, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione non è temporaneamente disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.</p> <p><b>Versione</b></p> <p>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 in modo permanente la versione. Se il <code>versionId</code> corrisponde a un indicatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene restituito impostato su <code>true</code>.</p> <ul style="list-style-type: none"> <li>• Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket abilitato alla versione, si ottiene la generazione di un indicatore di eliminazione. Il <code>versionId</code> per il contrassegno di eliminazione viene restituito utilizzando <code>x-amz-version-id</code> intestazione della risposta e la <code>x-amz-delete-marker</code> l'intestazione della risposta viene restituita impostata su <code>true</code>.</li> <li>• Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket sospeso della versione, si ottiene una cancellazione permanente di una versione 'null' già esistente o di un marker di eliminazione 'null' e la generazione di un nuovo marker di eliminazione 'null'. Il <code>x-amz-delete-marker</code> l'intestazione della risposta viene restituita impostata su <code>true</code>.</li> </ul> <p><b>Nota:</b> In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione.</p>
ELIMINARE più oggetti	<p>Autenticazione multifattore (MFA) e intestazione della risposta <code>x-amz-mfa</code> non sono supportati.</p> <p>È possibile eliminare più oggetti nello stesso messaggio di richiesta.</p>

Operazione	Implementazione
ELIMINA tag oggetti	<p>Utilizza tagging sottorisorsa per rimuovere tutti i tag da un oggetto. Implementato con tutti i comportamenti REST API di Amazon S3.</p> <p><b>Versione</b></p> <p>Se il <code>versionId</code> il parametro 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 indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione risposta impostata su <code>true</code>.</p>
OTTIENI oggetto	<p><a href="#">OTTIENI oggetto</a></p>
GET Object ACL (OTTIENI ACL oggetto)	<p>Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario dell'oggetto, indicando che il proprietario dispone dell'accesso completo all'oggetto.</p>
OTTENERE un blocco legale degli oggetti	<p><a href="#">USA blocco oggetti S3</a></p>
OTTIENI la conservazione degli oggetti	<p><a href="#">USA blocco oggetti S3</a></p>
OTTIENI tag di oggetti	<p>Utilizza tagging sottorisorsa per restituire tutti i tag per un oggetto. Implementato con tutti i comportamenti REST API di Amazon S3</p> <p><b>Versione</b></p> <p>Se il <code>versionId</code> il parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag della versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione risposta impostata su <code>true</code>.</p>
Oggetto TESTA	<p><a href="#">Oggetto TESTA</a></p>
RIPRISTINO POST-oggetto	<p><a href="#">RIPRISTINO POST-oggetto</a></p>
METTI oggetto	<p><a href="#">METTI oggetto</a></p>
METTI oggetto - Copia	<p><a href="#">METTI oggetto - Copia</a></p>
METTERE in attesa legale l'oggetto	<p><a href="#">USA blocco oggetti S3</a></p>

Operazione	Implementazione
METTI la conservazione degli oggetti	<p><a href="#">USA blocco oggetti S3</a></p>
INSERIRE tag degli oggetti	<p>Utilizza tagging sottorisorsa per aggiungere un set di tag a un oggetto esistente. Implementato con tutti i comportamenti REST API di Amazon S3</p> <p><b>Limiti tag oggetto</b></p> <p>È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole.</p> <p><b>Aggiornamenti dei tag e comportamento di acquisizione</b></p> <p>Quando si utilizza IL tag PUT Object per aggiornare i tag di un oggetto, StorageGRID non reinserisce l'oggetto. Ciò significa che l'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono 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 Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.</p> <p><b>Risoluzione dei conflitti</b></p> <p>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.</p> <p><b>Versione</b></p> <p>Se il <code>versionId</code> il parametro query 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 indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione risposta impostata su <code>true</code>.</p>

## Informazioni correlate

[Operazioni S3 monitorate nei registri di audit](#)

# USA 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 e specificare i periodi di conservazione predefiniti per ciascun bucket o le impostazioni di conservazione fino alla data e alle condizioni legali specifiche per ciascuna versione di oggetto aggiunta a tale bucket.

S3 Object Lock consente di specificare le impostazioni a livello di oggetto per impedire che gli oggetti vengano cancellati o sovrascritti per un periodo di tempo fisso o indefinito.

La funzione blocco oggetto StorageGRID S3 offre una singola modalità di conservazione equivalente alla modalità di conformità Amazon S3. Per impostazione predefinita, una versione dell'oggetto protetto non può essere sovrascritta o eliminata da alcun utente. La funzione blocco oggetti di StorageGRID S3 non supporta una modalità di governance e non consente agli utenti con autorizzazioni speciali di ignorare le impostazioni di conservazione o di eliminare gli oggetti protetti.

## Attiva il blocco oggetti S3 per il 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. È possibile utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager.

### [USA account tenant](#)

- Creare il bucket utilizzando una richiesta PUT bucket con `x-amz-bucket-object-lock-enabled` intestazione della richiesta.

### [Operazioni sui bucket](#)

Non è possibile aggiungere o disattivare il blocco oggetti S3 dopo la creazione del bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea il bucket.

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni S3 Object Lock. StorageGRID supporta i periodi di conservazione predefiniti per gli oggetti nei bucket blocco oggetti S3 e supporta l'operazione DEL bucket DI configurazione BLOCCO oggetti PUT. Il `s3:object-lock-remaining-retention-days` policy condition key imposta i periodi di conservazione minimi e massimi consentiti per gli oggetti.

## Determinare se il blocco oggetti S3 è attivato per il bucket

Per determinare se il blocco oggetti S3 è attivato, utilizzare [OTTIENI configurazione blocco oggetto](#) richiesta.

## Creare un oggetto con le impostazioni di blocco oggetti S3

Per specificare le impostazioni di blocco oggetti S3 quando si aggiunge una versione di oggetto a un bucket con blocco oggetti S3 attivato, eseguire una richiesta PUT object, PUT object - Copy o avviare la richiesta di caricamento multiparte. Utilizzare le seguenti intestazioni di richiesta.



È necessario attivare il blocco oggetti S3 quando si crea un bucket. Non è possibile aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

- `x-amz-object-lock-mode`, Che deve essere CONFORME (distinzione tra maiuscole e minuscole).



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 multipart.
- 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.
- Una successiva richiesta DI versione DELL'oggetto DELETE o di versioni DELL'oggetto DELETE avrà esito negativo se è precedente alla data di conservazione o se è attiva una conservazione a fini giudiziari.

## Aggiornare le impostazioni di blocco oggetti S3

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 deve essere COMPLIANCE (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.

## Informazioni correlate

[Gestire gli oggetti con ILM](#)

[USA account tenant](#)

[METTI oggetto](#)

[METTI oggetto - Copia](#)

[Avvia caricamento multiparte](#)

[Versione degli oggetti](#)

["Amazon Simple Storage Service User Guide \(Guida utente di Amazon Simple Storage Service\): Utilizzo di S3 Object Lock"](#)

## USA S3 Select

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



Gli elementi non elencati non sono supportati.

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

Solo gli account tenant con S3 Select abilitato possono eseguire query SelectObjectContent. Vedere [Considerazioni e requisiti per l'utilizzo di S3 Select](#).

## Clausole

- SELEZIONARE l'elenco
- CLAUSOLA FROM
- Clausola WHERE
- Clausola LIMIT

## Tipi di dati

- bool
- intero
- stringa
- fluttuare
- decimale, numerico
- data e ora

## Operatori

### Operatori logici

- E.
- NO
- OPPURE

### Operatori di confronto

- <
- >
- $\Leftarrow$
- $\geq$
- =
- =
- $\neq$
- !=
- TRA
- POLL

### Operatori di corrispondenza dei modelli

- MI PIACE
- \_
- %

### Operatori unitari

- È NULL
- NON È NULL

### Operatori matematici

- +
- -
- \*
- /
- %

StorageGRID segue la precedenza dell'operatore di selezione di AWS S3.

### Funzioni di aggregazione

- MEDIA()

- CONTEGGIO(\*)
- MAX()
- MIN()
- SOMMA()

## Funzioni condizionali

- CASO
- COALESCE
- NULLIF

## Funzioni di conversione

- CAST (per il tipo di dati supportato)

## Funzioni di data

- DATA\_ADD
- DATA\_DIFF
- ESTRARRE
- TO\_STRING
- TO\_TIMESTAMP
- UTCNOW

## Funzioni di stringa

- CHAR\_LENGTH, CHARACTER\_LENGTH
- ABBASSARE
- SOTTOSTRINGA
- TAGLIARE
- SUPERIORE

## Utilizzare la crittografia lato server

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

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni che si escludono a vicenda, in base alla modalità di gestione delle chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite da StorageGRID)**: Quando si invia una richiesta S3 per memorizzare 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 decrittare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente)**: Quando si invia una richiesta S3 per memorizzare un oggetto, viene fornita la propria chiave di crittografia. Quando si recupera un oggetto, si

fornisce la stessa chiave di crittografia come parte della 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 decifratura 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 l'oggetto corrispondente.



Se un oggetto viene 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 a oggetti:

- METTI oggetto
- METTI oggetto - Copia
- Avvia caricamento multipart

## Utilizzare SSE-C.

Per crittografare un oggetto con una chiave univoca gestita, vengono utilizzate tre intestazioni di richiesta:

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

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

- OTTIENI oggetto
- Oggetto TESTA
- METTI oggetto

- METTI oggetto - Copia
- Avvia caricamento multiparte
- Carica parte
- Carica parte - Copia

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

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

- È necessario utilizzare https.



StorageGRID rifiuta qualsiasi richiesta effettuata su http quando si utilizza SSE-C. Per motivi di sicurezza, è consigliabile considerare compromessa qualsiasi chiave inviata accidentalmente utilizzando http. Eliminare la chiave e ruotarla in base alle necessità.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire il mapping delle chiavi di crittografia agli oggetti. StorageGRID non memorizza le chiavi di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia che fornisce per ciascun oggetto.
- Se il bucket è abilitato per la versione, ogni versione dell'oggetto deve disporre di una propria chiave di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia utilizzata per ciascuna versione dell'oggetto.
- Poiché si gestiscono le chiavi di crittografia sul lato client, è necessario gestire anche eventuali protezioni 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 l'oggetto corrispondente.

- Se la replica CloudMirror è configurata per il bucket, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non riesce.

### Informazioni correlate

[OTTIENI oggetto](#)

[Oggetto TESTA](#)

[METTI oggetto](#)

[METTI oggetto - Copia](#)

[Avvia caricamento multiparte](#)

[Carica parte](#)

[Carica parte - Copia](#)

["Amazon S3 Developer Guide: Protezione dei dati mediante crittografia lato server con chiavi di crittografia fornite dal cliente \(SSE-C\)"](#)

## OTTIENI oggetto

È possibile utilizzare la richiesta di oggetti GET S3 per recuperare un oggetto da un bucket S3.

## OTTIENI oggetti oggetto e multipart

È possibile utilizzare `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multipart o segmentato. Il `x-amz-mp-parts-count` l'elemento response indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` a 1 per oggetti segmentati/multiparte e non segmentati/non multipart; tuttavia, il `x-amz-mp-parts-count` l'elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

## Intestazioni delle richieste 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 fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare 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 l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, consultare le considerazioni in "Usa crittografia lato server".

## UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. LE richieste GET per un oggetto con caratteri UTF-8 escapati 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 non supportata

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

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

## Versione

Se si seleziona `versionId` la sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "Not Found" (non trovato) con `x-amz-delete-marker` intestazione risposta impostata su `true`.

## Comportamento di GET Object per gli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un Cloud Storage Pool (vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni), il comportamento di una richiesta DI un oggetto GET dipende dallo stato dell'oggetto. Per ulteriori informazioni, consulta "HEAD Object".



Se un oggetto viene memorizzato in un Cloud Storage Pool e una o più copie dell'oggetto sono presenti anche nella griglia, LE richieste GET Object tenteranno di recuperare i dati dalla griglia, prima di recuperarli dal Cloud Storage Pool.

Stato dell'oggetto	Comportamento dell'oggetto GET
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Viene recuperata una copia dell'oggetto.
Oggetto sottoposto a transizione in uno stato non recuperabile	403 Forbidden, InvalidObjectState Utilizzare una richiesta DI ripristino dell'oggetto POST per ripristinare lo stato recuperabile dell'oggetto.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden, InvalidObjectState Attendere il completamento della richiesta DI ripristino dell'oggetto POST.
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Viene recuperata una copia dell'oggetto.

## Oggetti multipart o segmentati in un pool di storage cloud

Se hai caricato un oggetto multipart o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, la richiesta DI un oggetto GET potrebbe non essere restituita correttamente 200 OK quando alcune parti dell'oggetto sono già state trasferite in uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

In questi casi:

- La richiesta DELL'oggetto GET potrebbe restituire alcuni dati ma arrestarsi a metà del trasferimento.
- Potrebbe essere restituita una richiesta successiva di oggetto GET 403 Forbidden.

### Informazioni correlate

[Utilizzare la crittografia lato server](#)

Gestire gli oggetti con ILM

RIPRISTINO POST-oggetto

Operazioni S3 monitorate nei registri di audit

## Oggetto TESTA

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

### OGGETTI TESTA e multiparte

È possibile utilizzare `partNumber` richiedi il parametro per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. Il `x-amz-mp-parts-count` l'elemento response indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` a 1 per oggetti segmentati/multiparte e non segmentati/non multiparte; tuttavia, il `x-amz-mp-parts-count` l'elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

### Intestazioni delle richieste 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 fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare 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 l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, consultare le considerazioni in "Usa crittografia lato server".

### UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. Le richieste HEAD per un oggetto con caratteri UTF-8 escapati 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 non supportata

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

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

## Intestazioni di risposta per gli oggetti del Cloud Storage Pool

Se l'oggetto viene memorizzato in un Cloud Storage Pool (vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni), vengono restituite le seguenti intestazioni di risposta:

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

Le intestazioni delle risposte forniscono informazioni sullo stato di un oggetto quando viene spostato in un Cloud Storage Pool, facoltativamente trasferito in uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta all'oggetto HEAD
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK (Non viene restituita alcuna intestazione di risposta speciale).
Oggetto nel Cloud Storage Pool ma non ancora passato 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>  Fino a quando l'oggetto non passa a uno stato non recuperabile, il valore per <code>expiry-date</code> è impostato su un periodo di tempo lontano in futuro. L'ora esatta della transizione non è controllata dal sistema StorageGRID.
L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella 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 impostato su un periodo di tempo lontano in futuro.  <b>Nota:</b> Se la copia sulla griglia non è disponibile (ad esempio, un nodo di storage è inattivo), è necessario eseguire una richiesta DI ripristino DELL'oggetto POST per ripristinare la copia dal pool di storage cloud prima di poter recuperare l'oggetto.
L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella griglia	200 OK  <code>x-amz-storage-class: GLACIER</code>

Stato dell'oggetto	Risposta all'oggetto HEAD
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 2018 00:00:00 GMT" Il expiry-date Indica quando l'oggetto nel Cloud Storage Pool verrà riportato in uno stato non recuperabile.

## Oggetti multipart o segmentati nel Cloud Storage Pool

Se hai caricato un oggetto multipart o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, la richiesta di un oggetto HEAD potrebbe non essere corretta x-amz-restore: ongoing-request="false" quando alcune parti dell'oggetto sono già state trasferite in uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

## Versione

Se si seleziona `versionId` la sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "Not Found" (non trovato) con `x-amz-delete-marker` intestazione risposta impostata su `true`.

### Informazioni correlate

[Utilizzare la crittografia lato server](#)

[Gestire gli oggetti con ILM](#)

[RIPRISTINO POST-oggetto](#)

[Operazioni S3 monitorate nei registri di audit](#)

## RIPRISTINO POST-oggetto

È possibile utilizzare la richiesta di ripristino dell'oggetto POST S3 per ripristinare un oggetto memorizzato in un Cloud Storage Pool.

## **Tipo di richiesta supportato**

StorageGRID supporta solo le richieste DI ripristino degli oggetti POST per ripristinare un oggetto. Non supporta SELECT tipo di ripristino. Selezionare Requests Return XNot Implemented.

## **Versione**

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

## **Comportamento del ripristino degli oggetti POST sugli oggetti del Cloud Storage Pool**

Se un oggetto è stato memorizzato in un Cloud Storage Pool (vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni), una richiesta DI ripristino DELL'oggetto POST ha il seguente comportamento, in base allo stato dell'oggetto. Per ulteriori informazioni, consulta "HEAD Object".



Se un oggetto viene memorizzato in un Cloud Storage Pool e una o più copie dell'oggetto sono presenti anche nella griglia, non è necessario ripristinare l'oggetto emettendo una richiesta DI ripristino POST-oggetto. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

<b>Stato dell'oggetto</b>	<b>Comportamento del ripristino degli oggetti POST</b>
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	403 Forbidden, InvalidObjectState
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Non vengono apportate modifiche. <b>Nota:</b> Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificarne lo stato <code>expiry-date</code> .

Stato dell'oggetto	Comportamento del ripristino degli oggetti POST
Oggetto sottoposto a transizione in 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 viene riportato in uno stato non recuperabile.</p> <p>In alternativa, utilizzare <code>Tier</code> elemento <code>request</code> per determinare il tempo necessario per il completamento del processo di ripristino (Expedited, Standard, o Bulk). Se non si specifica <code>Tier</code>, il Standard viene utilizzato il tier.</p> <p><b>Attenzione:</b> Se un oggetto è stato spostato in S3 Glacier Deep Archive o il Cloud Storage Pool utilizza Azure Blob Storage, non è possibile ripristinarlo utilizzando Expedited tier. Viene visualizzato il seguente errore 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</p>
Oggetto in fase di ripristino da uno stato non recuperabile	409 Conflict, <code>RestoreAlreadyInProgress</code>
Oggetto completamente ripristinato nel Cloud Storage Pool	<p>200 OK</p> <p><b>Nota:</b> se un oggetto è stato ripristinato a uno stato recuperabile, è possibile modificarne lo stato <code>expiry-date</code> Inviando nuovamente la richiesta DI ripristino dell'oggetto POST con un nuovo valore per <code>Days</code>. La data di ripristino viene aggiornata in relazione all'ora della richiesta.</p>

#### Informazioni correlate

[Gestire gli oggetti con ILM](#)

[Oggetto TESTA](#)

[Operazioni S3 monitorate nei registri di audit](#)

## METTI oggetto

È possibile utilizzare la richiesta di oggetti PUT S3 per aggiungere un oggetto a un bucket.

#### Risolvi i conflitti

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.

## Dimensione dell'oggetto

La dimensione massima *consigliata* per un'operazione di singolo oggetto PUT è 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multipart.



In StorageGRID 11.6, la dimensione massima *supportata* per un'operazione di singolo oggetto PUT è 5 TiB (5,497,558,138,880 byte). Tuttavia, l'avviso **S3 PUT object size too large** (DIMENSIONE oggetto ECCESSIVA) viene attivato se si tenta di caricare un oggetto che supera i 5 GiB.

## Dimensione dei metadati dell'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 dell'utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata prendendo la somma del numero di byte nella codifica UTF-8 di ogni chiave e valore.

## UTF-8 caratteri nei metadati dell'utente

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

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

- LE richieste PUT, PUT Object-Copy, GET e HEAD hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapati.
- StorageGRID non restituisce `x-amz-missing-meta` header se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

## Limiti tag oggetto

È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoci. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole.

## Proprietà degli oggetti

In StorageGRID, tutti gli oggetti sono di proprietà dell'account del proprietario del bucket, inclusi 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 si specifica `aws-chunked` per Content-Encoding StorageGRID non verifica i seguenti elementi:

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

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

- 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 **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare creation-time come nome dei metadati che registrano quando l'oggetto è stato creato. Ad esempio:

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

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



Una regola ILM non può utilizzare sia un **tempo di creazione definito dall'utente** per il tempo di riferimento sia le opzioni bilanciate o rigide per il comportamento di Ingest. Quando viene creata la regola ILM viene restituito un errore.

- x-amz-tagging
- Intestazioni di richiesta blocco 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, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la versione dell'oggetto che resta aggiornata.

## USA blocco oggetti S3

- Intestazioni di richiesta 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:

- Il x-amz-acl intestazione della richiesta non supportata.
- Il x-amz-website-redirect-location l'intestazione della richiesta non è supportata e restituisce XNotImplemented.

## Opzioni di classe storage

Il x-amz-storage-class l'intestazione della richiesta è supportata. 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 memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza l'opzione Strict per il comportamento Ingest, l' x-amz-storage-class l'intestazione non ha alcun effetto.

È possibile utilizzare i seguenti valori per x-amz-storage-class:

- STANDARD (Impostazione predefinita)
  - **Doppio commit:** Se la regola ILM specifica l'opzione doppio commit per il comportamento di Ingest, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita in un nodo di storage diverso (doppio commit). Una volta valutato l'ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.
  - **Balanced:** Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

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

- REDUCED\_REDUNDANCY
  - **Commit doppio:** Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
  - **Balanced:** Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. Il REDUCED\_REDUNDANCY L'opzione è preferibile quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando REDUCED\_REDUNDANCY

elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

Utilizzando il REDUCED\_REDUNDANCY l'opzione non è consigliata in altre circostanze.

REDUCED\_REDUNDANCY aumenta il rischio di perdita dei dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.

**Attenzione:** Avere una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Specificare 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 eseguite quando l'oggetto viene valutato dal criterio ILM attivo e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

**Nota:** Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, il REDUCED\_REDUNDANCY l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il REDUCED\_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-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 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
- **SSE-C:** Utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.
  - x-amz-server-side-encryption-customer-algorithm: Specificare AES256.
  - x-amz-server-side-encryption-customer-key: Specificare 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.

**Attenzione:** le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, consultare le considerazioni in "Usa crittografia lato server".

**Nota:** se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

## Versione

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

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

#### Informazioni correlate

[Gestire gli oggetti con ILM](#)

[Operazioni sui bucket](#)

[Operazioni S3 monitorate nei registri di audit](#)

[Utilizzare la crittografia lato server](#)

[Come configurare le connessioni client](#)

## METTI oggetto - Copia

È possibile utilizzare la richiesta S3 PUT Object - Copy per creare una copia di un oggetto già memorizzato in S3. Un'operazione PUT object - Copy equivale all'esecuzione di UN'OPERAZIONE GET e poi PUT.

#### Risolvi i conflitti

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.

#### Dimensione dell'oggetto

La dimensione massima *consigliata* per un'operazione di singolo oggetto PUT è 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multipart.

 In StorageGRID 11.6, la dimensione massima *supportata* per un'operazione di singolo oggetto PUT è 5 TiB (5,497,558,138,880 byte). Tuttavia, l'avviso **S3 PUT object size too large** (DIMENSIONE oggetto ECCESSIVA) viene attivato se si tenta di caricare un oggetto che supera i 5 GiB.

#### UTF-8 caratteri nei metadati dell'utente

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

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

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapati.
- StorageGRID non restituisce `x-amz-missing-meta` header 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.

È possibile 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.

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

- Intestazioni della richiesta di blocco 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, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la versione dell'oggetto che resta aggiornata.

## USA blocco oggetti S3

- Intestazioni di richiesta 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

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

## Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

## Opzioni di classe storage

Il x-amz-storage-class L'intestazione della richiesta è supportata e influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM corrispondente specifica un comportamento di Ingest di doppio commit o bilanciato.

- STANDARD

(Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- REDUCED\_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.



Se si sta inserendo un oggetto in un bucket con il blocco oggetti S3 attivato, il REDUCED\_REDUNDANCY l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il REDUCED\_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

## Utilizzo di x-amz-copy-source in PUT Object - Copy

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

Se l'origine 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 reinserirà l'oggetto. Questo ha due conseguenze importanti:

- Non è possibile utilizzare PUT Object - Copy per crittografare un oggetto esistente o per modificare la crittografia di un oggetto esistente. Se si fornisce x-amz-server-side-encryption o il x-amz-server-side-encryption-customer-algorithm Intestazione, StorageGRID rifiuta la richiesta e restituisce XNotImplemented.
- L'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono 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 Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.

## Intestazioni di richiesta per la crittografia lato server

Se si utilizza la crittografia lato server, le intestazioni delle richieste fornite dipendono dalla crittografia dell'oggetto di origine e dalla crittografia dell'oggetto di destinazione.

- Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le seguenti tre intestazioni nella richiesta PUT Object - Copy, in modo che l'oggetto possa essere decrittato e quindi copiato:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` Specificare AES256.
  - `x-amz-copy-source-server-side-encryption-customer-key` Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto di origine.
- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca che si fornisce e si gestisce, includere 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.

**Attenzione:** le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, consultare le considerazioni in "Usa crittografia lato server".

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da SSE (StorageGRID), includere questa intestazione nella richiesta PUT Object - Copy:
  - `x-amz-server-side-encryption`

**Nota:** la `server-side-encryption` impossibile aggiornare il valore dell'oggetto. Invece, fare una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive: REPLACE`.

## Versione

Se il bucket di origine è configurato con la versione, 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 configurato con la versione, la versione generata viene restituita in `x-amz-version-id` intestazione della risposta. Se il controllo delle versioni viene sospeso per il bucket di destinazione, allora `x-amz-version-id` restituisce un valore "null".

### Informazioni correlate

[Gestire gli oggetti con ILM](#)

[Utilizzare la crittografia lato server](#)

[Operazioni S3 monitorate nei registri di audit](#)

[METTI oggetto](#)

## SelectObjectContent

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

Per ulteriori informazioni, consultare ["Documentazione AWS per SelectObjectContent"](#).

### Di cosa hai bisogno

- L'account tenant dispone dell'autorizzazione S3 Select.
- Lo hai fatto s3:GetObject autorizzazione per l'oggetto che si desidera sottoporre a query.
- L'oggetto che si desidera sottoporre a query è in formato CSV oppure è un file compresso GZIP o BZIP2 contenente un file in formato CSV.
- L'espressione SQL ha una lunghezza massima di 256 KB.
- Qualsiasi record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

### Esempio di sintassi della richiesta

```

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 query SQL

Questa query ottiene il nome dello stato, 2010 popolazioni, 2015 popolazioni stimate e la percentuale di cambiamento rispetto ai 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, ad esempio:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME, CENSUS2010POP, ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIMATE2013,POPESTIMATE2014, POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMATE2019,POPESTIMATE042020, POPESTIMATE2020 040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4799642,4816632,4831586, 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

```
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, ad esempio:

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 COMMERCIALITÀ 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.