



Supporto per l'API REST di Amazon S3

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-120/s3/s3-rest-api-supported-operations-and-limitations.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Sommario

Supporto per l'API REST di Amazon S3	1
Operazioni supportate e limitazioni dell'API REST S3 in StorageGRID	1
Gestione delle date	1
Intestazioni di richiesta comuni	1
Intestazioni di risposta comuni	1
Come StorageGRID S3 REST API autentica le richieste	2
Usa l'intestazione HTTP Authorization	2
Usa i parametri di query	2
Operazioni di servizio supportate in StorageGRID	2
Operazioni del bucket S3 e dettagli di implementazione in StorageGRID	3
Operazioni sugli oggetti	11
Come StorageGRID implementa le operazioni S3 REST API per gli oggetti	11
Operazioni Amazon S3 Select supportate in StorageGRID	15
Come StorageGRID utilizza la crittografia lato server	18
Crea una copia di un oggetto in StorageGRID con la richiesta S3 CopyObject	20
Recupera un oggetto da un bucket in StorageGRID con la richiesta GetObject	24
Recupera metadati da un oggetto in StorageGRID con la richiesta S3 HeadObject	26
Aggiungi un oggetto a un bucket in StorageGRID con la richiesta S3 PutObject	29
Ripristina un oggetto in StorageGRID con la richiesta S3 RestoreObject	35
Filtra i dati degli oggetti in StorageGRID con la richiesta S3 SelectObjectContent	36
Operazioni per caricamenti multipart	40
Operazioni di caricamento multipart supportate in StorageGRID	40
Come StorageGRID S3 REST API completa i caricamenti multipart	41
Intestazioni e opzioni delle richieste S3 CreateMultipartUpload in StorageGRID	43
Operazione S3 ListMultipartUploads e parametri supportati in StorageGRID	46
Intestazioni di richiesta supportate e non supportate per le operazioni S3 UploadPart in StorageGRID	47
Carica una parte di un oggetto in StorageGRID con l'operazione S3 UploadPartCopy	48
Risposte di errore dell'API REST S3 di StorageGRID	49
Codici di errore API S3 supportati	49
Codici di errore personalizzati di StorageGRID	51

Supporto per l'API REST di Amazon S3

Operazioni supportate e limitazioni dell'API REST S3 in StorageGRID

Il sistema StorageGRID implementa l'API Simple Storage Service (API Version 2006-03-01) con supporto per la maggior parte delle operazioni, ma con alcune limitazioni. Devi comprendere i dettagli di implementazione quando integri applicazioni client S3 REST API.

Il sistema StorageGRID supporta sia le richieste in stile virtual hosted che quelle in stile path.

Gestione delle date

L'implementazione StorageGRID dell'API REST S3 supporta solo formati di data HTTP validi.

Il sistema StorageGRID supporta solo formati di data HTTP validi per le intestazioni che accettano valori di data. La parte oraria della data può essere specificata nel formato Greenwich Mean Time (GMT) o nel formato Universal Coordinated Time (UTC) senza offset di fuso orario (+0000 deve essere specificato). Se includi l'`x-amz-date` intestazione nella tua richiesta, questa sovrascrive qualsiasi valore specificato nell'intestazione Date della richiesta. Quando usi AWS Signature Version 4, l'`x-amz-date` intestazione deve essere presente nella richiesta firmata perché l'intestazione Date non è supportata.

Intestazioni di richiesta comuni

Il sistema StorageGRID supporta le intestazioni di richiesta comuni definite da ["Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni"](#), con una sola eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per AWS Signature Version 2 Supporto per AWS Signature Version 4, con le seguenti eccezioni: • Quando fornisci il valore effettivo del checksum del payload <code>x-amz-content-sha256</code>, il valore viene accettato senza convalida, come se il valore <code>UNSIGNED-PAYLOAD</code> fosse stato fornito per l'intestazione. Quando fornisci un valore di intestazione <code>x-amz-content-sha256</code> che implica lo streaming <code>aws-chunked</code> (ad esempio, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), le firme dei chunk non vengono verificate rispetto ai dati del chunk.

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite dal *Simple Storage Service API Reference*, con una sola eccezione.

Intestazione di risposta	Implementazione
x-amz-id-2	Non utilizzato

Come StorageGRID S3 REST API autentica le richieste

Il sistema StorageGRID supporta sia l'accesso autenticato che l'accesso anonimo agli oggetti tramite l'API S3.

L'API S3 supporta Signature version 2 e Signature version 4 per l'autenticazione delle richieste API S3.

Le richieste autenticate devono essere firmate utilizzando il tuo access key ID e la tua secret access key.

Il sistema StorageGRID supporta due metodi di autenticazione: l'`Authorization`intestazione HTTP e l'utilizzo di parametri di query.

Usa l'intestazione HTTP Authorization

L'`Authorization`intestazione HTTP viene utilizzata da tutte le operazioni API S3, tranne le richieste di accesso anonimo dove consentito dalla policy del bucket. L'`Authorization`intestazione contiene tutte le informazioni di firma necessarie per autenticare una richiesta.

Usa i parametri di query

Puoi usare i parametri di query per aggiungere informazioni di autenticazione a un URL. Questa operazione è chiamata presigning dell'URL e può essere usata per concedere accesso temporaneo a risorse specifiche. Gli utenti con l'URL presigned non hanno bisogno di conoscere la chiave di accesso segreta per accedere alla risorsa, il che ti permette di fornire accesso limitato a terze parti a una risorsa.

Operazioni di servizio supportate in StorageGRID

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBuckets (precedentemente denominato GET Service)	Implementato con tutte le funzionalità dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
Ottieni l'utilizzo dello storage	La richiesta " Ottieni l'utilizzo dello storage "StorageGRID ti indica la quantità totale di spazio di archiviazione utilizzato da un account e per ogni bucket associato all'account. Questa è un'operazione sul servizio con un percorso / e un parametro di query personalizzato (`?x-ntap-sg-usage`aggiunto).

Operazione	Implementazione
OPZIONI /	Le applicazioni client possono inviare <code>OPTIONS</code> / richieste alla porta S3 su un Storage Node, senza fornire credenziali per l'autenticazione S3, per determinare se lo Storage Node è disponibile. Puoi usare questa richiesta per il monitoraggio o per permettere ai bilanciatori di carico esterni di identificare quando uno Storage Node è inattivo.

Operazioni del bucket S3 e dettagli di implementazione in StorageGRID

Il sistema StorageGRID supporta un massimo di 5.000 bucket per ogni account tenant S3.

Ogni grid può contenere un massimo di 100.000 bucket.

Per supportare 5.000 bucket, ogni Storage Node nella griglia deve avere almeno 64 GB di RAM.

Le restrizioni sui nomi dei bucket seguono le restrizioni standard della regione AWS US, ma dovresti limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste S3 in stile virtual hosted.

Per ulteriori informazioni, consulta quanto segue:

- ["Guida utente di Amazon Simple Storage Service: quote, restrizioni e limitazioni dei bucket"](#)
- ["Configura i nomi di dominio degli endpoint S3"](#)

Le operazioni `ListObjects` (GET Bucket) e `ListObjectVersions` (GET Bucket object versions) supportano StorageGRID ["valori di coerenza"](#).

Puoi verificare se gli aggiornamenti all'ora dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket. Vedi ["Ora dell'ultimo accesso GET Bucket"](#).

La tabella seguente descrive come StorageGRID implementa le operazioni sui bucket dell'API REST di S3. Per eseguire una qualsiasi di queste operazioni, devi fornire le credenziali di accesso appropriate per l'account.

Operazione	Implementazione
CreateBucket	Crea un nuovo bucket. Creando il bucket, ne diventi il proprietario. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere univoco in ogni sistema StorageGRID (non solo all'interno dell'account del tenant). ◦ Deve essere conforme al DNS. ◦ Devi inserire almeno 3 e non più di 63 caratteri. ◦ Può essere una serie di una o più etichette, con le etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. ◦ Non deve sembrare un indirizzo IP formattato come testo. ◦ Non dovresti usare punti nelle richieste di tipo virtual hosted. I punti causano problemi con la verifica del certificato wildcard del server. • Per impostazione predefinita, i bucket vengono creati nella <code>us-east-1</code> regione; tuttavia, puoi usare l' <code>LocationConstraint</code> elemento request nel corpo della richiesta per specificare una regione diversa. Quando usi l' <code>LocationConstraint</code> elemento, devi specificare il nome esatto di una regione definita tramite Grid Manager o Grid Management API. Contatta il system administrator se non conosci il nome della regione da usare. Nota: Si verificherà un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID. • Puoi includere l' <code>`x-amz-bucket-object-lock-enabled`</code> intestazione della richiesta per creare un bucket con S3 Object Lock abilitato. Vedi "Utilizza l'API REST S3 per configurare S3 Object Lock". Devi abilitare S3 Object Lock quando crei il bucket. Non puoi aggiungere o disabilitare S3 Object Lock dopo che il bucket è stato creato. S3 Object Lock richiede il versioning del bucket, che viene abilitato automaticamente quando crei il bucket.
DeleteBucket	Elimina il bucket.
DeleteBucketCors	Elimina la configurazione CORS per il bucket.
DeleteBucketEncryption	Elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non sono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedi "Crea configurazione del ciclo di vita S3" .
DeleteBucketPolicy	Elimina la policy associata al bucket.

Operazione	Implementazione
DeleteBucketReplication	Elimina la configurazione di replica associata al bucket.
DeleteBucketTagging	Utilizza la <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un bucket. Attenzione: se per questo bucket è impostato un tag di policy ILM non predefinito, sarà presente un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag del bucket con un valore assegnato. Non inviare una richiesta <code>DeleteBucketTagging</code> se è presente un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag del bucket. Invece, invia una richiesta <code>PutBucketTagging</code> con solo il <code>NTAP-SG-ILM-BUCKET-TAG</code> tag e il valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere il <code>NTAP-SG-ILM-BUCKET-TAG</code> tag del bucket.
GetBucketAcl	Restituisce una risposta positiva e l'ID, DisplayName e Permission del proprietario del bucket, indicando che il proprietario ha pieno accesso al bucket.
GetBucketCors	Restituisce la <code>cors</code> configurazione per il bucket.
GetBucketEncryption	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (precedentemente denominato GET Bucket lifecycle)	Restituisce la configurazione del ciclo di vita per il bucket. Vedi "Crea configurazione del ciclo di vita S3" .
GetBucketLocation	Restituisce la regione impostata utilizzando l'elemento <code>LocationConstraint</code> nella richiesta <code>CreateBucket</code> . Se la regione del bucket è <code>us-east-1</code> , viene restituita una stringa vuota per la regione.
GetBucketNotificationConfiguration (precedentemente denominato GET Bucket notification)	Restituisce la configurazione delle notifiche associata al bucket.
GetBucketPolicy	Restituisce la policy associata al bucket.
GetBucketReplication	Restituisce la configurazione di replica associata al bucket.
GetBucketTagging	Utilizza la <code>tagging</code> sottorisorsa per restituire tutti i tag per un bucket. Attenzione: se per questo bucket è impostato un tag di policy ILM diverso da quello predefinito, ci sarà un tag del bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> con un valore assegnato. Non modificare o rimuovere questo tag.

Operazione	Implementazione
GetBucketVersioning	Questa implementazione utilizza la <code>versioning</code> sottorisorsa per restituire lo stato di versioning di un bucket. • <i>blank</i>: Il versioning non è mai stato abilitato (il bucket è "Non versionato") • Abilitato: la gestione delle versioni è abilitata • Sospeso: la gestione delle versioni era precedentemente abilitata ed è sospesa
GetObjectLockConfigurati on	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurati. Vedi "Utilizza l'API REST S3 per configurare S3 Object Lock".
HeadBucket	Verifica se un bucket esiste e se hai l'autorizzazione per accedervi. Questa operazione restituisce: • <code>x-ntap-sg-bucket-id</code>: L'UUID del bucket in formato UUID. • <code>x-ntap-sg-trace-id</code>: L'ID di tracciamento univoco della richiesta associata.
ListObjects e ListObjectsV2 (precedentemente denominato GET Bucket)	Restituisce alcuni o tutti (fino a 1.000) gli oggetti in un bucket. La Storage Class per gli oggetti può avere uno di due valori, anche se l'oggetto è stato acquisito con l'opzione <code>REDUCED_REDUNDANCY</code> storage class: • <code>STANDARD</code>, il che indica che l'oggetto è memorizzato in un pool di storage costituito da Storage Nodes. • <code>GLACIER</code>, il che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. Se il bucket contiene un gran numero di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune <code>CommonPrefixes</code> che non contengono chiavi. Per le richieste <code>HeadObject</code> e <code>ListObject</code>, StorageGRID restituisce i timestamp <code>LastModified</code> con precisione diversa mentre AWS restituisce i timestamp con la stessa precisione, come mostrato negli esempi seguenti: • StorageGRID <code>HeadObject</code>: "LastModified": "2024-09-26T16:43:24+00:00" • StorageGRID <code>ListObject</code>: "LastModified": "2024-09-26T16:43:24.931000+00:00" • AWS <code>HeadObject</code>: "LastModified": "2023-10-17T00:19:54+00:00" • AWS <code>ListObject</code>: "LastModified": "2023-10-17T00:19:54+00:00"

Operazione	Implementazione
ListObjectVersions (precedentemente denominate GET Bucket Object versions)	Con l'accesso in lettura a un bucket, usando questa operazione con la <code>versions</code> sottorisorsa elenca i metadati di tutte le versioni degli oggetti nel bucket.
PutBucketCors	Imposta la configurazione CORS per un bucket così che il bucket possa gestire le richieste cross-origin. La condivisione delle risorse cross-origin (CORS) è un meccanismo di sicurezza che permette alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponi di usare un bucket S3 chiamato <code>images</code> per archiviare immagini. Impostando la configurazione CORS per il bucket <code>images</code> , puoi permettere che le immagini in quel bucket vengano visualizzate sul sito web <code>http://www.example.com</code> .
PutBucketEncryption	Imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è abilitata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con chiavi gestite da StorageGRID. Quando specifichi la regola di configurazione della crittografia lato server, imposta il <code>SSEAlgorithm</code> parametro su <code>AES256</code> e non usare il parametro <code>KMSMasterKeyID</code>. La configurazione di crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include l' <code>`x-amz-server-side-encryption-*</code> intestazione di richiesta).

Operazione	Implementazione
PutBucketLifecycleConfiguration <pre>(precedentemente denominato PUT Bucket lifecycle)</pre>	Crea una nuova configurazione del ciclo di vita per il bucket o sostituisce una configurazione del ciclo di vita esistente. StorageGRID supporta fino a 1.000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML: • Scadenza (Giorni, Data, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (Prefisso, Tag) • Stato • ID StorageGRID non supporta queste azioni: • AbortIncompleteMultipartUpload • Transizione Vedi "Crea configurazione del ciclo di vita S3". Per capire come l'azione di scadenza nel ciclo di vita di un bucket interagisce con le istruzioni di posizionamento ILM, vedi "Come funziona ILM durante l'intero ciclo di vita di un oggetto". Nota: la configurazione del ciclo di vita del bucket può essere utilizzata con i bucket che hanno S3 Object Lock abilitato, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

Operazione	Implementazione
PutBucketNotificationConfiguration <pre>(precedentemente denominato PUT Bucket notification)</pre>	Configura le notifiche per il bucket utilizzando il file XML di configurazione delle notifiche incluso nel corpo della richiesta. Dovresti essere consapevole dei seguenti dettagli di implementazione: - StorageGRID supporta come destinazioni gli argomenti Amazon Simple Notification Service (Amazon SNS), gli argomenti Kafka o gli endpoint webhook. Gli endpoint Simple Queue Service (SQS) o AWS Lambda non sono supportati. - La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID. Gli endpoint possono essere creati tramite Tenant Manager o la Tenant Management API. L'endpoint deve esistere affinché la configurazione delle notifiche abbia esito positivo. Se l'endpoint non esiste, viene restituito un errore con il codice 400 <code>Bad Request InvalidArgument</code>. - Non puoi configurare una notifica per i seguenti tipi di evento. Questi tipi di evento non sono supportati. <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> - Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, tranne per il fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente: eventSource <code>sgws:s3</code> awsRegion non incluso x-amz-id-2 non incluso arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Imposta i criteri associati al bucket. Vedi "Usa le policy di accesso per bucket e gruppi" .

Operazione	Implementazione
PutBucketReplication	Configura "Replica CloudMirror di StorageGRID" per il bucket utilizzando il file XML di configurazione della replica fornito nel corpo della richiesta. Per la replica CloudMirror, dovresti tenere presente i seguenti dettagli di implementazione: • StorageGRID supporta solo la V1 della configurazione di replica. Questo significa che StorageGRID non supporta l'uso dell'elemento <code>Filter</code> per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per dettagli, vedi "Guida utente di Amazon Simple Storage Service: configurazione della replica". • La replica dei bucket può essere configurata su bucket con versione o senza versione. • Puoi specificare un bucket di destinazione diverso in ciascuna regola del file XML di configurazione della replica. Un bucket di origine può replicare su più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID come specificato in Tenant Manager o nell'API di gestione del tenant. Vedi "Configura la replica CloudMirror". L'endpoint deve esistere affinché la configurazione della replica abbia successo. Se l'endpoint non esiste, la richiesta fallisce come 400 Bad Request. Il messaggio di errore indica: Unable to save the replication policy. The specified endpoint URN does not exist: <i>URN</i>. • Non è necessario specificare un <code>Role</code> nel file XML di configurazione. Questo valore non viene utilizzato da StorageGRID e, se inviato, verrà ignorato. • Se ometti la classe di archiviazione dal file XML di configurazione, StorageGRID utilizza la classe di archiviazione <code>STANDARD</code> per impostazione predefinita. • Se elimini un oggetto dal bucket di origine o elimini il bucket di origine stesso, il comportamento della replica tra regioni è il seguente: ◦ Se elimini l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non viene replicato e non ricevi alcuna notifica. ◦ Se elimini l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento di eliminazione standard di Amazon S3 per la V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza la <code>tagging</code> sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando aggiungi tag a un bucket, tieni presente le seguenti limitazioni: • Sia StorageGRID che Amazon S3 supportano fino a 50 tag per ogni bucket. • I tag associati a un bucket devono avere chiavi tag univoche. Una chiave tag può essere lunga fino a 128 caratteri Unicode. • I valori dei tag possono avere una lunghezza massima di 256 caratteri Unicode. • La chiave e i valori fanno distinzione tra maiuscole e minuscole. Attenzione: se per questo bucket è impostato un tag di policy ILM non predefinito, ci sarà un tag di bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> con un valore assegnato. Assicurati che il tag di bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> sia incluso con il valore assegnato in tutte le richieste <code>PutBucketTagging</code>. Non modificare o rimuovere questo tag. Nota: Questa operazione sovrascrive tutti i tag attualmente presenti nel bucket. Se ometti alcuni tag esistenti dal set, quei tag verranno rimossi dal bucket.
PutBucketVersioning	Utilizza la <code>versioning</code> sottorisorsa per impostare lo stato di versioning di un bucket esistente. Puoi impostare lo stato di versioning con uno dei seguenti valori: • Abilitato: Abilita il versioning per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco. • Sospeso: Disabilita il versioning per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID di versione <code>null</code>.
PutObjectLockConfiguration	Configura o rimuove la modalità di conservazione predefinita e il periodo di conservazione predefinito del bucket. Se il periodo di conservazione predefinito viene modificato, la <code>retain-until-date</code> delle versioni degli oggetti esistenti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Consulta "Utilizza l'API REST S3 per configurare S3 Object Lock" per informazioni dettagliate.

Operazioni sugli oggetti

Come StorageGRID implementa le operazioni S3 REST API per gli oggetti

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

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

- StorageGRID "**valori di coerenza**" è supportato da tutte le operazioni sugli oggetti, ad eccezione delle seguenti:
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". Il momento in cui viene effettuata la valutazione "latest-wins" si basa su quando 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, inclusi gli oggetti creati da un utente anonimo o da un altro account.

La tabella seguente descrive come StorageGRID implementa le operazioni sugli oggetti dell'API REST di S3.

Operazione	Implementazione
DeleteObject	Quando elabora una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni di archiviazione. Se ha successo, 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 le copie in coda per la rimozione e indica comunque il successo al client. Restrizioni • L'autenticazione a più fattori (MFA) e l'intestazione di risposta <code>x-amz-mfa</code> non sono supportate. • Le <code>If-None</code> e <code>If-None-Match</code> intestazioni sono accettate ma non funzionanti. Versioning Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare la <code>versionId</code> sottorisorsa. Usando questa sottorisorsa elimini definitivamente la versione. Se <code>versionId</code> corrisponde a un marcatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene restituita impostata su <code>true</code>. • Se un oggetto viene eliminato senza la <code>versionId</code> sottorisorsa su un bucket con versioning abilitato, viene generato un marcatore di eliminazione. Il <code>versionId</code> per il marcatore di eliminazione viene restituito utilizzando l' <code>x-amz-version-id</code> intestazione di risposta e l' <code>x-amz-delete-marker</code> intestazione di risposta viene restituita impostata su <code>true</code>. • Se un oggetto viene eliminato senza la <code>versionId</code> sottorisorsa su un bucket con versioning sospeso, questo comporta l'eliminazione permanente di una versione 'null' già esistente o di un marcatore di eliminazione 'null', e la generazione di un nuovo marcatore di eliminazione 'null'. L'intestazione <code>x-amz-delete-marker</code> della risposta viene restituita impostata su <code>true</code>. Nota: In alcuni casi, potrebbero esistere più marcatori di eliminazione per un oggetto. Vedi "Utilizza l'API REST S3 per configurare S3 Object Lock" per sapere come eliminare le versioni degli oggetti in modalità GOVERNANCE.
DeleteObjects (precedentemente denominato DELETE Multiple Objects)	L'autenticazione a più fattori (MFA) e l'intestazione di risposta <code>x-amz-mfa</code> non sono supportate. Puoi eliminare più oggetti nello stesso messaggio di richiesta. Vedi "Utilizza l'API REST S3 per configurare S3 Object Lock" per sapere come eliminare le versioni degli oggetti in modalità GOVERNANCE.

Operazione	Implementazione
DeleteObjectTagging	Utilizza la <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un oggetto. Versioning Se il <code>versionId</code> parametro di query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket versionato. Se la versione corrente dell'oggetto è un delete marker, viene restituito uno stato "MethodNotAllowed" con l' <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.
GetObject	"GetObject"
GetObjectAcl	Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, DisplayName e Permission del proprietario dell'oggetto, indicando che il proprietario ha pieno accesso all'oggetto.
GetObjectLegalHold	"Utilizza l'API REST S3 per configurare S3 Object Lock"
GetObjectRetention	"Utilizza l'API REST S3 per configurare S3 Object Lock"
GetObjectTagging	Utilizza la <code>tagging</code> sottorisorsa per restituire tutti i tag relativi a un oggetto. Versioning Se il <code>versionId</code> parametro di query non è specificato nella richiesta, l'operazione restituisce tutti i tag dalla versione più recente dell'oggetto in un bucket versionato. Se la versione corrente dell'oggetto è un delete marker, viene restituito uno stato "MethodNotAllowed" con l' <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject (precedentemente denominato PUT Object - Copy)	"CopyObject"
PutObjectLegalHold	"Utilizza l'API REST S3 per configurare S3 Object Lock"
PutObjectRetention	"Utilizza l'API REST S3 per configurare S3 Object Lock"

Operazione	Implementazione
PutObjectTagging	Utilizza la <code>tagging</code> sottorisorsa per aggiungere un insieme di tag a un oggetto esistente. 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 di tag univoche. Una chiave di tag può essere lunga fino a 128 caratteri Unicode e i valori dei tag possono essere lunghi fino a 256 caratteri Unicode. Chiavi e valori fanno distinzione tra maiuscole e minuscole. Aggiornamenti dei tag e comportamento di ingestione Quando usi PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non re-ingestisce l'oggetto. Questo significa che l'opzione per Ingest Behavior specificata nella regola ILM corrispondente non viene utilizzata. Eventuali modifiche al posizionamento dell'oggetto attivate dall'aggiornamento vengono applicate 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 intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio, perché una nuova posizione richiesta non è disponibile). L'oggetto aggiornato mantiene il suo posizionamento corrente finché non è possibile effettuare il posizionamento richiesto. Risoluzione dei conflitti Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". Il momento in cui viene effettuata la valutazione "latest-wins" si basa su quando il sistema StorageGRID completa una determinata richiesta, e non su quando i client S3 iniziano un'operazione. Versioning Se il <code>versionId</code> parametro di query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket versionato. Se la versione corrente dell'oggetto è un delete marker, viene restituito uno stato "MethodNotAllowed" con l' <code>x-amz-delete-marker</code> intestazione di risposta impostata su <code>true</code>.
SelectObjectContent	" SelectObjectContent "

Operazioni Amazon S3 Select supportate in StorageGRID

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



Gli articoli non elencati non sono supportati.

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

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

Clausole

- elenco SELECT
- clausola FROM
- clausola WHERE
- clausola LIMIT

Tipi di dati

- bool
- intero
- stringa
- galleggiante
- decimale, numerico
- timestamp

Operatori

Operatori logici

- E
- NON
- O

Operatori di confronto

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

Operatori di pattern matching

- MI PIACE
- _
- %

Operatori unitari

- È NULL
- NON È NULLO

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza degli operatori di Amazon S3 Select.

Funzioni aggregate

- AVG()
- COUNT(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- \${post_edited_translations.segment}
- \${post_edited_translations.segment}
- NULLIF

Funzioni di conversione

- \${post_edited_translations.segment}

Funzioni data

- \${post_edited_translations.segment}
- \${post_edited_translations.segment}
- ESTRAI
- \${post_edited_translations.segment}
- \${post_edited_translations.segment}

- UTCNOW

Funzioni di stringa

- CHAR_LENGTH, CHARACTER_LENGTH
- \${post_edited_translations.segment}
- \${post_edited_translations.segment}
- \${post_edited_translations.segment}
- \${post_edited_translations.segment}

Come StorageGRID utilizza la crittografia lato server

La crittografia lato server ti permette di proteggere i dati degli oggetti a riposo. StorageGRID crittografa i dati mentre scrive l'oggetto e li decrittografa quando accedi all'oggetto.

Se vuoi usare la crittografia lato server, puoi scegliere una delle due opzioni che si escludono a vicenda, in base a come vengono gestite le chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite da StorageGRID):** Quando invii una richiesta S3 per archiviare un oggetto, StorageGRID crittografa l'oggetto con una chiave univoca. Quando invii una richiesta S3 per recuperare l'oggetto, StorageGRID utilizza la chiave archiviata per decrittare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente):** Quando invii una richiesta S3 per archiviare un oggetto, fornisci la tua 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 i dati dell'oggetto ti vengono restituiti.

`${post_edited_translations.segment}`



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi l'oggetto corrispondente.



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

Usa SSE

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

`x-amz-server-side-encryption`

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

- ["PutObject"](#)
- ["CopyObject"](#)
- ["CreateMultipartUpload"](#)

`${post_edited_translations.segment}`

Per crittografare un oggetto con una chiave univoca che gestisci tu, usi tre intestazioni di richiesta:

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

`${post_edited_translations.segment}`

- `"GetObject"`
- `"HeadObject"`
- `"PutObject"`
- `"CopyObject"`
- `"CreateMultipartUpload"`
- `"UploadPart"`
- `"UploadPartCopy"`

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

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`



StorageGRID rifiuta qualsiasi richiesta effettuata tramite http quando si utilizza SSE-C. Per considerazioni sulla sicurezza, dovresti considerare compromessa qualsiasi chiave inviata accidentalmente tramite http. Scarta la chiave e ruotala come opportuno.

- `${post_edited_translations.segment}`
- Devi gestire la mappatura delle chiavi di crittografia agli oggetti. StorageGRID non memorizza le chiavi di crittografia. Sei tu a dover tenere traccia della chiave di crittografia che fornisci per ogni oggetto.
- Se il tuo bucket è abilitato al controllo delle versioni, ogni versione dell'oggetto dovrebbe avere la propria chiave di crittografia. Sei responsabile del tracciamento della chiave di crittografia utilizzata per ciascuna versione dell'oggetto.
- `${post_edited_translations.segment}`



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi l'oggetto corrispondente.

- Se per il bucket è configurata la replica cross-grid o la replica CloudMirror, non puoi acquisire oggetti SSE-C. L'operazione di acquisizione non riuscirà.

Informazioni correlate

["Amazon S3 User Guide: Utilizzo della crittografia lato server con chiavi fornite dal cliente \(SSE-C\)"](#)

Crea una copia di un oggetto in StorageGRID con la richiesta S3 CopyObject

Puoi usare la richiesta S3 CopyObject per creare una copia di un oggetto già archiviato in S3. Un'operazione CopyObject è come eseguire GetObject seguita 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". Il momento in cui viene effettuata la valutazione "latest-wins" si basa su quando 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 di 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 PutObject operation è 5 TiB (5.497.558.138.880 byte).



Se hai eseguito l'aggiornamento da StorageGRID 11.6 o versioni precedenti, l'avviso "Dimensioni oggetto S3 PUT troppo grandi" verrà attivato se provi a caricare un oggetto che supera 5 GiB. Se hai una nuova installazione di StorageGRID 11.7 o 11.8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le future release di StorageGRID non supporteranno il caricamento di oggetti più grandi di 5 GiB.

Caratteri UTF-8 nei metadati utente

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

StorageGRID non analizza né interpreta i caratteri UTF-8 preceduti da escape inclusi nel nome o nel valore della chiave o dei metadati definiti dall'utente. I caratteri UTF-8 preceduti da 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 l'`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 ti permette di copiare l'oggetto e i metadati.

Puoi specificare `REPLACE` per sovrascrivere i metadati esistenti quando copi l'oggetto o per aggiornare i metadati dell'oggetto.

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

Puoi specificare `REPLACE` per sovrascrivere i tag esistenti quando copi l'oggetto o per aggiornare i tag.

- Intestazioni della richiesta S3 Object Lock:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Se una richiesta viene effettuata senza queste intestazioni, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la `retain-until-date`. Vedi ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#).

- Intestazioni della 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`

Vedi [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
- If-Match

The `If-Match` header è accettato ma non funzionale.

- If-None-Match

The `If-None-Match` header è accettato ma non funzionale.

- x-amz-checksum-algorithm

Quando copi un oggetto, se l'oggetto di origine ha un checksum, StorageGRID non copia quel valore di checksum nel nuovo oggetto. Questo comportamento si applica sia che tu provi sia che tu non provi a usare `x-amz-checksum-algorithm` nella richiesta dell'oggetto.

- x-amz-website-redirect-location

Opzioni di classe di archiviazione

L' `x-amz-storage-class` intestazione della richiesta è supportata e influisce su quante copie di oggetti StorageGRID crea se la regola ILM corrispondente utilizza il Dual commit o Balanced "opzione di ingest".

- STANDARD

(Predefinito) Specifica un'operazione di ingestione a doppio commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ripiega sulla creazione di copie intermedie.

- REDUCED_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ripiega sulla creazione di copie intermedie.



Se stai inserendo un oggetto in un bucket con S3 Object Lock abilitato, l' `REDUCED_REDUNDANCY` opzione viene ignorata. Se stai inserendo un oggetto in un bucket Compliant legacy, l' `REDUCED_REDUNDANCY` opzione restituisce un errore. StorageGRID esegue sempre un ingest con doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzando x-amz-copy-source in CopyObject

Se il bucket e la chiave di origine, specificati nell' `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 l' `x-amz-metadata-directive` header è specificato come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non re-ingestisce l'oggetto. Questo ha due importanti conseguenze:

- Non puoi usare CopyObject per crittografare un oggetto esistente sul posto o per cambiare la crittografia di un oggetto esistente sul posto. Se fornisci l' `x-amz-server-side-encryption` intestazione o l'

``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. Eventuali modifiche al posizionamento degli oggetti attivate dall'aggiornamento vengono applicate 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 intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio, perché una nuova posizione richiesta non è disponibile). L'oggetto aggiornato mantiene il suo posizionamento corrente finché non è possibile effettuare il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se usi ["usa la crittografia lato server"](#), le intestazioni di richiesta che fornisci dipendono dal fatto che l'oggetto sorgente sia crittografato e se hai intenzione di crittografare l'oggetto di destinazione.

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



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

- Se vuoi crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da StorageGRID (SSE), includi questa intestazione nella richiesta CopyObject:
 - `x-amz-server-side-encryption`



Il `server-side-encryption` valore dell'oggetto non può essere aggiornato. Invece, crea una copia con un nuovo `server-side-encryption` valore usando `x-amz-metadata-directive: REPLACE`.

Versioning

Se il bucket di origine è versionato, puoi usare l'``x-amz-copy-source`` intestazione per copiare l'ultima versione

di un oggetto. Per copiare una versione specifica di un oggetto, devi specificare esplicitamente la versione da copiare usando la ``versionId`` sottorisorsa. Se il bucket di destinazione è versionato, la versione generata viene restituita nell' ``x-amz-version-id`` intestazione della risposta. Se il versionamento è sospeso per il bucket di destinazione, allora ``x-amz-version-id`` restituisce un valore "null".

Recupera un oggetto da un bucket in StorageGRID con la richiesta `GetObject`

Puoi usare la richiesta S3 `GetObject` per recuperare un oggetto da un bucket S3.

`GetObject` e oggetti composti da più parti

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

Puoi impostare `partNumber` su 1 sia per gli oggetti segmentati/multipart che per quelli non segmentati/non multipart; tuttavia, l'elemento di risposta `x-amz-mp-parts-count` viene restituito solo per gli 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 con escape nei metadati definiti dall'utente non restituiscono l'intestazione `x-amz-missing-meta` se il nome o il valore della chiave include caratteri non stampabili.

Intestazione di richiesta supportata

La seguente intestazione di richiesta è supportata:

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

L'Range`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 di richiesta non supportata

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

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

Versioning

Se una `versionId` sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket versionato. Se la versione corrente dell'oggetto è un delete marker, viene restituito uno stato "Not Found" con l' `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)

Utilizza tutte e tre le intestazioni se l'oggetto è crittografato con una chiave univoca che hai fornito tu.

- `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
- ``x-amz-server-side-encryption-customer-key`` Specifica la tua 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 che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi anche l'oggetto corrispondente. Prima di usare chiavi fornite dal cliente per proteggere i dati degli oggetti, consulta le considerazioni in ["\\${post_edited_translations.segment}"](#).

Comportamento di GetObject per gli oggetti del cloud storage pool

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



Se un oggetto è memorizzato in un Cloud Storage Pool e una o più copie dello stesso oggetto esistono anche nella grid, le richieste GetObject tenteranno di recuperare i dati dalla grid 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 memorizzato in un pool di storage o utilizzando la codifica di cancellazione	200 OK Viene recuperata una copia dell'oggetto.
Oggetto presente nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Viene recuperata una copia dell'oggetto.
Oggetto passato a uno stato non recuperabile	403 Forbidden, InvalidObjectState Usa una richiesta "RestoreObject" per ripristinare l'oggetto in uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden, InvalidObjectState Attendi che la richiesta RestoreObject sia completata.
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Viene recuperata una copia dell'oggetto.

Oggetti multipart o segmentati in un Cloud Storage Pool

Se hai caricato un oggetto multipart 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 200 OK in modo errato quando alcune parti dell'oggetto sono già passate 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 replica cross-grid

Se usi ["federazione di grid"](#) e ["replicazione cross-grid"](#) è abilitato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta `GetObject`. La risposta include l'intestazione di risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	<code>\${post_edited_translations.segment}</code>
Fonte	• <code>\${post_edited_translations.segment}</code> • IN SOSPESO: L'oggetto non è ancora stato replicato. • ERRORE: La replica non è riuscita a causa di un errore permanente. Devi risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta l'intestazione ``x-amz-replication-status``.

Recupera metadati da un oggetto in StorageGRID con la richiesta S3 HeadObject

Puoi usare 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, puoi usare `HeadObject` per determinare lo stato di transizione dell'oggetto.

HeadObject e oggetti composti da più parti

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

Puoi impostare `partNumber` su 1 sia per gli oggetti segmentati/multipart che per quelli non segmentati/non multipart; tuttavia, l'elemento di risposta `x-amz-mp-parts-count` viene restituito solo per gli 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 HEAD per un oggetto con caratteri UTF-8 con escape nei metadati definiti dall'utente non restituiscono l'intestazione `x-amz-missing-meta` se il nome o il valore della chiave include caratteri non stampabili.

Intestazione di richiesta supportata

La seguente intestazione di richiesta è supportata:

- `x-amz-checksum-mode`

Il `partNumber` parametro e `Range` l'intestazione non sono supportati 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 di richiesta non supportata

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

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

Versioning

Se una `versionId` sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket versionato. Se la versione corrente dell'oggetto è un delete marker, viene restituito uno stato "Not Found" con l' `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)

Utilizza tutte e tre queste intestazioni se l'oggetto è crittografato con una chiave univoca che hai fornito.

- `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
- `x-amz-server-side-encryption-customer-key`: Specifica la tua 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 che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi anche l'oggetto corrispondente. Prima di usare chiavi fornite dal cliente per proteggere i dati degli oggetti, consulta le considerazioni in ["\\${post_edited_translations.segment}"](#).

HeadObject risposte per gli oggetti del cloud storage pool

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

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

Le intestazioni della risposta forniscono informazioni sullo stato di un oggetto mentre viene spostato in un Cloud Storage Pool, facoltativamente passato 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 memorizzato in un pool di storage o utilizzando la codifica di cancellazione	200 OK (Non viene restituita alcuna intestazione di risposta speciale.)
Oggetto presente nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Finché l'oggetto non passa a uno stato non recuperabile, il valore per expiry-date viene impostato su un momento lontano nel 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 ancora sulla griglia	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Il valore per expiry-date è impostato su un momento lontano nel futuro. Nota: Se la copia sulla griglia non è disponibile (ad esempio, un Storage Node non è attivo), devi inviare una richiesta "RestoreObject" per ripristinare la copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.
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"

Stato dell'oggetto	Risposta a HeadObject
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 a uno stato non recuperabile.

Oggetti multiparte o segmentati nel Cloud Storage Pool

Se hai caricato un oggetto composto da più parti 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 `x-amz-restore: ongoing-request="false"` in modo errato quando alcune parti dell'oggetto sono già passate a uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

HeadObject e replicazione cross-grid

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

Griglia	<code>\${post_edited_translations.segment}</code>
Fonte	<code>\${post_edited_translations.segment}</code> IN SOSPESO: L'oggetto non è ancora stato replicato. ERRORE: La replica non è riuscita a causa di un errore permanente. Devi risolvere l'errore.
Destinazione	REPLICA: L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta l'`x-amz-replication-status` intestazione.

Aggiungi un oggetto a un bucket in StorageGRID con la richiesta S3 PutObject

Puoi usare 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". Il momento in cui viene effettuata la valutazione "latest-wins" si basa su quando 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 di 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 PutObject operation è 5 TiB (5.497.558.138.880 byte).



Se hai eseguito l'aggiornamento da StorageGRID 11.6 o versioni precedenti, l'avviso "Dimensioni oggetto S3 PUT troppo grandi" verrà attivato se provi a caricare un oggetto che supera 5 GiB. Se hai una nuova installazione di StorageGRID 11.7 o 11.8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le future release di StorageGRID non supporteranno il caricamento di oggetti più grandi di 5 GiB.

Dimensione dei metadati utente

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

Caratteri UTF-8 nei metadati utente

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

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

- PutObject, CopyObject, GetObject e HeadObject hanno successo se i metadati definiti dall'utente includono caratteri UTF-8 con escape.
- StorageGRID non restituisce l'`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 di tag univoche. Una chiave di tag può essere lunga fino a 128 caratteri Unicode e i valori dei tag possono essere lunghi fino a 256 caratteri Unicode. Chiavi e valori fanno distinzione tra maiuscole e minuscole.

Proprietà dell'oggetto

In StorageGRID, tutti gli oggetti sono di proprietà dell'account 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 specifichi `aws-chunked` per Content-EncodingStorageGRID, non vengono verificati i seguenti elementi:

- StorageGRID non verifica il `chunk-signature` rispetto ai dati dei chunk.
- StorageGRID non verifica il valore che fornisci per `x-amz-decoded-content-length` rispetto all'oggetto.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codifica di trasferimento a blocchi è supportata se `aws-chunked` payload signing viene utilizzata anche.

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

Quando specifichi la coppia nome-valore per i metadati definiti dall'utente, usa questo formato generale:

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

Se vuoi usare l'opzione **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, devi usare `creation-time` come nome del metadato che registra quando è stato creato l'oggetto. Ad esempio:

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

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



Una regola ILM non può utilizzare contemporaneamente un **orario di creazione definito dall'utente** per l'orario di riferimento e l'opzione di ingest Bilanciata o Rigorosa. Viene restituito un errore quando viene creata la regola ILM.

- `x-amz-tagging`
- Intestazioni della richiesta S3 Object Lock
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

Se una richiesta viene effettuata 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 quale conservarlo. Vedi ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#).

- Intestazioni della 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`

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

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `If-Match`

The `If-Match` header è accettato ma non funzionale.

- `If-None-Match`

The `If-None-Match` header è accettato ma non funzionale.

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

L'`x-amz-website-redirect-location` intestazione restituisce ``XNotImplemented`.

Opzioni di classe di archiviazione

L'`x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per ``x-amz-storage-class` influisce su come StorageGRID protegge i dati degli oggetti durante l'ingest e non su quante copie persistenti dell'oggetto vengono memorizzate nel sistema StorageGRID (che è determinato da ILM).

Se la regola ILM che corrisponde a un oggetto ingerito utilizza l'opzione di ingest rigorosa, l'``x-amz-storage-class` header 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 il comportamento di acquisizione, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita a un altro Storage Node (doppio commit). Quando l'ILM viene valutato, StorageGRID

determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento nella regola. Se non lo fanno, potrebbero essere necessarie nuove copie dell'oggetto in posizioni diverse e le copie intermedie iniziali potrebbero dover essere eliminate.

- **Bilanciato:** Se la regola ILM specifica l'opzione Bilanciato e StorageGRID non può creare immediatamente tutte le copie specificate nella regola, StorageGRID crea due copie intermedie su nodi di storage diversi.

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

- **REDUCED_REDUNDANCY**

- **Doppio commit:** Se la regola ILM specifica l'opzione Doppio commit per il comportamento di acquisizione, StorageGRID crea una singola copia intermedia mentre l'oggetto viene acquisito (commit singolo).
- **Bilanciato:** Se la regola ILM specifica l'opzione Bilanciato, StorageGRID crea una singola copia intermedia solo se il sistema non può creare immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L'opzione REDUCED_REDUNDANCY è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso, usare REDUCED_REDUNDANCY elimina la creazione e l'eliminazione non necessarie di una copia aggiuntiva dell'oggetto per ogni operazione di ingest.

Usare l' REDUCED_REDUNDANCY`opzione non è consigliato in altre circostanze. REDUCED_REDUNDANCY Aumenta il rischio di perdita di dati degli oggetti durante l'ingestione. Ad esempio, potresti perdere dati se la singola copia viene inizialmente memorizzata su un Storage Node che si guasta prima che possa avvenire la valutazione ILM.



Avere una sola copia replicata per un determinato periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quell'oggetto viene perso se un Storage Node si guasta o presenta un errore significativo. Perdi anche temporaneamente l'accesso all'oggetto durante procedure di manutenzione come gli aggiornamenti.

La specifica REDUCED_REDUNDANCY influisce solo su quante copie vengono create quando un oggetto viene acquisito per la prima volta. Non influisce su quante copie dell'oggetto vengono create quando l'oggetto viene valutato dalle policy ILM attive e non comporta che i dati vengano archiviati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se stai inserendo un oggetto in un bucket con S3 Object Lock abilitato, l'`REDUCED\_REDUNDANCY`opzione viene ignorata. Se stai inserendo un oggetto in un bucket Compliant legacy, l'`REDUCED\_REDUNDANCY`opzione restituisce un errore. StorageGRID esegue sempre un ingest con doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta per la crittografia lato server

Puoi usare 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:** Usa la seguente intestazione se vuoi crittografare l'oggetto con una chiave univoca gestita da StorageGRID.
 - `x-amz-server-side-encryption`

Quando l' `x-amz-server-side-encryption` intestazione non è inclusa nella richiesta PutObject, l'"[impostazione di crittografia dell'oggetto memorizzato](#)" a livello di grid viene omesso dalla risposta PutObject.

- **SSE-C:** Utilizza tutte e tre queste intestazioni se vuoi crittografare l'oggetto con una chiave univoca che fornisci e gestisci.
 - `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
 - `x-amz-server-side-encryption-customer-key`: Specifica la tua chiave di crittografia per il nuovo oggetto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Specifica l'MD5 digest della chiave di crittografia del nuovo oggetto.



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



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

Versioning

Se il versioning è abilitato per un bucket, un identificativo univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta tramite l'intestazione di risposta `x-amz-version-id`.

Se la gestione delle versioni viene sospesa, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione con valore nullo, verrà sovrascritta.

Calcoli della firma per l'intestazione Authorization

Quando usi l' `Authorization` intestazione per autenticare le richieste, StorageGRID si differenzia da AWS nei seguenti modi:

- StorageGRID non richiede che le `host`` intestazioni siano incluse all'interno di ``CanonicalHeaders`.
- StorageGRID non richiede `Content-Type` di essere incluso all'interno di `CanonicalHeaders`.
- StorageGRID non richiede che le `x-amz-*` intestazioni siano incluse all'interno di `CanonicalHeaders`.



Come best practice, includi sempre queste intestazioni all'interno di `CanonicalHeaders` per assicurarti che vengano verificate; tuttavia, se le escludi, StorageGRID non restituisce un errore.

Per ulteriori dettagli, consultare "[Calcolo della firma per l'intestazione di autorizzazione: trasferimento del payload in un unico blocco \(AWS Signature Version 4\)](#)".

Informazioni correlate

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

Ripristina un oggetto in StorageGRID con la richiesta S3 RestoreObject

Puoi usare 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 tipo di ripristino `SELECT`. Le richieste Select restituiscono `XNotImplemented`.

Versioning

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

Comportamento di RestoreObject sugli oggetti del Cloud Storage Pool

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



Se un oggetto è archiviato in un Cloud Storage Pool e una o più copie dell'oggetto esistono anche nella grid, non è necessario ripristinare l'oggetto inviando una richiesta RestoreObject. Invece, puoi recuperare direttamente la copia locale usando una richiesta GetObject.

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto non presente in un Cloud Storage Pool	403 Forbidden, InvalidObjectState
Oggetto presente nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	<code>`200 OK`</code> Non apporti modifiche. Nota: Prima che un oggetto sia passato a uno stato non recuperabile, non puoi cambiarne <code>expiry-date</code> .
Oggetto passato a uno stato non recuperabile	<code>`202 Accepted`</code> Ripristini una copia recuperabile dell'oggetto nel Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Alla fine di questo periodo, l'oggetto torna a uno stato non recuperabile. Facoltativamente, usa l' <code>Tier</code> elemento request per determinare quanto tempo impiegherà il processo di ripristino per essere completato (<code>`Expedited`</code> , <code>Standard</code> o <code>Bulk</code>). Se non specifichi <code>Tier</code> , viene utilizzato il livello <code>Standard</code> . Importante: se un oggetto è stato migrato a S3 Glacier Deep Archive o se il Cloud Storage Pool utilizza Azure Blob storage, non puoi ripristinarlo usando il <code>Expedited</code> livello. Viene restituito il seguente errore 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto in fase di ripristino da uno stato non recuperabile	409 Conflict, RestoreAlreadyInProgress
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Nota: Se un oggetto è stato ripristinato a uno stato recuperabile, puoi modificarne <code>expiry-date</code> riemettendo la richiesta RestoreObject con un nuovo valore per <code>Days</code> . La data di ripristino viene aggiornata rispetto all'ora della richiesta.

Filtra i dati degli oggetti in StorageGRID con la richiesta S3 SelectObjectContent

Puoi usare la richiesta S3 SelectObjectContent per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL.

Per ulteriori informazioni, vedi ["Riferimento all'API di Amazon Simple Storage Service: SelectObjectContent"](#).

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Hai `s3:GetObject` l'autorizzazione per l'oggetto che vuoi interrogare.
- L'oggetto che vuoi 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 in formato Parquet. Devi specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è 512 MB.
 - Devi usare i tipi di dati specificati nello schema dell'oggetto.
 - Non puoi usare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.
- La tua espressione SQL ha una lunghezza massima di 256 KB.
- Ciascun record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi 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 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 recupera il nome dello stato, la popolazione del 2010, la popolazione stimata per il 2015 e la % di variazione dai dati del censimento statunitense. I record presenti nel file che non corrispondono a 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 si presentano così:


```
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`, si presentano così:

```
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
```

`${post_edited_translations.segment}`

```
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
```

Operazioni per caricamenti multipart

Operazioni di caricamento multiparte supportate in StorageGRID

Questa sezione descrive come StorageGRID supporta le operazioni per i caricamenti multipart.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multipart:

- Non dovresti superare 1.000 caricamenti multipart simultanei in un singolo bucket perché i risultati delle query `ListMultipartUploads` per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multipart. I client S3 devono seguire queste linee guida:
 - Ciascuna parte di un caricamento multipart deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).
 - L'ultima parte può essere inferiore a 5 MiB (5.242.880 byte).
 - In generale, le dimensioni delle parti dovrebbero essere le più grandi possibili. Ad esempio, usa parti da 5 GiB per un oggetto da 100 GiB. Poiché ogni parte è considerata un oggetto unico, usare parti di grandi dimensioni riduce il sovraccarico dei metadati di StorageGRID.
 - Per oggetti più piccoli di 5 GiB, considera di usare il caricamento non multipart.
- L'ILM viene valutato per ogni parte di un oggetto multipart durante l'ingestione e per l'oggetto nel suo complesso al termine del caricamento multipart, se la regola ILM utilizza la modalità `Balanced` o `Strict` "[opzione di ingest](#)". Dovresti sapere come questo influisce sul posizionamento di oggetti e parti:
 - Se ILM cambia durante un caricamento multipart su S3, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento. Qualsiasi parte non posizionata correttamente viene messa in coda per una nuova valutazione da parte di ILM e spostata nella

posizione corretta in un secondo momento.

- Quando valuti ILM per una parte, StorageGRID filtra in base alla dimensione della parte, non alla dimensione dell'oggetto. Questo significa che le parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo insieme. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, ogni parte da 1 GB di un caricamento multipart da 10 parti viene archiviata in DC2 all'ingest. Tuttavia, quando ILM viene valutato per l'oggetto nel suo insieme, tutte le parti dell'oggetto vengono spostate in DC1.
- Tutte le operazioni di caricamento multipart supportano StorageGRID **"valori di coerenza"**.
- Quando un oggetto viene inserito tramite caricamento multipart, **"Soglia di segmentazione dell'oggetto (1 GiB)"** non viene applicato.
- Come richiesto, puoi usare **"crittografia lato server"** con i caricamenti multipart. Per usare SSE (crittografia lato server con chiavi gestite da StorageGRID), includi l' `x-amz-server-side-encryption` header della richiesta solo nella richiesta CreateMultipartUpload. Per usare SSE-C (crittografia lato server con chiavi fornite dal cliente), specifichi le stesse tre intestazioni di richiesta della chiave di crittografia sia nella richiesta CreateMultipartUpload che in ogni successiva richiesta UploadPart.
- Un oggetto caricato in più parti viene incluso in un **"bucket branch"** se l'ingestione è stata avviata prima del timestamp Before del bucket di base, indipendentemente da quando il caricamento viene completato.

Operazione	Implementazione
AbortMultipartUpload	Implementato con tutte le funzionalità dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
CompleteMultipartUpload	Vedi "CompleteMultipartUpload"
CreateMultipartUpload (precedentemente denominato Initiate Multipart Upload)	Vedi "CreateMultipartUpload"
ListMultipartUploads	Vedi "ListMultipartUploads"
ListParts	Implementato con tutte le funzionalità dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
UploadPart	Vedi "UploadPart"
UploadPartCopy	Vedi "UploadPartCopy"

Come StorageGRID S3 REST API completa i caricamenti multiparte

L'operazione CompleteMultipartUpload completa il caricamento di un oggetto suddiviso in più parti assemblando le parti precedentemente caricate.



StorageGRID supporta valori non consecutivi in ordine crescente per il parametro di richiesta `partNumber` con CompleteMultipartUpload. Il parametro può iniziare con qualsiasi valore.

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". Il momento in cui viene effettuata la valutazione "latest-wins" si basa su quando il sistema StorageGRID completa una determinata richiesta, e non su quando i client S3 iniziano un'operazione.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

L' `x-amz-storage-class` intestazione influisce su quante copie di oggetti StorageGRID crea se la regola ILM corrispondente specifica il ["Opzione di doppio commit o di acquisizione bilanciata"](#).

- STANDARD

(Predefinito) Specifica un'operazione di ingestione a doppio commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ripiega sulla creazione di copie intermedie.

- REDUCED_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ripiega sulla creazione di copie intermedie.



Se stai inserendo un oggetto in un bucket con S3 Object Lock abilitato, l' `REDUCED_REDUNDANCY` opzione viene ignorata. Se stai inserendo un oggetto in un bucket Compliant legacy, l' `REDUCED_REDUNDANCY` opzione restituisce un errore. StorageGRID esegue sempre un ingest con doppio commit per garantire che i requisiti di conformità siano soddisfatti.



Se un caricamento in più parti non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono eliminati dal sistema.



Il ETag valore restituito non è una somma MD5 dei dati, ma segue l'implementazione dell'API di Amazon S3 del ETag valore per gli oggetti multipart.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- If-Match

The If-Match header è accettato ma non funzionale.

- If-None-Match

The If-None-Match header è accettato ma non funzionale.

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Versioning

Questa operazione completa un caricamento in più parti. Se la gestione delle versioni è abilitata per un bucket, la versione dell'oggetto viene creata al termine del caricamento in più parti.

Se il versioning è abilitato per un bucket, un identificativo univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta tramite l'intestazione di risposta `x-amz-version-id`.

Se la gestione delle versioni viene sospesa, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione con valore nullo, verrà sovrascritta.



Quando la gestione delle versioni è abilitata per un bucket, il completamento di un caricamento multipart crea sempre una nuova versione, anche se sono presenti caricamenti multipart simultanei completati sulla stessa chiave oggetto. Quando la gestione delle versioni non è abilitata per un bucket, è possibile avviare un caricamento multipart e poi far sì che un altro caricamento multipart venga avviato e completato prima sulla stessa chiave oggetto. Nei bucket senza gestione delle versioni, ha la precedenza il caricamento multipart che viene completato per ultimo.

Replica, notifica o notifica dei metadati non riuscita

Se il bucket in cui avviene il caricamento multipart è configurato per un servizio di piattaforma, il caricamento multipart ha esito positivo anche se l'azione di replica o notifica associata non riesce.

Un tenant può attivare la replica non riuscita o la notifica aggiornando i metadati o i tag dell'oggetto. Un tenant può inviare nuovamente i valori esistenti per evitare di apportare modifiche indesiderate.

Consulta ["Risolvi i problemi dei servizi della piattaforma"](#).

Intestazioni e opzioni delle richieste S3 CreateMultipartUpload in StorageGRID

L'operazione `CreateMultipartUpload` (precedentemente denominata `Initiate Multipart Upload`) avvia un caricamento multipart per un oggetto e restituisce un ID di caricamento.

L'`x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` influisce su come StorageGRID protegge i dati degli oggetti durante l'ingest e non su quante copie persistenti dell'oggetto vengono memorizzate nel sistema StorageGRID (che è determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza la modalità Strict ["opzione di ingest"](#), l'`x-amz-storage-class` 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 di acquisizione a doppio commit, non appena un oggetto viene acquisito, viene creata una seconda copia di quell'oggetto e distribuita a un nodo di archiviazione diverso (doppio commit). Quando viene valutato l'ILM, StorageGRID determina se queste

copie intermedie iniziali soddisfano le istruzioni di posizionamento nella regola. Se non lo fanno, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e potrebbe essere necessario eliminare le copie intermedie iniziali.

- **Bilanciato:** Se la regola ILM specifica l'opzione Bilanciato e StorageGRID non può creare immediatamente tutte le copie specificate nella regola, StorageGRID crea due copie intermedie su nodi di storage diversi.

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

- `REDUCED_REDUNDANCY`

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

Usare l' `REDUCED_REDUNDANCY` opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` Aumenta il rischio di perdita di dati degli oggetti durante l'ingestione. Ad esempio, potresti perdere dati se la singola copia viene inizialmente memorizzata su un Storage Node che si guasta prima che possa avvenire la valutazione ILM.



Avere una sola copia replicata per un determinato periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quell'oggetto viene perso se un Storage Node si guasta o presenta un errore significativo. Perdi anche temporaneamente l'accesso all'oggetto durante procedure di manutenzione come gli aggiornamenti.

La specifica `REDUCED_REDUNDANCY` influisce solo su quante copie vengono create quando un oggetto viene acquisito per la prima volta. Non influisce su quante copie dell'oggetto vengono create quando l'oggetto viene valutato dalle policy ILM attive e non comporta che i dati vengano archiviati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se stai inserendo un oggetto in un bucket con S3 Object Lock abilitato, l' `REDUCED_REDUNDANCY` opzione viene ignorata. Se stai inserendo un oggetto in un bucket Compliant legacy, l' `REDUCED_REDUNDANCY` opzione restituisce un errore. StorageGRID esegue sempre un ingest con doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`
- `x-amz-checksum-algorithm`

Attualmente è supportato solo il valore `SHA256` per `x-amz-checksum-algorithm`.

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

Quando specifichi la coppia nome-valore per i metadati definiti dall'utente, usa questo formato generale:

```
x-amz-meta-_name_: `value`
```

Se vuoi usare l'opzione **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, devi usare `creation-time` come nome del metadato che registra quando è stato creato l'oggetto. Ad esempio:

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

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



Aggiungere `creation-time` come metadati definiti dall'utente non è consentito se aggiungi un oggetto a un bucket con la Compliance legacy abilitata. Viene restituito un errore.

- Intestazioni della richiesta S3 Object Lock:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Se una richiesta viene effettuata senza queste intestazioni, vengono utilizzate le impostazioni di periodo di conservazione predefinite del bucket per calcolare la `retain-until-date` della versione dell'oggetto.

["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)

- Intestazioni della 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`

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



Per informazioni su come StorageGRID gestisce i caratteri UTF-8, vedi ["PutObject"](#).

Intestazioni di richiesta per la crittografia lato server

Puoi usare le seguenti intestazioni di richiesta per crittografare un oggetto multipart con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE:** Usa la seguente intestazione nella richiesta `CreateMultipartUpload` se vuoi crittografare l'oggetto con una chiave univoca gestita da `StorageGRID`. Non specificare questa intestazione in nessuna delle richieste `UploadPart`.

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

- **SSE-C:** Utilizza tutte e tre queste intestazioni nella richiesta `CreateMultipartUpload` (e in ogni richiesta `UploadPart` successiva) se vuoi crittografare l'oggetto con una chiave univoca che fornisci e gestisci tu.

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

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

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



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

Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata:

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

L'`x-amz-website-redirect-location` intestazione restituisce ``XNotImplemented`.

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

Operazione S3 `ListMultipartUploads` e parametri supportati in `StorageGRID`

L'operazione `ListMultipartUploads` elenca i caricamenti multipart in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i carichi, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

Intestazioni di richiesta supportate e non supportate per le operazioni S3 UploadPart in StorageGRID

L'operazione UploadPart carica una parte di un caricamento multipart per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- x-amz-server-side-encryption-customer-algorithm: Specifica AES256.
- x-amz-server-side-encryption-customer-key: Specifica la stessa chiave di crittografia che hai fornito nella richiesta CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Specifica lo stesso digest MD5 che hai fornito nella richiesta CreateMultipartUpload.



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi anche l'oggetto corrispondente. Prima di usare chiavi fornite dal cliente per proteggere i dati degli oggetti, consulta le considerazioni in ["\\${post_edited_translations.segment}"](#).

Se hai specificato un checksum SHA-256 durante la richiesta CreateMultipartUpload, devi includere anche la seguente intestazione di richiesta in ogni richiesta UploadPart:

- x-amz-checksum-sha256: Specifica il checksum SHA-256 per questa parte.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i carichi,

caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

Carica una parte di un oggetto in StorageGRID con l'operazione S3 UploadPartCopy

L'operazione UploadPartCopy carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione UploadPartCopy è implementata con tutto il comportamento dell'API REST di Amazon S3. Soggetta a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificato in `x-amz-copy-source-range` all'interno del sistema StorageGRID.

Sono supportate le seguenti intestazioni di richiesta:

- `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`

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
- `x-amz-server-side-encryption-customer-key`: Specifica la stessa chiave di crittografia che hai fornito nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica lo stesso digest MD5 che hai fornito nella richiesta CreateMultipartUpload.

Se l'oggetto sorgente è crittografato utilizzando una chiave fornita dal cliente (SSE-C), devi includere le seguenti tre intestazioni nella richiesta UploadPartCopy, così l'oggetto può essere decrittografato e poi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specifica AES256.
- ``x-amz-copy-source-server-side-encryption-customer-key``: Specifica la chiave di crittografia che hai fornito quando hai creato l'oggetto sorgente.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 che hai fornito quando hai creato l'oggetto sorgente.



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi anche l'oggetto corrispondente. Prima di usare chiavi fornite dal cliente per proteggere i dati degli oggetti, consulta le considerazioni in ["\\${post_edited_translations.segment}"](#).

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

Risposte di errore dell'API REST S3 di StorageGRID

Il sistema StorageGRID supporta tutte le risposte di errore standard dell'API REST S3 che si applicano. Inoltre, l'implementazione di StorageGRID aggiunge diverse risposte personalizzate.

Codici di errore API S3 supportati

Nome	stato HTTP
AccessDenied	403 Vietato
BadDigest	400 Richiesta non valida
BucketAlreadyExists	409 Conflitto
BucketNotEmpty	409 Conflitto
IncompleteBody	400 Richiesta non valida
InternalError	500 Errore interno del server
InvalidAccessKeyId	403 Vietato
InvalidArgument	400 Richiesta non valida
InvalidBucketName	400 Richiesta non valida
InvalidBucketState	409 Conflitto
InvalidDigest	400 Richiesta non valida
InvalidEncryptionAlgorithmError	400 Richiesta non valida
InvalidPart	400 Richiesta non valida
InvalidPartOrder	400 Richiesta non valida
InvalidRange	416 Intervallo richiesto non soddisfacibile

Nome	stato HTTP
InvalidRequest	400 Richiesta non valida
InvalidStorageClass	400 Richiesta non valida
InvalidTag	400 Richiesta non valida
InvalidURI	400 Richiesta non valida
KeyTooLong	400 Richiesta non valida
XML non valido	400 Richiesta non valida
MetadataTooLarge	400 Richiesta non valida
MethodNotAllowed	405 Metodo non consentito
MissingContentLength	411 Lunghezza richiesta
MissingRequestBodyError	400 Richiesta non valida
MissingSecurityHeader	400 Richiesta non valida
NoSuchBucket	404 Non trovato
NoSuchKey	404 Non trovato
NoSuchUpload	404 Non trovato
NotImplemented	501 Non implementato
NoSuchBucketPolicy	404 Non trovato
ObjectLockConfigurationNotFoundError	404 Non trovato
PreconditionFailed	412 Precondizione non soddisfatta
RequestTimeTooSkewed	403 Vietato
ServiceUnavailable	503 Servizio non disponibile
SignatureDoesNotMatch	403 Vietato
TooManyBuckets	400 Richiesta non valida

Nome	stato HTTP
UserKeyMustBeSpecified	400 Richiesta non valida

Codici di errore personalizzati di StorageGRID

Nome	Descrizione	stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket Compliant legacy	400 Richiesta non valida
XBucketPolicyParseException	Impossibile analizzare il JSON della bucket policy ricevuta.	400 Richiesta non valida
XComplianceConflict	Operazione negata a causa di impostazioni di Compliance obsolete.	403 Vietato
XComplianceRiduzioneRidondanzaVietato	La ridondanza ridotta non è consentita nel bucket Compliant legacy	400 Richiesta non valida
XMaxBucketPolicyLengthExceeded	La tua policy supera la lunghezza massima consentita per la policy del bucket.	400 Richiesta non valida
XMissingInternalRequestHeader	Manca un'intestazione in una richiesta interna.	400 Richiesta non valida
XNoSuchBucketCompliance	Il bucket specificato non ha la Compliance legacy abilitata.	404 Non trovato
XNotAcceptable	La richiesta contiene una o più intestazioni di accettazione che non possono essere soddisfatte.	406 Non accettabile
XNotImplemented	La richiesta che hai fornito implica una funzionalità che non è implementata.	501 Non implementato

Informazioni sul copyright

Copyright © 2026 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.