Supporto per Amazon S3 REST API

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

Supporto per Amazon S3 REST API

Dettagli sull'implementazione dell'API REST S3

Il sistema StorageGRID implementa l'API del servizio di storage semplice (API versione 2006-03-01) con il supporto per la maggior parte delle operazioni e con alcune limitazioni. È necessario comprendere i dettagli dell'implementazione quando si integrano le applicazioni client API REST S3.

Il sistema StorageGRID supporta sia richieste virtuali in stile host che richieste in stile percorso.

Gestione della data

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

Il sistema StorageGRID supporta solo i formati di data HTTP validi per tutte le intestazioni che accettano i valori di data. La parte temporale della data può essere specificata nel formato GMT (Greenwich Mean Time) o UTC (Universal Coordinated Time) senza offset del fuso orario (deve essere specificato ++1). Se si include l' `x-amz-date`intestazione nella richiesta, questo sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza la versione 4 della firma AWS, l' `x-amz-date`intestazione deve essere presente nella richiesta firmata perché l'intestazione della data non è supportata.

Intestazioni di richiesta comuni

Il sistema StorageGRID supporta le intestazioni delle richieste comuni definite da "Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni", con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per firma AWS versione 2 Supporto per firma AWS versione 4, con le seguenti eccezioni: • Quando si fornisce il valore checksum del payload effettivo in `x-amz-content-sha256`, il valore viene accettato senza convalida, come se il valore `UNSIGNED-PAYLOAD` fosse stato fornito per l'intestazione. Quando si fornisce un `x-amz-content-sha256` valore di intestazione che implica `aws-chunked` lo streaming (ad esempio, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), le firme dei frammenti non vengono verificate in base ai dati dei frammenti.
x-amz-security-token	Non implementato. Resi `XNotImplemented`.

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite dal *riferimento API del servizio di storage semplice*, con un'eccezione.

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

Autenticare le richieste

Il sistema StorageGRID supporta l'accesso anonimo e autenticato agli oggetti utilizzando l'API S3.

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

Le richieste autenticate devono essere firmate utilizzando l'ID della chiave di accesso e la chiave di accesso segreta.

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

Utilizzare l'intestazione autorizzazione HTTP

L'intestazione HTTP `Authorization` viene utilizzata da tutte le operazioni API S3, ad eccezione delle richieste anonime, laddove consentito dal criterio bucket. L' `Authorization`intestazione contiene tutte le informazioni di firma necessarie per autenticare una richiesta.

Utilizzare i parametri di query

È possibile utilizzare i parametri di query per aggiungere informazioni di autenticazione a un URL. Questa operazione è nota come prefirma dell'URL, che può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL con prefisso non devono conoscere la chiave di accesso segreta per accedere alla risorsa, consentendo così l'accesso limitato a una risorsa da parte di terze parti.

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBucket (Precedentemente denominato GET Service)	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
OTTIENI l'utilizzo dello storage	La richiesta StorageGRID "OTTIENI l'utilizzo dello storage"indica la quantità totale di storage utilizzata da un account e per ogni bucket associato all'account. Si tratta di un'operazione sul servizio con un percorso di / e un parametro di query personalizzato (`?x-ntap-sg-usage`) aggiunto.

Operazione	Implementazione
OPZIONI /	Le applicazioni client possono `OPTIONS /` inviare richieste alla porta S3 su un nodo di archiviazione, senza fornire credenziali di autenticazione S3, per determinare se il nodo di archiviazione è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di storage è inattivo.

Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 5,000 bucket per ciascun account tenant S3.

Ogni griglia può avere un massimo di 100.000 secchi.

Per supportare 5.000 bucket, ogni nodo di storage nella griglia deve avere un minimo di 64 GB di RAM.

Le restrizioni dei nomi dei bucket seguono le restrizioni delle regioni AWS US Standard, ma è necessario limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste di tipo host virtuale S3.

Per ulteriori informazioni, vedere quanto segue:

- "Guida utente di Amazon Simple Storage Service: Quote, restrizioni e limitazioni dei bucket"
- "Configurare i nomi di dominio degli endpoint S3"

Le operazioni ListObjects (GET Bucket) e ListObjectVersions (GET Bucket Object Versions) supportano StorageGRID "valori di coerenza".

È possibile verificare se gli aggiornamenti dell'ultimo tempo di accesso sono attivati o disattivati per i singoli bucket. Vedere "OTTIENI l'ultimo tempo di accesso a bucket".

La seguente tabella descrive come StorageGRID implementa le operazioni del bucket API REST S3. Per eseguire una di queste operazioni, è necessario fornire le credenziali di accesso necessarie per l'account.

Operazione	Implementazione
CreateBucket	Crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). ◦ Deve essere conforme al DNS. ◦ Deve contenere almeno 3 e non più di 63 caratteri. ◦ Può essere una serie di una o più etichette, con 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 essere simile a un indirizzo IP formattato con testo. ◦ Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. • Per impostazione predefinita, i bucket vengono creati nella `us-east-1` regione; tuttavia, è possibile utilizzare l' `LocationConstraint`elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza l' `LocationConstraint`elemento, è necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API di gestione griglia. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare. **Nota**: Si verifica un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID. • È possibile includere l' `x-amz-bucket-object-lock-enabled`intestazione della richiesta per creare un bucket con blocco oggetto S3 attivato. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3". È necessario attivare il blocco oggetti S3 quando si crea il bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea 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 vengono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedere "Creare la configurazione del ciclo di vita S3".

Operazione	Implementazione
DeleteBucketPolicy	Elimina il criterio allegato al bucket.
DeleteBucketReplication	Elimina la configurazione di replica collegata al bucket.
DeleteBucketTagging	Utilizza la `tagging` sottorisorsa per rimuovere tutti i tag da un bucket. **Attenzione**: Se per questo bucket è impostato un tag criterio ILM non predefinito, vi sarà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket con un valore assegnato. Non inviare una richiesta DeleteBucketTagging se è presente un `NTAP-SG-ILM-BUCKET-TAG` tag bucket. Al contrario, eseguire una richiesta PutBucketTagging con solo il `NTAP-SG-ILM-BUCKET-TAG` tag e il relativo valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere l' `NTAP-SG-ILM-BUCKET-TAG`etichetta della benna.
GetBucketAcl	Restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario del bucket, indicando che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce la `cors` configurazione per la benna.
GetBucketEncryption	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket GET)	Restituisce la configurazione del ciclo di vita per il bucket. Vedere "Creare la configurazione del ciclo di vita S3".
GetBucketLocation	Restituisce l'area impostata utilizzando l' `LocationConstraint`elemento nella richiesta `CreateBucket`. Se la regione del bucket è `us-east-1`, viene restituita una stringa vuota per la regione.
GetBucketNotificationConfiguration (Precedentemente denominata notifica bucket GET)	Restituisce la configurazione di notifica collegata al bucket.
GetBucketPolicy	Restituisce la policy allegata al bucket.
GetBucketReplication	Restituisce la configurazione di replica collegata al bucket.

Operazione	Implementazione
GetBucketTagging	Utilizza la `tagging` sottorisorsa per restituire tutti i tag per un bucket. **Attenzione**: Se per questo bucket è impostato un tag criterio ILM non predefinito, vi sarà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket con un valore assegnato. Non modificare o rimuovere questo tag.
GetBucketVersioning	Questa implementazione utilizza la `versioning` sottorisorsa per restituire lo stato di versione di un bucket. • *Blank*: La versione non è mai stata abilitata (bucket "Unversioned") • Enabled (attivato): Il controllo delle versioni è attivato • Suspended (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso
GetObjectLockConfiguration	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurato. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".
HeadBucket	Determina se esiste un bucket e si dispone dell'autorizzazione per accedervi. Questa operazione restituisce: • `x-ntap-sg-bucket-id`: UUID del bucket in formato UUID. • `x-ntap-sg-trace-id`: L'ID di traccia univoco della richiesta associata.
ListObjects e ListObjectsV2 (Precedentemente denominato GET Bucket)	Restituisce alcuni o tutti gli oggetti (fino a 1.000) in un bucket. La classe di archiviazione per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con l' `REDUCED_REDUNDANCY`opzione della classe di archiviazione: • `STANDARD`, Che indica che l'oggetto è memorizzato in un pool di archiviazione costituito da nodi di archiviazione. • `GLACIER`, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. Se il bucket contiene un numero elevato di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune `CommonPrefixes` che non contengono chiavi.
ListObjectVersions (Precedentemente denominate versioni oggetto GET Bucket)	Con l'accesso IN LETTURA IN un bucket, questa operazione con le `versions` risorse secondarie elenca i metadati di tutte le versioni di oggetti nel bucket.

Operazione	Implementazione
PutBucketCors	Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire le richieste cross-origin. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Ad esempio, si supponga di utilizzare un bucket S3 denominato `images` per memorizzare la grafica. Impostando la configurazione CORS per il `images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito Web `http://www.example.com`.
PutBucketEncryption	Consente di impostare lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è attivata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati.StorageGRID supporta la crittografia lato server con le chiavi gestite da StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare il `SSEAlgorithm` parametro su `AES256` e non utilizzare il `KMSMasterKeyID` parametro. La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include l' `x-amz-server-side-encryption-*`intestazione della richiesta).
PutBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket PUT)	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 Vedere "Creare la configurazione del ciclo di vita S3". Per comprendere in che modo l'azione scadenza in un ciclo di vita bucket interagisce con le istruzioni di posizionamento ILM, vedere "Come ILM opera per tutta la vita di un oggetto". **Nota**: La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

Operazione	Implementazione

PutBucketNotificationConfiguration
 	
(Precedentemente denominata notifica bucket PUT)
	Configura le notifiche per il bucket utilizzando l'XML di configurazione delle notifiche incluso nel corpo della richiesta. È necessario conoscere i seguenti dettagli di implementazione:
	
	• StorageGRID supporta gli argomenti di Amazon Simple Notification Service (Amazon SNS) o Kafka come destinazioni. Gli endpoint SQS (Simple Queue Service) o Amazon Lambda non sono supportati.
	• La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID. Gli endpoint possono essere creati utilizzando il tenant Manager o l'API di gestione tenant.
	
	L'endpoint deve esistere perché la configurazione della notifica abbia esito positivo. Se l'endpoint non esiste, viene restituito un `400 Bad Request` errore con il codice `InvalidArgument`.
	
	• Non è possibile configurare una notifica per i seguenti tipi di evento. Questi tipi di evento sono **non** supportati.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ad eccezione del fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente:
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ **AwsRegion**
	
	non incluso
	
	◦ **x-amz-id-2**
	
	non incluso
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Imposta il criterio associato al bucket. Vedere "Utilizza policy di accesso a bucket e gruppi".

Operazione	Implementazione
PutBucketReplication	Si configura "Replica di StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica di CloudMirror, è necessario conoscere i seguenti dettagli di implementazione: • StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo dell' `Filter`elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, vedere "Guida utente di Amazon Simple Storage Service: Configurazione della replica". • La replica del bucket può essere configurata su bucket con versione o senza versione. • È possibile specificare un bucket di destinazione diverso in ciascuna regola dell'XML di configurazione della replica. Un bucket di origine può replicare in più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID, come specificato in Gestione tenant o nell'API di gestione tenant. Vedere "Configurare la replica di CloudMirror". L'endpoint deve esistere per il successo della configurazione della replica. Se l'endpoint non esiste, la richiesta non riesce come `400 Bad Request`. il messaggio di errore indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Non è necessario specificare un `Role` nell'XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato. • Se si omette la classe di archiviazione dall'XML di configurazione, StorageGRID utilizza la `STANDARD` classe di archiviazione per impostazione predefinita. • Se si elimina un oggetto dal bucket di origine o si elimina lo stesso bucket di origine, il comportamento della replica tra regioni è il seguente: ◦ Se si elimina l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non viene replicato e non viene inviata alcuna notifica. ◦ Se elimini l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento standard di eliminazione di Amazon S3 per V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza la `tagging` sottorisorsa per aggiungere o aggiornare una serie di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket. • Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode. • I valori dei tag possono contenere fino a 256 caratteri Unicode. • Chiave e valori distinguono tra maiuscole e minuscole. **Attenzione**: Se per questo bucket è impostato un tag criterio ILM non predefinito, vi sarà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket con un valore assegnato. Assicurarsi che il `NTAP-SG-ILM-BUCKET-TAG` tag bucket sia incluso con il valore assegnato in tutte le richieste PutBucketTagging. Non modificare o rimuovere questo tag. **Nota**: Questa operazione sovrascriverà tutti i tag correnti già presenti nel bucket. Se qualsiasi tag esistente viene omesso dal set, tali tag verranno rimossi per il bucket.
PutBucketVersioning	Utilizza la `versioning` sottorisorsa per impostare lo stato di versione di un bucket esistente. È possibile impostare lo stato di versione con uno dei seguenti valori: • Enabled (attivato): Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco. • Suspended (sospeso): Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione `null` .
PutObjectLockConfiguration	Configura o rimuove la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito. Se il periodo di conservazione predefinito viene modificato, la data di conservazione delle versioni degli oggetti esistenti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Per informazioni dettagliate, vedere"Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Operazioni sugli oggetti

Operazioni sugli oggetti

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

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

- StorageGRID "valori di coerenza"è supportato da tutte le operazioni sugli oggetti, ad eccezione di quanto segue:
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent
- Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.
- Impossibile accedere agli oggetti dati acquisiti nel sistema StorageGRID tramite Swift tramite S3.

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

Operazione	Implementazione
DeleteObject (Elimina oggetto)	L'autenticazione multifattore (MFA) e l'intestazione della risposta `x-amz-mfa` non sono supportate. Durante l'elaborazione di una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito. **Versione** Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare la `versionId` sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il `versionId` corrisponde a un marcatore di eliminazione, l'intestazione della risposta `x-amz-delete-marker` viene riportata impostata su `true`. • Se un oggetto viene eliminato senza la `versionId` sottorisorsa in un bucket con il controllo delle versioni attivato, viene generato un indicatore di eliminazione. Il `versionId` marcatore per l'eliminazione viene restituito utilizzando l' `x-amz-version-id`intestazione della risposta e l' `x-amz-delete-marker`intestazione della risposta viene riportata impostata su `true`. • Se un oggetto viene eliminato senza la `versionId` sottorisorsa in un bucket con la versione sospesa, si ottiene l'eliminazione permanente di una versione 'null' già esistente o di un marcatore 'null' e la generazione di un nuovo marcatore 'null'. L' `x-amz-delete-marker`intestazione della risposta viene riportata impostata su `true`. **Nota**: In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.
DeleteObjects (Precedentemente denominato ELIMINA più oggetti)	L'autenticazione multifattore (MFA) e l'intestazione della risposta `x-amz-mfa` non sono supportate. È possibile eliminare più oggetti nello stesso messaggio di richiesta. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.

Operazione	Implementazione
DeleteObjectTagging	Utilizza la `tagging` sottorisorsa per rimuovere tutti i tag da un oggetto. **Versione** Se il `versionId` parametro query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l' `x-amz-delete-marker`intestazione della risposta impostata su `true`.
GetObject	"GetObject"
GetObjectAcl	Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario dell'oggetto, indicando che il proprietario dispone dell'accesso completo all'oggetto.
GetObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectTagging	Utilizza la `tagging` sottorisorsa per restituire tutti i tag per un oggetto. **Versione** Se il `versionId` parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag della versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l' `x-amz-delete-marker`intestazione della risposta impostata su `true`.
HeadObject (oggetto intestazione)	"HeadObject (oggetto intestazione)"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
Oggetto CopyObject (Precedentemente denominato oggetto PUT - Copia)	"Oggetto CopyObject"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

Operazione	Implementazione
PutObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
PutObjectTagging	Utilizza la `tagging` sottorisorsa per aggiungere una serie di tag a un oggetto esistente. **Limiti tag oggetto** È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole. **Aggiornamenti dei tag e comportamento di acquisizione** Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non acquisisce nuovamente l'oggetto. Ciò significa che l'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto. **Risoluzione dei conflitti** Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione. **Versione** Se il `versionId` parametro query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l' `x-amz-delete-marker`intestazione della risposta impostata su `true`.
SelectObjectContent	"SelectObjectContent"

USA S3 Select

StorageGRID supporta le seguenti condizioni, tipi di dati e operatori Amazon S3 Select per "Comando SelectObjectContent".

Gli elementi non elencati non sono supportati.

Per la sintassi, vedere "SelectObjectContent". Per ulteriori informazioni su S3 Select, vedere "Documentazione AWS per S3 Select" .

Solo gli account tenant con S3 Select abilitato possono eseguire query SelectObjectContent. Consultare la "Considerazioni e requisiti per l'utilizzo di S3 Select".

Clausole

- SELEZIONARE l'elenco
- CLAUSOLA FROM
- Clausola WHERE
- Clausola di LIMITAZIONE

Tipi di dati

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

Operatori

Operatori logici

- E.
- NO
- OPPURE

Operatori di confronto

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- TRA
- POLL

Operatori di corrispondenza dei modelli

- MI PIACE
- _
- %

Operatori unitari

- È NULL
- NON È NULL

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni di aggregazione

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

Funzioni condizionali

- CASO
- COALESCE
- NULLIF

Funzioni di conversione

- CAST (per il tipo di dati supportato)

Funzioni di data

- DATA_ADD
- DATA_DIFF

- ESTRARRE
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funzioni di stringa

- CHAR_LENGTH, CHARACTER_LENGTH
- ABBASSARE
- SOTTOSTRINGA
- TAGLIARE
- SUPERIORE

Utilizzare la crittografia lato server

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

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

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

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

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

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

Utilizzare SSE

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

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

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

- "PutObject"

- "Oggetto CopyObject"
- "CreateMultipartUpload"

Utilizzare SSE-C.

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

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

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

- "GetObject"
- "HeadObject (oggetto intestazione)"
- "PutObject"
- "Oggetto CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

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

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

- È necessario utilizzare https.

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

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

versione dell'oggetto.

- Poiché si gestiscono le chiavi di crittografia sul lato client, è necessario gestire anche eventuali protezioni aggiuntive, come la rotazione delle chiavi, sul lato client.

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

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

Informazioni correlate

"Manuale dell'utente di Amazon S3: Utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)"

Oggetto CopyObject

È possibile utilizzare la richiesta CopyObject S3 per creare una copia di un oggetto già memorizzato in S3. Un'operazione CopyObject è la stessa dell'esecuzione di GetObject seguito da PutObject.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare "caricamento multiparte" invece.

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

> Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di 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 versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

UTF-8 caratteri nei metadati dell'utente

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

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

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapiti.
- 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 consente di copiare l'oggetto e i metadati associati.

  È possibile specificare `REPLACE` se sovrascrivere i metadati esistenti durante la copia dell'oggetto o se aggiornare i metadati dell'oggetto.

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

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

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

    Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

- Intestazioni di richiesta SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Vedere Intestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

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

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

Opzioni di classe storage

L' `x-amz-storage-class`intestazione della richiesta è supportata e influisce sul numero di copie degli oggetti create da StorageGRID se la regola ILM corrispondente utilizza il doppio commit o bilanciato "opzione di acquisizione".

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

  > Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l' `REDUCED_REDUNDANCY`opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di x-amz-copy-source in CopyObject

Se il bucket e la chiave di origine, specificati nell' `x-amz-copy-source`intestazione, 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`intestazione viene specificata come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non reinserisce l'oggetto. Questo ha due conseguenze importanti:

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la

crittografia di un oggetto esistente sul posto. Se si fornisce 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 Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.

  Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se si utilizza "usa crittografia lato server", le intestazioni di richiesta fornite dipendono dal fatto che l'oggetto di origine sia crittografato e dal fatto che si intenda crittografare l'oggetto di destinazione.

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

  > Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a "utilizzo della crittografia lato server".

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

    > `server-side-encryption`Impossibile aggiornare il valore dell'oggetto. Eseguire invece una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive`: `REPLACE`.

Versione

Se il bucket di origine è in versione, è possibile utilizzare l' `x-amz-copy-source`intestazione per copiare la versione più recente di un oggetto. Per copiare una versione specifica di un oggetto, è necessario specificare esplicitamente la versione da copiare utilizzando la `versionId` sottorisorsa. Se il bucket di destinazione è in versione, la versione generata viene restituita nell' `x-amz-version-id`intestazione della risposta. Se la versione è sospesa per il bucket target, `x-amz-version-id` restituisce un valore "null".

GetObject

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

Oggetti GetObject e multiparte

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

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

UTF-8 caratteri nei metadati dell'utente

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

Intestazione richiesta supportata

È supportata la seguente intestazione della richiesta:

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

  L' `Range`intestazione non è supportata con `x-amz-checksum-mode` per GetObject. Quando si include `Range` nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore checksum nella risposta.

Intestazione della richiesta non supportata

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

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

Versione

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

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

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

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

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in "Utilizzare la crittografia lato server".

Comportamento degli oggetti GetObject per Cloud Storage Pool

Se un oggetto è stato memorizzato in "Pool di cloud storage", il comportamento di una richiesta GetObject dipende dallo stato dell'oggetto. Per ulteriori informazioni, vedere"HeadObject (oggetto intestazione)".

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

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

Oggetti multiparte o segmentati in un pool di storage cloud

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta GetObject potrebbe restituire erroneamente `200 OK` quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono state ancora ripristinate.

In questi casi:

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

Replica GetObject e cross-grid

Se si utilizza "federazione di grid" ed "replica cross-grid" è attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **COMPLETATO**: La replica è riuscita. • **PENDING**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

> StorageGRID non supporta la `x-amz-replication-status` testata.

HeadObject (oggetto intestazione)

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

Oggetti HeadObject e multiparte

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

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

UTF-8 caratteri nei metadati dell'utente

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

Intestazione richiesta supportata

È supportata la seguente intestazione della richiesta:

- `x-amz-checksum-mode`

  Il `partNumber` parametro e `Range` l'intestazione non sono supportati con `x-amz-checksum-mode` per HeadObject. Quando vengono inclusi nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore checksum nella risposta.

Intestazione della richiesta non supportata

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

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

Versione

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

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

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

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

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in "Utilizzare la crittografia lato server".

Risposte HeadObject per gli oggetti Cloud Storage Pool

Se l'oggetto è memorizzato in "Pool di cloud storage", vengono restituite le seguenti intestazioni di risposta:

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

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

Stato dell'oggetto	Risposta a HeadObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	`200 OK` (Non viene restituita alcuna intestazione di risposta speciale).

Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Fino a quando l'oggetto non viene spostato in uno stato non recuperabile, il valore per viene impostato su un `expiry-date` tempo lontano in futuro. L'ora esatta della transizione non è controllata dal sistema StorageGRID.

L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella griglia	`200 OK`
	
	`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 certo tempo lontano in futuro.
	
	Nota: Se la copia nella griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario eseguire una "RestoreObject" richiesta di ripristino della copia dal pool di archiviazione cloud prima di poter recuperare correttamente l'oggetto.

L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella 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 20 2018 00:00:00 GMT"`
	
	`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 multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire erroneamente `x-amz-restore: ongoing-request="false"` quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono state ancora ripristinate.

HeadObject e replica cross-grid

Se si utilizza "federazione di grid" ed "replica cross-grid" è attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta HeadObject. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **COMPLETATO**: La replica è riuscita. • **PENDING**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

> StorageGRID non supporta la `x-amz-replication-status` testata.

PutObject

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

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare "caricamento multiparte" invece.

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

> Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di 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 versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati dell'utente

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

UTF-8 caratteri nei metadati dell'utente

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

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

- Le richieste PutObject, CopyObject, GetObject e HeadObject hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 di 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 tag oggetto

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

Proprietà degli oggetti

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

  - StorageGRID non verifica il `chunk-signature` rispetto ai dati del blocco.
  - StorageGRID non verifica il valore fornito 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` si utilizza anche la firma del payload.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

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

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

  Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano al momento della creazione dell'oggetto. Ad esempio:

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

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

  > Una regola ILM non può utilizzare sia un **tempo di creazione definito dall'utente** per il tempo di riferimento che l'opzione di acquisizione bilanciata o rigorosa. Quando viene creata la regola ILM viene restituito un errore.
- `x-amz-tagging`
- Intestazioni di richiesta blocco oggetti S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`

- `x-amz-object-lock-legal-hold`

  Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

- Intestazioni di richiesta SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

  Vedere Intestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

  La `x-amz-website-redirect-location` testata ritorna `XNotImplemented`.

Opzioni di classe storage

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

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

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

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

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

- `REDUCED_REDUNDANCY`
  - **Commit doppio**: Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
  - **Balanced**: Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L' `REDUCED_REDUNDANCY`opzione viene utilizzata in modo ottimale quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso l'utilizzo di `REDUCED_REDUNDANCY` elimina la creazione e la cancellazione non necessarie di una copia degli oggetti extra per ogni operazione di acquisizione.

  L'uso dell' `REDUCED_REDUNDANCY`opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.

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

La specifica `REDUCED_REDUNDANCY` influisce solo sul numero di copie create al momento della prima acquisizione di un oggetto. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

> Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l' `REDUCED_REDUNDANCY`opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta per la crittografia lato server

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

- **SSE**: Utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID.
  - `x-amz-server-side-encryption`

    Quando l' `x-amz-server-side-encryption`intestazione non è inclusa nella richiesta PutObject, l'intera griglia "impostazione di crittografia degli oggetti archiviati"viene omessa dalla risposta PutObject.

- **SSE-C**: Utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.

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

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a "utilizzo della crittografia lato server".

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

Versione

Se la versione è abilitata per un bucket, viene generato automaticamente un univoco `versionId` per la versione dell'oggetto che viene memorizzato. Questo `versionId` viene anche restituito nella risposta utilizzando l' `x-amz-version-id`intestazione della risposta.

Se la versione è sospesa, la versione oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, verrà sovrascritta.

Calcoli della firma per l'intestazione autorizzazione

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

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

> Come procedura consigliata generale, includere sempre queste intestazioni all'interno `CanonicalHeaders` per assicurarsi che siano verificate; tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce un errore.

Per ulteriori informazioni, fare riferimento alla "Calcoli della firma per l'intestazione dell'autorizzazione: Trasferimento del payload in un singolo chunk (firma AWS versione 4)".

Informazioni correlate

- "Gestire gli oggetti con ILM"
- "Riferimento API Amazon Simple Storage Service: PutObject"

RestoreObject

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

Tipo di richiesta supportato

StorageGRID supporta solo le richieste RestoreObject per ripristinare un oggetto. Non supporta il `SELECT` tipo di restauro. Selezionare Richieste restituite `XNotImplemented`.

Versione

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

Comportamento di RestoreObject negli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in una "Pool di cloud storage", una richiesta RestoreObject presenta il seguente comportamento, in base allo stato dell'oggetto. Per ulteriori informazioni, vedere"HeadObject (oggetto intestazione)".

> Se un oggetto viene memorizzato in un Cloud Storage Pool ed esistono anche una o più copie dell'oggetto nella griglia, non è necessario ripristinarlo inviando una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	`403 Forbidden`, `InvalidObjectState`
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK` Non vengono apportate modifiche. **Nota**: Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificare il suo `expiry-date`.
Oggetto sottoposto a transizione in uno stato non recuperabile	`202 Accepted` Ripristina una copia recuperabile dell'oggetto in Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto viene riportato in uno stato non recuperabile. Facoltativamente, utilizzare l' `Tier`elemento di richiesta per determinare il tempo necessario per completare il processo di ripristino (`Expedited`, , `Standard` o `Bulk`). Se non si specifica `Tier`, viene utilizzato il `Standard` livello. **Importante**: Se un oggetto è stato spostato in S3 Glacier Deep Archive o Cloud Storage Pool utilizza l'archiviazione BLOB di Azure, non puoi ripristinarlo utilizzando il `Expedited` Tier. Viene restituito il seguente errore `403 Forbidden` , `InvalidTier`: `Retrieval option is not supported by this storage class`.
Oggetto in fase di ripristino da uno stato non recuperabile	`409 Conflict`, `RestoreAlreadyInProgress`

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` **Nota:** se un oggetto è stato ripristinato ad uno stato recuperabile, è possibile modificarlo `expiry-date` riemettendo la richiesta RestoreObject con un nuovo valore per `Days`. La data di ripristino viene aggiornata in relazione all'ora della richiesta.

SelectObjectContent

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

Per ulteriori informazioni, vedere "Riferimento API Amazon Simple Storage Service: SelectObjectContent".

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Si dispone dell' `s3:GetObject`autorizzazione per l'oggetto che si desidera sottoporre a query.
- L'oggetto che si desidera sottoporre a query 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 in parquet:
    - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
    - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
    - La dimensione massima del gruppo di righe non compresso è di 512 MB.
    - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
    - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.
- L'espressione SQL ha una lunghezza massima di 256 KB.
- Qualsiasi record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi per le richieste CSV

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

Esempio di sintassi della richiesta di 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 ottiene il nome dello stato, 2010 popolazioni, 2015 popolazioni stimate e la percentuale di cambiamento rispetto ai dati del censimento degli Stati Uniti. I record nel file che non sono stati vengono ignorati.

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

Le prime righe del file da interrogare, `SUB-EST2020_ALL.csv`, sono simili a quanto segue:

```
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`, sono simili a queste:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Esempio di utilizzo di AWS-CLI (Parquet)

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

Le prime righe del file di output, Changes.csv, sono le seguenti:

```
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 multiparte

Operazioni per caricamenti multiparte

Questa sezione descrive come StorageGRID supporta le operazioni per gli upload di più parti.

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

- Non si devono superare i 1.000 caricamenti simultanei di più parti in un singolo bucket, poiché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multicpart. I client S3 devono seguire queste linee guida:
  - Ciascuna parte di un caricamento multiparte 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 devono essere il più grandi possibile. Ad esempio, utilizzare le dimensioni delle parti di 5 GiB per un oggetto 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce l'overhead dei metadati StorageGRID.
  - Per gli oggetti di dimensioni inferiori a 5 GiB, prendere in considerazione l'utilizzo di un caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte nel momento in cui viene acquisito e per l'oggetto nel suo insieme al completamento del caricamento multiparte, se la regola ILM utilizza il bilanciato o rigoroso "opzione di acquisizione". Devi essere consapevole di come questo influisca sul posizionamento di oggetti e parti:

- Se ILM cambia mentre è in corso un caricamento multiparte S3, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. Qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.
- Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi sono memorizzati a DC1 GB mentre tutti gli oggetti più piccoli sono memorizzati a DC2 GB, ogni parte da 1 GB di un caricamento multiparte in 10 parti viene memorizzata a DC2 GB al momento dell'acquisizione. Tuttavia, quando ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.

- Tutte le operazioni di caricamento multiparte supportano StorageGRID "valori di coerenza".
- Quando un oggetto viene acquisito utilizzando il caricamento multiparte, "Soglia di segmentazione degli oggetti (1 GiB)"non viene applicato.
- Se necessario, è possibile utilizzare "crittografia lato server" con caricamenti multiparte. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere l' `x-amz-server-side-encryption`intestazione della richiesta solo nella richiesta CreateMultipartUpload. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni richiesta UploadPart successiva.

Operazione	Implementazione
AbortMultipartUpload	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
CompleteMultipartUpload	Vedere "CompleteMultipartUpload"
CreateMultipartUpload (Precedentemente denominato Initiate Multipart Upload)	Vedere "CreateMultipartUpload"
ListMultipartUploads	Vedere "ListMultipartUploads"
ListParts	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
UploadPart	Vedere "UploadPart"
UploadPartCopy	Vedere "UploadPartCopy"

CompleteMultipartUpload

L'operazione CompleteMultipartUpload completa il caricamento multiparte di un oggetto assemblando le parti caricate in precedenza.

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

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

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 sul numero di copie di oggetti create da StorageGRID se la regola ILM corrispondente specifica "Dual commit o opzione di acquisizione bilanciata".

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

  > Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l' `REDUCED_REDUNDANCY`opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

> Se un caricamento multiparte non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono cancellati dal sistema.

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

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

Versione

Questa operazione completa un caricamento multiparte. Se il controllo delle versioni è attivato per un bucket, la versione dell'oggetto viene creata al termine del caricamento multiparte.

Se la versione è abilitata per un bucket, viene generato automaticamente un univoco `versionId` per la

versione dell'oggetto che viene memorizzato. Questo `versionId` viene anche restituito nella risposta utilizzando l' `x-amz-version-id`intestazione della risposta.

Se la versione è sospesa, la versione oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, verrà sovrascritta.

> Quando il controllo delle versioni è attivato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se ci sono caricamenti multipli simultanei completati sulla stessa chiave a oggetti. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e fare in modo che un altro caricamento multiparte venga avviato e completato prima sulla stessa chiave a oggetti. Nei bucket senza versione, il caricamento multiparte che completa l'ultimo ha la precedenza.

Replica, notifica o notifica dei metadati non riuscite

Se il bucket in cui si verifica il caricamento multiparte è configurato per un servizio di piattaforma, il caricamento multiparte riesce anche se l'azione di replica o notifica associata non riesce.

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

Fare riferimento alla "Risolvere i problemi relativi ai servizi della piattaforma".

CreateMultipartUpload

L'operazione CreateMultipartUpload (precedentemente denominata Initiate Multipart Upload) avvia un caricamento multiparte 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 sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza Strict "opzione di acquisizione", l' `x-amz-storage-class`intestazione non ha alcun effetto.

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

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

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

- `REDUCED_REDUNDANCY`
  - **Dual Commit**: Se la regola ILM specifica l'opzione Dual Commit, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (Single Commit).
  - **Balanced**: Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L' `REDUCED_REDUNDANCY`opzione viene utilizzata in modo ottimale quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso l'utilizzo di `REDUCED_REDUNDANCY` elimina la creazione e la cancellazione non necessarie di una copia degli oggetti extra per ogni operazione di acquisizione.

  L'uso dell' `REDUCED_REDUNDANCY`opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.

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

La specifica `REDUCED_REDUNDANCY` influisce solo sul numero di copie create al momento della prima acquisizione di un oggetto. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

> Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l' `REDUCED_REDUNDANCY`opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

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

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

  Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per

una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano al momento della creazione dell'oggetto. Ad esempio:

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

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

> L'aggiunta `creation-time` come metadati definiti dall'utente non è consentita se si aggiunge un oggetto a un bucket in cui è abilitata la conformità legacy. Viene restituito un errore.

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

    Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la versione dell'oggetto che resta aggiornata.

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

- Intestazioni di richiesta SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Intestazioni di richiesta per la crittografia lato server

> Per informazioni sul modo in cui StorageGRID gestisce i caratteri UTF-8, vedere "PutObject".

Intestazioni di richiesta per la crittografia lato server

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

- **SSE**: Utilizzare la seguente intestazione nella richiesta CreateMultipartUpload se si desidera 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**: Utilizzare tutte e tre le intestazioni nella richiesta CreateMultipartUpload (e in ogni richiesta UploadPart successiva) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.

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

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a "utilizzo della crittografia lato server".

Intestazioni di richiesta non supportate

La seguente intestazione della richiesta non è supportata:

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

  La `x-amz-website-redirect-location` testata ritorna `XNotImplemented`.

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

ListMultipartUploads

L'operazione ListMultipartUploads elenca i caricamenti multiparte 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`

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

UploadPart

L'operazione UploadPart carica una parte in un upload multiparte 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 è stata specificata la crittografia SSE-C per la richiesta CreateMultipartUpload, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

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

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in "Utilizzare la crittografia lato server".

Se è stato specificato un checksum SHA-256 durante la richiesta CreateMultipartUpload, è necessario includere anche l'intestazione della richiesta seguente in ogni richiesta UploadPart:

- `x-amz-checksum-sha256`: Specificare 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`

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

UploadPartCopy

L'operazione UploadPartCopy carica una parte di un oggetto copiando i dati da un

oggetto esistente come origine dati.

L'operazione UploadPartCopy viene implementata con tutto il comportamento dell'API REST Amazon S3. Soggetto a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificati in nel `x-amz-copy-source-range` 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 è stata specificata la crittografia SSE-C per la richiesta CreateMultipartUpload, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPartCopy:

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

Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta UploadPartCopy, in modo che l'oggetto possa essere decrittografato e quindi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto sorgente.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in "Utilizzare la crittografia lato server".

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

Risposte agli errori

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

Codici di errore S3 API supportati

Nome	Stato HTTP
Accesso negato	403 proibita
BadDigest	400 richiesta errata
BucketAlreadyExists	409 conflitto
BucketNotEmpty	409 conflitto
IncompleteBody	400 richiesta errata
InternalError	500 errore interno del server
InvalidAccessKeyId	403 proibita
Documento invalidato	400 richiesta errata
InvalidBucketName	400 richiesta errata
InvalidBucketState	409 conflitto
InvalidDigest	400 richiesta errata
InvalidEncryptionAlgorithmError	400 richiesta errata
InvalidPart	400 richiesta errata
InvalidPartOrder	400 richiesta errata
InvalidRange	416 intervallo richiesto non riscontrabile
InvalidRequest	400 richiesta errata
InvalidStorageClass	400 richiesta errata
InvalidTag	400 richiesta errata

Nome	Stato HTTP
InvalidURI	400 richiesta errata
KeyTooLong	400 richiesta errata
MalformedXML	400 richiesta errata
MetadataTooLarge	400 richiesta errata
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
MissingRequestBodyError	400 richiesta errata
MissingSecurityHeader	400 richiesta errata
NoSuchBucket	404 non trovato
NoSuchKey	404 non trovato
NoSuchUpload	404 non trovato
Non soddisfatto	501 non implementato
NoSuchBucketPolicy	404 non trovato
ObjectLockConfigurationNotFoundError	404 non trovato
PrecondizioneFailed	412 precondizione non riuscita
RequestTimeTooSkewed	403 proibita
ServiceUnavailable (Servizio non disponibile)	503 Servizio non disponibile
SignatureDoesNotMatch	403 proibita
TooManyBucket	400 richiesta errata
UserKeyMustBeSpecified	400 richiesta errata

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket compatibile legacy	400 richiesta errata
XBucketPolicyParseException	Impossibile analizzare JSON policy bucket ricevuta.	400 richiesta errata
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 proibita
XComplianceRiduciRedundancyProibita	La ridondanza ridotta non è consentita nel bucket compatibile legacy	400 richiesta errata
XMaxBucketPolicyLengthExceed	La policy supera la lunghezza massima consentita della policy bucket.	400 richiesta errata
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 richiesta errata
Conformità XNoSuchBucketCompliance	Nel bucket specificato non è attivata la compliance legacy.	404 non trovato
XNotAcceptable (XNotAccettabile)	La richiesta contiene una o più intestazioni di accettazione che non possono essere soddisfatte.	406 non accettabile
XNotImplemented	La richiesta fornita implica funzionalità non implementate.	501 non implementato

Informazioni sul copyright

Informazioni sul marchio commerciale