Supporto per l'API REST di Amazon S3

StorageGRID software

NetApp
December 03, 2025

Sommario

Supporto per l'API REST di Amazon S3

Dettagli di implementazione dell'API REST S3

Il sistema StorageGRID implementa l'API Simple Storage Service (versione API 2006-03-01) con supporto per la maggior parte delle operazioni e con alcune limitazioni. Quando si integrano applicazioni client S3 REST API, è necessario comprendere i dettagli di implementazione.

Il sistema StorageGRID supporta sia le richieste in stile host virtuale sia quelle in stile percorso.

Gestione delle date

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

Il sistema StorageGRID supporta solo formati di data HTTP validi per tutte le intestazioni che accettano valori di data. La parte oraria della data può essere specificata nel formato Greenwich Mean Time (GMT) o nel formato Universal Coordinated Time (UTC) senza differenza di fuso orario (è necessario specificare +0000). Se includi il `x-amz-date` nell'intestazione della richiesta, sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza AWS Signature versione 4, `x-amz-date` l'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 di richiesta comuni definite da "Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni" , con una eccezione.

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

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite da *Simple Storage Service API Reference*, con un'eccezione.

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

Autenticare le richieste

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

L'API S3 supporta la versione 2 e la versione 4 della firma 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: HTTP `Authorization` intestazione e utilizzando parametri di query.

Utilizzare l'intestazione di autorizzazione HTTP

L'HTTP `Authorization` L'intestazione viene utilizzata da tutte le operazioni API S3, ad eccezione delle richieste anonime, ove consentito dalla policy del bucket. IL `Authorization` L'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 e può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL prefirmato non hanno bisogno di conoscere la chiave di accesso segreta per accedere alla risorsa, il che consente di fornire a terze parti un accesso limitato a una risorsa.

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

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

Operazione	Implementazione
OPZIONI /	Le applicazioni client possono emettere `OPTIONS /` 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 archiviazione è inattivo.

Operazioni sui bucket

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

Ogni griglia può avere un massimo di 100.000 bucket.

Per supportare 5.000 bucket, ogni nodo di archiviazione nella griglia deve disporre di almeno 64 GB di RAM.

Le restrizioni sui nomi dei bucket seguono le restrizioni della regione AWS US Standard, ma è opportuno limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste in stile hosting virtuale S3.

Per maggiori informazioni vedere quanto segue:

- "Guida per l'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 all'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket. Vedere "GET Ora dell'ultimo accesso al bucket" .

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

Operazione	Implementazione
CreaBucket	Crea un nuovo bucket. Creando il bucket, ne diventi il proprietario. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere univoco in ogni sistema StorageGRID (non solo 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 contenere solo lettere minuscole, numeri e trattini. ◦ Non deve avere l'aspetto di un indirizzo IP formattato come testo. ◦ Non utilizzare punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server. • Per impostazione predefinita, i bucket vengono creati in `us-east-1` regione; tuttavia, è possibile utilizzare il `LocationConstraint` elemento di richiesta nel corpo della richiesta per specificare una regione diversa. Quando si utilizza il `LocationConstraint` elemento, è necessario specificare il nome esatto di una regione definita tramite Grid Manager o Grid Management API. Se non conosci il nome della regione da utilizzare, contatta l'amministratore di sistema. **Nota**: si verificherà un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID. • Puoi includere il `x-amz-bucket-object-lock-enabled` intestazione della richiesta per creare un bucket con S3 Object Lock abilitato. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" . Quando si crea il bucket, è necessario abilitare S3 Object Lock. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket. S3 Object Lock richiede il controllo delle versioni dei bucket, che viene abilitato automaticamente quando si crea il bucket.
EliminaBucket	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 tutti i nuovi oggetti aggiunti al bucket non vengono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedere "Crea la configurazione del ciclo di vita S3" .
DeleteBucketPolicy	Elimina la policy associata al bucket.

Operazione	Implementazione
DeleteBucketReplication	Elimina la configurazione di replica associata al bucket.
DeleteBucketTagging	Utilizza il `tagging` sottorisorsa per rimuovere tutti i tag da un bucket. **Attenzione**: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è assegnato un valore. Non inviare una richiesta DeleteBucketTagging se è presente un `NTAP-SG-ILM-BUCKET-TAG` etichetta del secchio. Invece, emetti una richiesta PutBucketTagging con solo `NTAP-SG-ILM-BUCKET-TAG` tag e il valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere il `NTAP-SG-ILM-BUCKET-TAG` etichetta del secchio.
OttieniBucketAcl	Restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario del bucket, a indicare che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce il `cors` configurazione per il bucket.
Ottieni crittografia dei bucket	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (in precedenza denominato ciclo di vita del bucket GET)	Restituisce la configurazione del ciclo di vita per il bucket. Vedere "Crea la configurazione del ciclo di vita S3" .
OttieniPosizioneBucket	Restituisce la regione impostata utilizzando `LocationConstraint` elemento nella richiesta CreateBucket. Se la regione del bucket è `us-east-1` , viene restituita una stringa vuota per la regione.
Configurazione di notifica di GetBucket (in precedenza denominata notifica GET Bucket)	Restituisce la configurazione delle notifiche allegata al bucket.
OttieniPoliticaBucket	Restituisce la policy associata al bucket.
OttieniReplicazioneBucket	Restituisce la configurazione di replica associata al bucket.

Operazione	Implementazione
OttieniBucketTagging	Utilizza il `tagging` sottorisorsa per restituire tutti i tag per un bucket. **Attenzione**: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è assegnato un valore. Non modificare o rimuovere questo tag.
GetBucketVersioning	Questa implementazione utilizza il `versioning` sottorisorsa per restituire lo stato di controllo delle versioni di un bucket. • *blank*: il controllo delle versioni non è mai stato abilitato (il bucket è "Senza controllo delle versioni") • Abilitato: il controllo delle versioni è abilitato • Sospeso: il controllo delle versioni era precedentemente abilitato ed è sospeso
Ottieni configurazione blocco oggetto	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurati. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .
HeadBucket	Determina se esiste un bucket e se si dispone dell'autorizzazione per accedervi. Questa operazione restituisce: • `x-ntap-sg-bucket-id`: L'UUID del bucket nel formato UUID. • `x-ntap-sg-trace-id`: ID traccia univoco della richiesta associata.
ListObjects e ListObjectsV2 (precedentemente denominato GET Bucket)	Restituisce alcuni o tutti (fino a 1.000) gli oggetti in un bucket. La classe di archiviazione per gli oggetti può avere uno dei due valori, anche se l'oggetto è stato ingerito con `REDUCED_REDUNDANCY` opzione classe di archiviazione: • `STANDARD`, che indica che l'oggetto è archiviato 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 che hanno lo stesso prefisso, la risposta potrebbe includere alcune `CommonPrefixes` che non contengono chiavi.
ListObjectVersions (precedentemente denominate versioni GET Bucket Object)	Con accesso READ su un bucket, utilizzando questa operazione con `versions` La sottorisorsa elenca i metadati di tutte le versioni degli oggetti nel bucket.

Operazione	Implementazione
PutBucketCors	Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire richieste multiorigine. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponiamo di utilizzare un bucket S3 denominato `images` per memorizzare la grafica. Impostando la configurazione CORS per `images` bucket, puoi consentire che le immagini in quel bucket vengano visualizzate sul sito web `http://www.example.com` .
PutBucketEncryption	Imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è abilitata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con chiavi gestite StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare `SSEAlgorithm` parametro a `AES256` e non usare il `KMSMasterKeyID` parametro. La configurazione di crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include `x-amz-server-side-encryption-*` intestazione della richiesta).
Configurazione del ciclo di vita di PutBucket (in precedenza denominato ciclo di vita del 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: • AnnullaIncompletoCaricamento multiparte • Transizione Vedere "Crea la configurazione del ciclo di vita S3" . Per comprendere come l'azione di scadenza nel ciclo di vita di un bucket interagisce con le istruzioni di posizionamento ILM, vedere"Come funziona l'ILM durante la vita di un oggetto" . **Nota**: la configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

Operazione	Implementazione

Configurazione della notifica PutBucket
 	
(in precedenza denominata notifica PUT Bucket)
	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 come destinazioni gli argomenti Amazon Simple Notification Service (Amazon SNS) o Kafka. Gli endpoint Simple Queue Service (SQS) 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 Tenant Manager o Tenant Management API.
	
	Affinché la configurazione della notifica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, un `400 Bad Request` l'errore viene restituito con il codice `InvalidArgument` .
	
	• Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di eventi **non** sono supportati.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, con la differenza che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente:
	◦ **fonteevento**
	
	`sgws:s3`
	
	◦ **awsRegion**
	
	non incluso
	
	◦ **x-amz-id-2**
	
	non incluso
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Imposta la policy associata al bucket. Vedere "Utilizzare criteri di accesso a bucket e gruppi" .

Operazione	Implementazione
PutBucketReplication	Configura"Replica StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica CloudMirror, è necessario conoscere i seguenti dettagli di implementazione: • StorageGRID supporta solo la versione 1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'uso di `Filter` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per i dettagli, vedere "Guida per l'utente di Amazon Simple Storage Service: configurazione della replica" . • La replica dei bucket può essere configurata su bucket con o senza versione. • È possibile specificare un bucket di destinazione diverso in ogni regola del file XML di configurazione della replica. Un bucket di origine può replicarsi su più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID come specificato in Tenant Manager o nell'API Tenant Management. Vedere "Configurare la replica di CloudMirror" . Affinché la configurazione della replica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, la richiesta fallisce come `400 Bad Request` Il messaggio di errore afferma: `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 `STANDARD` classe di archiviazione predefinita. • Se si elimina un oggetto dal bucket di origine o si elimina il bucket di origine stesso, il comportamento della replica tra regioni è il seguente: ◦ Se elimini l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non verrà replicato e non riceverai alcuna notifica. ◦ Se si elimina l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento di eliminazione standard di Amazon S3 per la V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza il `tagging` sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • Sia StorageGRID che Amazon S3 supportano fino a 50 tag per ogni bucket. • I tag associati a un bucket devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode. • I valori dei tag possono avere una lunghezza massima di 256 caratteri Unicode. • Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole. **Attenzione**: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è assegnato un valore. Assicuratevi che il `NTAP-SG-ILM-BUCKET-TAG` Il tag bucket è 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 vengono omessi tag esistenti dal set, tali tag verranno rimossi dal bucket.
PutBucketVersioning	Utilizza il `versioning` sottorisorsa per impostare lo stato di controllo delle versioni di un bucket esistente. È possibile impostare lo stato di controllo delle versioni con uno dei seguenti valori: • Abilitato: abilita il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID versione univoco. • Sospeso: disattiva il controllo delle versioni per gli 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 fino alle versioni esistenti degli oggetti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Vedere"Utilizzare l'API REST S3 per configurare S3 Object Lock" per informazioni dettagliate.

Operazioni sugli oggetti

Operazioni sugli oggetti

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

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

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

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

Operazione	Implementazione
EliminaOggetto	Autenticazione a più fattori (MFA) e intestazione di risposta `x-amz-mfa` non sono supportati. Durante l'elaborazione di una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni archiviate. In caso di esito positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e quindi segnala l'esito positivo al client. **Controllo delle versioni** Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare `versionId` sottorisorsa. L'utilizzo di questa sottorisorsa elimina definitivamente la versione. Se il `versionId` corrisponde a un marcatore di eliminazione, l'intestazione della risposta `x-amz-delete-marker` viene restituito impostato su `true` . • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket con controllo delle versioni abilitato, si traduce nella generazione di un marcatore di eliminazione. IL `versionId` per il marcatore di eliminazione viene restituito utilizzando il `x-amz-version-id` intestazione di risposta e `x-amz-delete-marker` l'intestazione di risposta viene restituita impostata su `true` . • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket con controllo delle versioni sospeso, si traduce nell'eliminazione permanente di una versione 'null' già esistente o di un marcatore di eliminazione 'null' e nella generazione di un nuovo marcatore di eliminazione 'null'. IL `x-amz-delete-marker` l'intestazione di risposta viene restituita impostata su `true` . **Nota**: in alcuni casi, potrebbero esistere più marcatori di eliminazione per un oggetto. Vedere"Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.
EliminaOggetti (in precedenza denominato DELETE Multiple Objects)	Autenticazione a più fattori (MFA) e intestazione di risposta `x-amz-mfa` non sono supportati. È possibile eliminare più oggetti nello stesso messaggio di richiesta. Vedere"Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.

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

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

Utilizzare S3 Select

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

Tutti gli elementi non elencati non sono supportati.

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

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

Clausole

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

Tipi di dati

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

Operatori

Operatori logici

- E
- NON
- O

Operatori di confronto

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

Operatori di corrispondenza di pattern

- COME
- _
- %

Operatori unitari

- È NULLO
- NON È NULLO

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni aggregate

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

Funzioni condizionali

- CASO
- COALESCERE
- NULLIF

Funzioni di conversione

- CAST (per i tipi di dati supportati)

Funzioni di data

- DATA_AGGIUNGI
- DATE_DIFF
- ESTRARRE
- A_STRINGA
- TO_TIMESTAMP

- UTCNOW

Funzioni stringa

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

Utilizzare la crittografia lato server

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

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

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

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

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

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

Utilizzare SSE

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

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

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

- "MettiOggetto"
- "CopiaOggetto"
- "CreaCaricamentoMultiparte"

Utilizzare SSE-C

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

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

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

- "OttieniOggetto"
- "HeadObject"
- "MettiOggetto"
- "CopiaOggetto"
- "CreaCaricamentoMultiparte"
- "CaricaParte"
- "CaricaParteCopia"

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

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

- Devi usare https.

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

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

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

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

Informazioni correlate

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

CopiaOggetto

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

Risolvere i conflitti

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

Dimensione dell'oggetto

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

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

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

Caratteri UTF-8 nei metadati utente

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

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

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

  Puoi specificare `REPLACE` per sovrascrivere i metadati esistenti durante la copia dell'oggetto o per aggiornare i metadati dell'oggetto.
- `x-amz-storage-class`
- `x-amz-tagging-directive`: Il valore predefinito è `COPY` , che consente di copiare l'oggetto e tutti i tag.

  Puoi specificare `REPLACE` per sovrascrivere i tag esistenti durante la copia dell'oggetto o per aggiornare i tag.
- Intestazioni delle richieste di blocco degli oggetti S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se viene effettuata una richiesta senza queste intestazioni, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .
- Intestazioni delle richieste SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VedereIntestazioni 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 quel valore di checksum nel nuovo oggetto. Questo comportamento si applica indipendentemente dal fatto che tu provi o meno a utilizzare `x-amz-checksum-algorithm` nella richiesta dell'oggetto.

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

Opzioni di classe di archiviazione

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

Utilizzo di x-amz-copy-source in CopyObject

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

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

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la crittografia di un oggetto esistente sul posto. Se fornisci il `x-amz-server-side-encryption`

intestazione o il `x-amz-server-side-encryption-customer-algorithm` intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented` .

- L'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.

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

Intestazioni di richiesta per la crittografia lato server

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

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

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

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

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

Controllo delle versioni

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

OttieniOggetto

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

GetObject e oggetti multipart

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

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

Caratteri UTF-8 nei metadati utente

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

Intestazione della richiesta supportata

È supportata la seguente intestazione di richiesta:

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

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

Intestazione della richiesta non supportata

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

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

Controllo delle versioni

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

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

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

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

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

Comportamento di GetObject per gli oggetti Cloud Storage Pool

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

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

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

Oggetti multiparte o segmentati in un pool di archiviazione cloud

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

In questi casi:

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

GetObject e replicazione tra griglie

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

Griglia	Stato di replicazione
Fonte	• **COMPLETO**: La replica è riuscita. • **IN ATTESA**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

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

HeadObject

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

HeadObject e oggetti multiparte

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

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

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le

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

Intestazione della richiesta supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`

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

Intestazione della richiesta non supportata

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

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

Controllo delle versioni

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

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

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

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

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

Risposte HeadObject per gli oggetti Cloud Storage Pool

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

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

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

Stato dell'oggetto	Risposta a HeadObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	`200 OK`(Non viene restituita alcuna intestazione di risposta speciale.)

Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Finché l'oggetto non viene portato in uno stato non recuperabile, il valore per `expiry-date` è ambientato in un lontano futuro. Il momento esatto della transizione non è controllato dal sistema StorageGRID .

L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche sulla griglia	`200 OK`
	
	`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 ambientato in un lontano futuro.
	
	Nota: se la copia sulla griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario emettere un"Ripristina oggetto" richiedere di ripristinare la copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.

L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia sulla griglia	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Oggetto in fase di ripristino da uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Stato dell'oggetto	Risposta a HeadObject

Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	IL `expiry-date` indica quando l'oggetto nel Cloud Storage Pool tornerà a uno stato non recuperabile.

Oggetti multiparte o segmentati in Cloud Storage Pool

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

HeadObject e replicazione cross-grid

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

Griglia	Stato di replicazione
Fonte	• **COMPLETO**: La replica è riuscita. • **IN ATTESA**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

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

MettiOggetto

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

Risolvere i conflitti

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

Dimensione dell'oggetto

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

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

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

Dimensione dei metadati utente

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

Caratteri UTF-8 nei metadati utente

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

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

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

Limiti dei tag degli oggetti

Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole.

Proprietà dell'oggetto

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

- `Content-Encoding`

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

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

  La codifica di trasferimento in blocchi è supportata se `aws-chunked` viene utilizzata anche la firma del payload.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

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

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

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

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

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

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

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

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

  VedereIntestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

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

Opzioni di classe di archiviazione

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

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

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

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

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

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

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

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

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

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

Intestazioni di richiesta per la crittografia lato server

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

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

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

- **SSE-C**: utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo

oggetto.

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

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

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

Controllo delle versioni

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

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

Calcoli della firma per l'intestazione di autorizzazione

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

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

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

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

Informazioni correlate

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

Ripristina oggetto

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

Tipo di richiesta supportato

StorageGRID supporta solo le richieste RestoreObject per ripristinare un oggetto. Non supporta il `SELECT` tipo

di restauro. Seleziona le richieste di ritorno `XNotImplemented` .

Controllo delle versioni

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

Comportamento di RestoreObject sugli oggetti Cloud Storage Pool

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

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

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM oppure l'oggetto non si trova in un Cloud Storage Pool	`403 Forbidden` , `InvalidObjectState`
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	`200 OK`Non vengono apportate modifiche. **Nota**: prima che un oggetto sia passato a uno stato non recuperabile, non è possibile modificarne lo stato. `expiry-date` .
Oggetto passato a uno stato non recuperabile	`202 Accepted`Ripristina una copia recuperabile dell'oggetto nel Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto torna a uno stato non recuperabile. Facoltativamente, utilizzare il `Tier` elemento di richiesta per determinare quanto tempo impiegherà il processo di ripristino per essere completato(`Expedited` , `Standard` , O `Bulk`). Se non specifichi `Tier` , IL `Standard` viene utilizzato il livello. **Importante**: se un oggetto è stato trasferito a S3 Glacier Deep Archive o il pool di archiviazione cloud utilizza l'archiviazione BLOB di Azure, non è possibile ripristinarlo utilizzando `Expedited` livello. 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 in uno stato recuperabile, è possibile modificarne lo stato `expiry-date` riemettendo la richiesta RestoreObject con un nuovo valore per `Days` . La data di ripristino viene aggiornata in base al momento della richiesta.

SelezionaOggettoContenuto

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

Per maggiori informazioni vedere "Riferimento API di Amazon Simple Storage Service: SelectObjectContent" .

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Hai `s3:GetObject` autorizzazione per l'oggetto che si desidera interrogare.
- L'oggetto che si desidera interrogare deve essere in uno dei seguenti formati:
  - **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
  - **Parquet**. Requisiti aggiuntivi per gli oggetti Parquet:
    - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
    - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
    - La dimensione massima del gruppo di righe non compresso è 512 MB.
    - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
    - Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.
- La lunghezza massima dell'espressione SQL è di 256 KB.
- Ogni record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi della richiesta CSV

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

Esempio di sintassi della richiesta Parquet

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

Esempio di query SQL

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

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

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

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

Esempio di utilizzo di AWS-CLI (CSV)

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

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

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 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, hanno questo aspetto:

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

Operazioni per caricamenti multiparte

Operazioni per caricamenti multiparte

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

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

- Non dovresti superare i 1.000 caricamenti multipart simultanei in un singolo bucket perché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID impone limiti dimensionali AWS per le parti multiparte. I client S3 devono seguire queste linee guida:
  - Ogni parte di un caricamento multiparte deve avere una dimensione compresa tra 5 MiB (5.242.880 byte) e 5 GiB (5.368.709.120 byte).
  - L'ultima parte può essere inferiore a 5 MiB (5.242.880 byte).
  - In generale, le dimensioni delle parti dovrebbero essere le più grandi possibile. Ad esempio, utilizzare dimensioni di parti pari a 5 GiB per un oggetto da 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce il sovraccarico dei metadati StorageGRID .
  - Per oggetti di dimensioni inferiori a 5 GiB, si consiglia di utilizzare il caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte mentre viene ingerito e per l'oggetto nel suo complesso quando il caricamento multiparte viene completato, se la regola ILM utilizza Bilanciato o Rigoroso"opzione di ingestione" . È necessario essere consapevoli di come ciò influisce 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. Ogni parte non posizionata

correttamente viene messa in coda per la rivalutazione ILM e successivamente spostata nella posizione corretta.

    - Quando si valuta l'ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate 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 vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2 al momento dell'acquisizione. Tuttavia, quando l'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 ingerito tramite caricamento multiparte,"soglia di segmentazione degli oggetti (1 GiB)" non viene applicato.
- Se necessario, puoi utilizzare"crittografia lato server" con caricamenti in più parti. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere `x-amz-server-side-encryption` intestazione della richiesta solo nella richiesta CreateMultipartUpload. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), è necessario specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni successiva richiesta UploadPart.

Operazione	Implementazione
Annulla caricamento multiparte	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
Caricamento multiparte completo	Vedere"Caricamento multiparte completo"
CreaCaricamentoMultiparte (in precedenza denominato Avvia caricamento multiparte)	Vedere"CreaCaricamentoMultiparte"
Caricamenti multiparte di List	Vedere"Caricamenti multiparte di List"
ElencoParti	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
CaricaParte	Vedere"CaricaParte"
CaricaParteCopia	Vedere"CaricaParteCopia"

Caricamento multiparte completo

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 `partNumber` parametro di richiesta con CompleteMultipartUpload. Il parametro può iniziare con qualsiasi valore.

Risolvere i conflitti

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

  IL `x-amz-storage-class` l'intestazione influisce sul numero di copie dell'oggetto che StorageGRID crea se la regola ILM corrispondente specifica"Opzione di commit doppio o di ingestione bilanciata" .

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

Controllo delle versioni

Questa operazione completa un caricamento in più parti. Se per un bucket è abilitato il controllo delle versioni, la versione dell'oggetto viene creata dopo il completamento del caricamento multiparte.

Se il controllo delle versioni è abilitato per un bucket, univoco `versionId` viene generato automaticamente

per la versione dell'oggetto memorizzato. Questo `versionId` viene restituito anche nella risposta utilizzando il `x-amz-version-id` intestazione di risposta.

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

> Quando il controllo delle versioni è abilitato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se sono stati completati caricamenti multiparte simultanei sulla stessa chiave oggetto. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e quindi avviare e completare prima un altro caricamento multiparte sulla stessa chiave dell'oggetto. Nei bucket senza controllo delle versioni, ha la precedenza il caricamento multiparte completato per ultimo.

Replicazione, notifica o notifica dei metadati non riuscita

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

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

Fare riferimento a "Risolvere i problemi dei servizi della piattaforma" .

CreaCaricamentoMultiparte

L'operazione CreateMultipartUpload (in precedenza denominata Initiate Multipart Upload) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

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

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

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

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

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

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

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

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

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

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

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

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

stato creato l'oggetto. Per esempio:

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

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

> Aggiunta `creation-time` poiché i metadati definiti dall'utente non sono consentiti se si aggiunge un oggetto a un bucket in cui è abilitata la conformità legacy. Verrà restituito un errore.

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

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

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

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

    Intestazioni di richiesta per la crittografia lato server

> Per informazioni su come StorageGRID gestisce i caratteri UTF-8, vedere"MettiOggetto" .

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multiparte con la 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 queste intestazioni nella richiesta CreateMultipartUpload (e in ogni successiva richiesta UploadPart) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo

oggetto.

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

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

Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata:

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

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

Controllo delle versioni

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

Caricamenti multiparte di List

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`

Controllo delle versioni

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

CaricaParte

L'operazione UploadPart carica una parte in un caricamento 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 hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in"Utilizzare la crittografia lato server" .

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

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

Controllo delle versioni

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

CaricaParteCopia

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

L'operazione UploadPartCopy è implementata con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.

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

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Intestazioni di richiesta per la crittografia lato server

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

- `x-amz-server-side-encryption-customer-algorithm`: 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 sorgente è 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`: Specifica la chiave di crittografia fornita al momento della creazione dell'oggetto sorgente.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 fornito quando hai creato l'oggetto sorgente.

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

Controllo delle versioni

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

Risposte di errore

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

Codici di errore API S3 supportati

Nome	Stato HTTP
Accesso negato	403 Proibito
BadDigest	400 Richiesta non valida
BucketAlreadyExists	409 Conflitto
BucketNotEmpty	409 Conflitto
Corpo incompleto	400 Richiesta non valida
Errore interno	500 Errore interno del server
ID chiave di accesso non valido	403 Proibito
Argomento non valido	400 Richiesta non valida
NomeBucketNonValido	400 Richiesta non valida
StatoBucketNonValido	409 Conflitto
InvalidDigest	400 Richiesta non valida
Errore algoritmo di crittografia non valido	400 Richiesta non valida
Parte non valida	400 Richiesta non valida
OrdineParteNonValido	400 Richiesta non valida
Intervallo non valido	416 Intervallo richiesto non soddisfacibile
Richiesta non valida	400 Richiesta non valida
Classe di archiviazione non valida	400 Richiesta non valida
Tag non valido	400 Richiesta non valida
URI non valido	400 Richiesta non valida
KeyTooLong	400 Richiesta non valida
XML malformato	400 Richiesta non valida

Nome	Stato HTTP
Metadati troppo grandi	400 Richiesta non valida
Metodo non consentito	405 Metodo non consentito
Lunghezza del contenuto mancante	411 Lunghezza richiesta
Errore mancante nel corpo della richiesta	400 Richiesta non valida
MissingSecurityHeader	400 Richiesta non valida
NoSuchBucket	404 Non trovato
Nessuna chiave	404 Non trovato
NoSuchUpload	404 Non trovato
Non implementato	501 Non implementato
NoSuchBucketPolicy	404 Non trovato
Errore ObjectLockConfigurationNotFound	404 Non trovato
Precondizione fallita	412 Precondizione fallita
RequestTimeTooSkewed	403 Proibito
Servizio non disponibile	503 Servizio non disponibile
Firma non corrisponde	403 Proibito
Troppi secchi	400 Richiesta non valida
UserKeyMustBeSpecified	400 Richiesta non valida

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket conforme legacy	400 Richiesta non valida

Nome	Descrizione	Stato HTTP
XBucketPolicyParseException	Impossibile analizzare il JSON del criterio del bucket ricevuto.	400 Richiesta non valida
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 Proibito
XComplianceReducedRedundancyForbidden	La ridondanza ridotta non è consentita nel bucket Compliant legacy	400 Richiesta non valida
XMaxBucketPolicyLengthExceeded	La tua policy supera la lunghezza massima consentita per il bucket.	400 Richiesta non valida
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 Richiesta non valida
XNoSuchBucketCompliance	Nel bucket specificato non è abilitata la conformità legacy.	404 Non trovato
XNon accettabile	La richiesta contiene una o più intestazioni di accettazione che non è stato possibile soddisfare.	406 Non accettabile
XNonImplementato	La richiesta da te fornita implica una funzionalità non implementata.	501 Non implementato

Informazioni sul copyright

Informazioni sul marchio commerciale