Operazioni e limitazioni supportate dall'API REST S3

StorageGRID

NetApp
October 03, 2025

Sommario

Operazioni e limitazioni supportate dall'API REST S3

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

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

- "Autenticare le richieste"
- "Operazioni sul servizio"
- "Operazioni sui bucket"
- "Operazioni personalizzate sui bucket"
- "Operazioni sugli oggetti"
- "Operazioni per caricamenti multiparte"
- "Risposte agli errori"

Gestione della data

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

Il sistema StorageGRID supporta solo i formati di data HTTP validi per tutte le intestazioni che accettano i valori di data. La parte temporale della data può essere specificata nel formato GMT (Greenwich Mean Time) o UTC (Universal Coordinated Time) senza offset del fuso orario (deve essere specificato ++1). Se si include `x-amz-date` Intestazione nella richiesta, sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza la firma AWS versione 4, il `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 intestazioni di richiesta comuni definite dal *riferimento API del servizio di storage semplice*, con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per firma AWS versione 2 Supporto per firma AWS versione 4, con le seguenti eccezioni: • Il valore SHA256 non viene calcolato per il corpo della richiesta. Il valore inviato dall'utente viene accettato senza convalida, come se il valore `UNSIGNED-PAYLOAD` è stato fornito per `x-amz-content-sha256` intestazione.

Intestazione della richiesta	Implementazione
x-amz-security-token	Non implementato. Ritorno `XNotImplemented`.

Intestazioni di risposta comuni

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

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

Informazioni correlate

"Documentazione Amazon Web Services (AWS): Riferimento API Amazon Simple Storage Service"

Autenticare le richieste

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

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

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

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

Utilizzo dell'intestazione autorizzazione HTTP

Il protocollo HTTP `Authorization` Header viene utilizzato da tutte le operazioni API S3, ad eccezione delle richieste anonime, laddove consentito dalla policy bucket. Il `Authorization` header contiene tutte le informazioni di firma richieste per autenticare una richiesta.

Utilizzo dei parametri di query

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

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
OTTIENI assistenza	Implementato con tutti i comportamenti REST API di Amazon S3.
OTTIENI l'utilizzo dello storage	La richiesta GET Storage Usage indica la quantità totale di storage in uso da un account e per ciascun bucket associato all'account. Si tratta di un'operazione sul servizio con un percorso di / e un parametro di query personalizzato (`?x-ntap-sg-usage`) aggiunto.
OPZIONI /	Le applicazioni client possono avere problemi `OPTIONS /` Richiede alla porta S3 su un nodo di storage, senza fornire credenziali di autenticazione S3, di determinare se il nodo di storage è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di storage è inattivo.

Informazioni correlate

"OTTIENI la richiesta di utilizzo dello storage"

Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 1,000 bucket per ciascun account tenant S3.

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

"Documentazione di Amazon Web Services (AWS): Limitazioni e limitazioni del bucket"

"Nomi di dominio degli endpoint per la richiesta S3"

LE operazioni GET bucket (Elenca oggetti) e GET Bucket Versions supportano i controlli di coerenza StorageGRID.

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

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

Operazione	Implementazione
ELIMINA bucket	Implementato con tutti i comportamenti REST API di Amazon S3.

Operazione	Implementazione
ELIMINA cors bucket	Questa operazione elimina la configurazione CORS per il bucket.
ELIMINA crittografia bucket	Questa operazione elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non vengono crittografati.
ELIMINA ciclo di vita bucket	Questa operazione elimina la configurazione del ciclo di vita dal bucket.
ELIMINA policy bucket	Questa operazione elimina la policy associata al bucket.
ELIMINA replica bucket	Questa operazione elimina la configurazione di replica collegata al bucket.
ELIMINA tag bucket	Questa operazione utilizza `tagging` sottorisorsa per rimuovere tutti i tag da un bucket.
GET Bucket (Elenca oggetti), versione 1 e versione 2	Questa operazione restituisce alcuni o tutti (fino a 1,000) gli oggetti in un bucket. La classe Storage per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con `REDUCED_REDUNDANCY` opzione classe di storage: • `STANDARD`, Che indica che l'oggetto è memorizzato in un pool di storage costituito da nodi di storage. • `GLACIER`, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. Se il bucket contiene un numero elevato di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune `CommonPrefixes` che non contengono chiavi.
OTTIENI acl bucket	Questa operazione restituisce una risposta positiva e l'ID, il DisplayName e il permesso del proprietario del bucket, indicando che il proprietario ha pieno accesso al bucket.
OTTIENI bucket cors	Questa operazione restituisce il `cors` configurazione per il bucket.

Operazione	Implementazione
OTTIENI la crittografia bucket	Questa operazione restituisce la configurazione di crittografia predefinita per il bucket.
OTTIENI il ciclo di vita del bucket	Questa operazione restituisce la configurazione del ciclo di vita del bucket.
OTTIENI posizione bucket	Questa operazione restituisce la regione impostata utilizzando `LocationConstraint` Elemento nella richiesta PUT bucket. Se l'area del bucket è `us-east-1`, viene restituita una stringa vuota per la regione.
OTTIENI notifica bucket	Questa operazione restituisce la configurazione di notifica allegata al bucket.
SCARICA le versioni degli oggetti bucket	Con l'accesso IN LETTURA su un bucket, questa operazione con `versions` la sottorisorsa elenca i metadati di tutte le versioni degli oggetti nel bucket.
OTTIENI la policy bucket	Questa operazione restituisce la policy allegata al bucket.
OTTIENI la replica bucket	Questa operazione restituisce la configurazione di replica collegata al bucket.
OTTIENI il contrassegno bucket	Questa operazione utilizza `tagging` sottorisorsa per restituire tutti i tag per un bucket.
SCARICA la versione di bucket	Questa implementazione utilizza `versioning` sottorisorsa per restituire lo stato di versione di un bucket. Lo stato di versione restituito indica se il bucket è "Unversioned" o se la versione del bucket è "enabled" o "Suspended".
OTTIENI configurazione blocco oggetto	Questa operazione determina se S3 Object Lock è attivato per un bucket. "Utilizzo di S3 Object Lock"
BENNA PER LA TESTA	Questa operazione determina se esiste un bucket e se si dispone dell'autorizzazione per accedervi.

Operazione	Implementazione
METTI bucket	Questa operazione crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). ◦ Deve essere conforme al DNS. ◦ Deve contenere almeno 3 e non più di 63 caratteri. ◦ Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. ◦ Non deve essere simile a un indirizzo IP formattato con testo. ◦ Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. • Per impostazione predefinita, i bucket vengono creati in `us-east-1` regione; tuttavia, è possibile utilizzare `LocationConstraint` elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza `LocationConstraint` È necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API Grid Management. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare. **Nota**: Si verifica un errore se la richiesta PUT bucket utilizza un'area non definita in StorageGRID. • È possibile includere `x-amz-bucket-object-lock-enabled` Richiedi intestazione per creare un bucket con blocco oggetti S3 attivato. È necessario attivare il blocco oggetti S3 quando si crea il bucket. Non è possibile aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea il bucket. "Utilizzo di S3 Object Lock"

Operazione	Implementazione
METTI cors bucket	Questa operazione imposta la configurazione del CORS per un bucket in modo che il bucket possa gestire le richieste di origine incrociata. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Si supponga, ad esempio, di utilizzare un bucket S3 denominato `images` per memorizzare le immagini. Impostando la configurazione CORS per `images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito web `http://www.example.com`.
METTI la crittografia bucket	Questa operazione imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è attivata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati.StorageGRID supporta la crittografia lato server con le chiavi gestite da StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare `SSEAlgorithm` parametro a. `AES256`e non utilizzare `KMSMasterKeyID` parametro. La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento degli oggetti specifica già la crittografia, ovvero se la richiesta include `x-amz-server-side-encryption-*` intestazione della richiesta).

Operazione	Implementazione
METTI IL ciclo di vita del bucket	Questa operazione 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) • Non currentVersionExpiration (non currentDays) • Filtro (prefisso, tag) • Stato • ID StorageGRID non supporta queste azioni: • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transizione Per capire come l'azione di scadenza in un ciclo di vita del bucket interagisce con le istruzioni di posizionamento di ILM, consulta "funzionamento di ILM durante la vita di un oggetto" nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni. **Nota**: La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

Operazione	Implementazione

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

METTI la policy bucket	Questa operazione imposta la policy associata al bucket.

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

Operazione	Implementazione
INSERIRE il contrassegno bucket	Questa operazione utilizza `tagging` sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket. • Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode. • I valori dei tag possono contenere fino a 256 caratteri Unicode. • Chiave e valori distinguono tra maiuscole e minuscole.
METTERE il bucket in versione	Questa implementazione utilizza `versioning` sottorisorsa per impostare lo stato di versione di un bucket esistente. È possibile impostare lo stato di versione con uno dei seguenti valori: • Enabled (attivato): Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco. • Suspended (sospeso): Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione `null`.

Informazioni correlate

"Documentazione Amazon Web Services (AWS): Replica tra regioni"

"Controlli di coerenza"

"OTTIENI la richiesta dell'ultimo accesso al bucket"

"Policy di accesso a bucket e gruppi"

"Utilizzo di S3 Object Lock"

"Operazioni S3 registrate nei registri di audit"

"Gestire gli oggetti con ILM"

"Utilizzare un account tenant"

Creazione di una configurazione del ciclo di vita S3

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono cancellati dal sistema StorageGRID.

Il semplice esempio di questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando alcuni oggetti vengono cancellati (scaduti) da specifici bucket S3. L'esempio in questa sezione è a solo scopo illustrativo. Per i dettagli completi sulla creazione delle configurazioni del ciclo di vita S3, consulta la sezione sulla gestione del ciclo di vita degli oggetti nella *Amazon Simple Storage Service Developer Guide*. Nota: StorageGRID supporta solo le azioni di scadenza e non le azioni di transizione.

"Amazon Simple Storage Service Developer Guide: Gestione del ciclo di vita degli oggetti"

Che cos'è una configurazione del ciclo di vita

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in specifici bucket S3. Ogni regola specifica quali oggetti sono interessati e quando scadranno (in una data specifica o dopo un certo numero di giorni).

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: Consente di eliminare un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dalla data di acquisizione dell'oggetto.
- NoncurrentVersionExpiration (NoncurrentExpiration versione): Consente di eliminare un oggetto quando viene raggiunto un numero di giorni specificato, a partire da quando l'oggetto è diventato non corrente.
- Filtro (prefisso, tag)
- Stato
- ID

Se si applica una configurazione del ciclo di vita a un bucket, le impostazioni del ciclo di vita del bucket sovrascrivono sempre le impostazioni ILM di StorageGRID. StorageGRID utilizza le impostazioni di scadenza per il bucket, non ILM, per determinare se eliminare o conservare oggetti specifici.

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora applicabili all'oggetto. Oppure, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni di posizionamento ILM per l'oggetto. Per ulteriori informazioni, vedere "funzionamento di ILM durante la vita di un oggetto" nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

> La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- ELIMINA ciclo di vita bucket
- OTTIENI il ciclo di vita del bucket
- METTI IL ciclo di vita del bucket

Creazione della configurazione del ciclo di vita

Come primo passo nella creazione di una configurazione del ciclo di vita, è possibile creare un file JSON che includa una o più regole. Ad esempio, questo file JSON include tre regole, come segue:

1. La regola 1 si applica solo agli oggetti che corrispondono al prefisso `category1/` e che hanno un `key2` valore di `tag2`. Il `Expiration` Il parametro specifica che gli oggetti corrispondenti al filtro scadranno alla

mezzanotte del 22 agosto 2020.

2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2/`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno 100 giorni dopo l'acquisizione.

> Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato acquisito. Se la data corrente supera la data di acquisizione più il numero di giorni, alcuni oggetti potrebbero essere rimossi dal bucket non appena viene applicata la configurazione del ciclo di vita.

3. La regola 3 si applica solo agli oggetti che corrispondono al prefisso `category3/`. Il `Expiration` parametro specifica che qualsiasi versione non corrente degli oggetti corrispondenti scadrà 50 giorni dopo che diventeranno non aggiornati.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Applicazione di una configurazione del ciclo di vita a un bucket

Dopo aver creato il file di configurazione del ciclo di vita, lo si applica a un bucket inviando una richiesta DI ciclo di vita PUT bucket.

Questa richiesta applica la configurazione del ciclo di vita nel file di esempio agli oggetti in un bucket denominato `testbucket`:bucket

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Per verificare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, emettere una richiesta DI ciclo di vita GET Bucket. Ad esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Una risposta corretta elenca la configurazione del ciclo di vita appena applicata.

La convalida della scadenza del ciclo di vita del bucket si applica a un oggetto

È possibile determinare se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico quando si invia una richiesta DI oggetto PUT, HEAD o GET. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata associata.

> Poiché il ciclo di vita del bucket ha la priorità su ILM, il sistema `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere "come viene determinata la conservazione degli oggetti" nelle istruzioni per l'esecuzione dell'amministrazione di StorageGRID.

Ad esempio, questa richiesta DI oggetti PUT è stata emessa il 22 giugno 2020 e inserisce un oggetto in `testbucket` bucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta corretta indica che l'oggetto scadrà tra 100 giorni (01 ottobre 2020) e che corrisponde alla regola 2 della configurazione del ciclo di vita.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Ad esempio, questa richiesta di oggetto HEAD è stata utilizzata per ottenere metadati per lo stesso oggetto nel bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La risposta di successo include i metadati dell'oggetto e indica che l'oggetto scadrà tra 100 giorni e che corrisponde alla regola 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Informazioni correlate

"Operazioni sui bucket"

"Gestire gli oggetti con ILM"

Operazioni personalizzate sui bucket

Il sistema StorageGRID supporta operazioni bucket personalizzate aggiunte all'API REST S3 e specifiche del sistema.

La seguente tabella elenca le operazioni di bucket personalizzate supportate da StorageGRID.

Operazione	Descrizione	Per ulteriori informazioni
COERENZA del bucket	Restituisce il livello di coerenza applicato a un determinato bucket.	"OTTIENI una richiesta di coerenza bucket"

Operazione	Descrizione	Per ulteriori informazioni
METTI la coerenza del bucket	Imposta il livello di coerenza applicato a un bucket specifico.	"INSERIRE la richiesta di coerenza del bucket"
OTTIENI l'ultimo tempo di accesso a bucket	Restituisce se gli ultimi aggiornamenti dell'ora di accesso sono attivati o disattivati per un bucket specifico.	"OTTIENI la richiesta dell'ultimo accesso al bucket"
TEMPO ULTIMO accesso bucket	Consente di attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso per un determinato bucket.	"METTI richiesta dell'ultimo tempo di accesso al bucket"
ELIMINA la configurazione di notifica dei metadati del bucket	Elimina l'XML di configurazione della notifica dei metadati associato a un bucket specifico.	"ELIMINA la richiesta di configurazione della notifica dei metadati del bucket"
OTTIENI la configurazione della notifica dei metadati del bucket	Restituisce l'XML di configurazione della notifica dei metadati associato a un bucket specifico.	"OTTIENI una richiesta di configurazione per la notifica dei metadati del bucket"
INSERIRE la configurazione della notifica dei metadati del bucket	Configura il servizio di notifica dei metadati per un bucket.	"INSERIRE la richiesta di configurazione della notifica dei metadati del bucket"
APPORTARE modifiche al bucket per la conformità	Obsoleto e non supportato: Non è più possibile creare nuovi bucket con Compliance abilitata.	"Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket"
OTTIENI la compliance del bucket	Obsoleto ma supportato: Restituisce le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.	"Deprecato: OTTIENI una richiesta di conformità bucket"
METTI la compliance del bucket	Obsoleto ma supportato: Consente di modificare le impostazioni di conformità per un bucket compatibile esistente.	"Deprecato: INSERIRE la richiesta di conformità del bucket"

Informazioni correlate

"Operazioni S3 registrate nei registri di audit"

Operazioni sugli oggetti

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

- "Utilizzo di S3 Object Lock"
- "Utilizzo della crittografia lato servver"
- "OTTIENI oggetto"
- "Oggetto TESTA"
- "RIPRISTINO POST-oggetto"
- "METTI oggetto"
- "METTI oggetto - Copia"

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

- I controlli di coerenza StorageGRID sono supportati da tutte le operazioni sugli oggetti, ad eccezione di quanto segue:
  - GET Object ACL (OTTIENI ACL oggetto)
  - `OPTIONS /`
  - METTERE in attesa legale l'oggetto
  - METTI la conservazione degli oggetti
- Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.
- Non è possibile accedere agli oggetti dati acquisiti nel sistema StorageGRID tramite Swift tramite S3.

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

Operazione	Implementazione
ELIMINA oggetto	Autenticazione multifattore (MFA) e intestazione della risposta `x-amz-mfa` non sono supportati. Durante l'elaborazione di una richiesta DI ELIMINAZIONE degli oggetti, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione non è temporaneamente disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito. **Versione** Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare `versionId` sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il `versionId` corrisponde a un indicatore 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 abilitato alla versione, si ottiene la generazione di un indicatore di eliminazione. Il `versionId` per il contrassegno di eliminazione viene restituito utilizzando `x-amz-version-id` intestazione della risposta e la `x-amz-delete-marker` l'intestazione della risposta viene restituita impostata su `true`. • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket sospeso della versione, si ottiene una cancellazione permanente di una versione 'null' già esistente o di un marker di eliminazione 'null' e la generazione di un nuovo marker di eliminazione 'null'. Il `x-amz-delete-marker` l'intestazione della risposta viene restituita impostata su `true`. **Nota**: In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione.
ELIMINARE più oggetti	Autenticazione multifattore (MFA) e intestazione della risposta `x-amz-mfa` non sono supportati. È possibile eliminare più oggetti nello stesso messaggio di richiesta.

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

Operazione	Implementazione
METTI oggetto - Copia	"METTI oggetto - Copia"
METTERE in attesa legale l'oggetto	"Utilizzo di S3 Object Lock"
METTI la conservazione degli oggetti	"Utilizzo di S3 Object Lock"

Operazione	Implementazione
INSERIRE tag degli oggetti	Utilizza `tagging` sottorisorsa per aggiungere un set di tag a un oggetto esistente. Implementato con tutti i comportamenti REST API di Amazon S3 **Aggiornamenti dei tag e comportamento di acquisizione** Quando si utilizza IL tag PUT Object per aggiornare i tag di un oggetto, StorageGRID non reinserisce l'oggetto. Ciò significa che l'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto. **Risoluzione dei conflitti** Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un'operazione. **Versione** Se il `versionId` il parametro query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione risposta impostata su `true`.

Informazioni correlate

"Controlli di coerenza"

"Operazioni S3 registrate nei registri di audit"

Utilizzo di S3 Object Lock

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato e specificare le impostazioni di conservazione fino alla data e conservazione legale per ogni versione dell'oggetto aggiunta a tale bucket.

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

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

Abilitazione di S3 Object Lock per un bucket

Se l'impostazione globale di blocco oggetti S3 è attivata per il sistema StorageGRID, è possibile attivare il blocco oggetti S3 quando si crea ciascun bucket. È possibile utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager.

  "Utilizzare un account tenant"

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

  "Operazioni sui bucket"

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

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni S3 Object Lock. StorageGRID non supporta la conservazione predefinita per gli oggetti nei bucket blocco oggetti S3, pertanto l'operazione DEL bucket CONFIGURAZIONE BLOCCO oggetti PUT non è supportata.

Determinare se S3 Object Lock (blocco oggetti S3) è attivato per un bucket

Per determinare se S3 Object Lock è attivato, utilizzare la richiesta GET Object Lock Configuration.

"Operazioni sui bucket"

Creazione di un oggetto con le impostazioni S3 Object Lock

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

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

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

  > Se si specifica `x-amz-object-lock-mode`, è inoltre necessario specificare `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
  - La data di conservazione deve essere in futuro.
- `x-amz-object-lock-legal-hold`

  Se la conservazione legale È ATTIVA (sensibile al maiuscolo/minuscolo), l'oggetto viene collocato sotto una conservazione legale. Se l'opzione Legal Hold è disattivata, non viene effettuata alcuna conservazione a fini giudiziari. Qualsiasi altro valore genera un errore 400 Bad Request (InvalidArgument).

Se si utilizza una di queste intestazioni di richiesta, tenere presente le seguenti restrizioni:

- Il `Content-MD5` l'intestazione della richiesta è obbligatoria, se presente `x-amz-object-lock-*` L'intestazione della richiesta è presente nella richiesta DELL'oggetto PUT. `Content-MD5` Non è richiesto per METTERE oggetto - copiare o avviare caricamento multiparte.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` L'intestazione della richiesta è presente, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta DI oggetti PUT supporta l'utilizzo di `x-amz-storage-class: REDUCED_REDUNDANCY` Per far corrispondere il comportamento di AWS. Tuttavia, quando un oggetto viene acquisito in un bucket con il blocco oggetti S3 attivato, StorageGRID eseguirà sempre un ingest a doppio commit.
- Una risposta successiva ALLA versione DELL'oggetto GET o HEAD includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e. `x-amz-object-lock-legal-hold`, se configurato e se il mittente della richiesta ha il corretto `s3:Get*` permessi.
- Una successiva richiesta DI versione DELL'oggetto DELETE o di versioni DELL'oggetto DELETE avrà esito negativo se è precedente alla data di conservazione o se è attiva una conservazione a fini giudiziari.

Aggiornamento delle impostazioni di blocco oggetti S3

Se è necessario aggiornare le impostazioni di conservazione o conservazione a fini giudiziari per una versione di oggetto esistente, è possibile eseguire le seguenti operazioni di sottorisorsa oggetto:

- `PUT Object legal-hold`

  Se IL nuovo valore di conservazione a fini giudiziari è ATTIVO, l'oggetto viene collocato sotto una conservazione a fini giudiziari. Se il valore di conservazione a fini giudiziari è OFF, la conservazione a fini giudiziari viene revocata.

- `PUT Object retention`
  - Il valore della modalità deve essere COMPLIANCE (distinzione tra maiuscole e minuscole).
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.

- Se una versione a oggetti ha un valore di conservazione esistente fino alla data odierna, è possibile aumentarlo. Il nuovo valore deve essere in futuro.

Informazioni correlate

"Gestire gli oggetti con ILM"

"Utilizzare un account tenant"

"METTI oggetto"

"METTI oggetto - Copia"

"Avvia caricamento multiparte"

"Versione degli oggetti"

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

Utilizzo della crittografia lato server

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

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

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

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

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

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

Utilizzo di SSE

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

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

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

- METTI oggetto
- METTI oggetto - Copia
- Avvia caricamento multiparte

Utilizzo di SSE-C.

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

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

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

- OTTIENI oggetto
- Oggetto TESTA
- METTI oggetto
- METTI oggetto - Copia
- Avvia caricamento multiparte
- Carica parte
- Carica parte - Copia

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

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

- È necessario utilizzare https.

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

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire il mapping delle chiavi di crittografia agli oggetti. StorageGRID non memorizza le chiavi di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia che fornisce per ciascun oggetto.

- Se il bucket è abilitato per la versione, ogni versione dell'oggetto deve disporre di una propria chiave di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia utilizzata per ciascuna versione dell'oggetto.
- Poiché si gestiscono le chiavi di crittografia sul lato client, è necessario gestire anche eventuali protezioni aggiuntive, come la rotazione delle chiavi, sul lato client.

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

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

Informazioni correlate

"OTTIENI oggetto"

"Oggetto TESTA"

"METTI oggetto"

"METTI oggetto - Copia"

"Avvia caricamento multiparte"

"Carica parte"

"Carica parte - Copia"

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

OTTIENI oggetto

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

Il parametro di richiesta del numero di parte non è supportato

Il `partNumber` Il parametro di richiesta non è supportato per le richieste DI oggetti GET. Non è possibile eseguire una richiesta GET per recuperare una parte specifica di un oggetto multiparte. Viene visualizzato un errore 501 non implementato con il seguente messaggio:

```
GET Object by partNumber is not implemented
```

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

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

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

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

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

UTF-8 caratteri nei metadati dell'utente

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

Intestazione della richiesta non supportata

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

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

Versione

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

Comportamento di GET Object per gli oggetti Cloud Storage Pool

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

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

Stato dell'oggetto	Comportamento dell'oggetto GET
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	`200 OK` Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK` Viene recuperata una copia dell'oggetto.

Stato dell'oggetto	Comportamento dell'oggetto GET
Oggetto sottoposto a transizione in uno stato non recuperabile	`403 Forbidden, InvalidObjectState` Utilizzare una richiesta DI ripristino dell'oggetto POST per ripristinare lo stato recuperabile dell'oggetto.
Oggetto in fase di ripristino da uno stato non recuperabile	`403 Forbidden, InvalidObjectState` Attendere il completamento della richiesta DI ripristino dell'oggetto POST.
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` Viene recuperata una copia dell'oggetto.

Oggetti multiparte o segmentati in un pool di storage cloud

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

In questi casi:

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

Informazioni correlate

"Utilizzo della crittografia lato server"

"Gestire gli oggetti con ILM"

"RIPRISTINO POST-oggetto"

"Operazioni S3 registrate nei registri di audit"

Oggetto TESTA

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

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

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

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

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

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

UTF-8 caratteri nei metadati dell'utente

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

Intestazione della richiesta non supportata

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

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

Intestazioni di risposta per gli oggetti del Cloud Storage Pool

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

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

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

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

Stato dell'oggetto	Risposta all'oggetto HEAD

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

L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella griglia	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Il valore per `expiry-date` è impostato su un periodo di tempo lontano in futuro.
	
	Nota: Se la copia sulla griglia non è disponibile (ad esempio, un nodo di storage è inattivo), è necessario eseguire una richiesta DI ripristino DELL'oggetto POST per ripristinare la copia dal pool di storage cloud prima di poter recuperare l'oggetto.

L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella griglia	`200 OK`
	
	`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 all'oggetto HEAD

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 verrà riportato in uno stato non recuperabile.

Oggetti multiparte o segmentati in un pool di storage cloud

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

Versione

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

Informazioni correlate

"Utilizzo della crittografia lato server"

"Gestire gli oggetti con ILM"

"RIPRISTINO POST-oggetto"

"Operazioni S3 registrate nei registri di audit"

RIPRISTINO POST-oggetto

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

Tipo di richiesta supportato

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

Versione

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

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

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

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

Stato dell'oggetto	Comportamento del ripristino degli oggetti POST
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	`403 Forbidden`, `InvalidObjectState`
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	`200 OK` Non vengono apportate modifiche. **Nota**: Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificarne lo stato `expiry-date`.
Oggetto sottoposto a transizione in 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 viene riportato in uno stato non recuperabile. In alternativa, utilizzare `Tier` elemento request per determinare il tempo necessario per il completamento del processo di ripristino (`Expedited`, `Standard`, o. `Bulk`). Se non si specifica `Tier`, il `Standard` viene utilizzato il tier. **Attenzione**: Se un oggetto è stato spostato in S3 Glacier Deep Archive o il Cloud Storage Pool utilizza Azure Blob Storage, non è possibile ripristinarlo utilizzando `Expedited` tier. Viene visualizzato il seguente errore `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.
Oggetto in fase di ripristino da uno stato non recuperabile	`409 Conflict`, `RestoreAlreadyInProgress`

Stato dell'oggetto	Comportamento del ripristino degli oggetti POST
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` **Nota:** se un oggetto è stato ripristinato a uno stato recuperabile, è possibile modificarne lo stato `expiry-date` Inviando nuovamente la richiesta DI ripristino dell'oggetto POST con un nuovo valore per `Days`. La data di ripristino viene aggiornata in relazione all'ora della richiesta.

Informazioni correlate

"Gestire gli oggetti con ILM"

"Oggetto TESTA"

"Operazioni S3 registrate nei registri di audit"

METTI oggetto

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

Risoluzione dei conflitti

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

Dimensione dell'oggetto

StorageGRID supporta oggetti di dimensioni fino a 5 TB.

Dimensione dei metadati dell'utente

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

UTF-8 caratteri nei metadati dell'utente

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

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

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

Limiti tag oggetto

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

Proprietà degli oggetti

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

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

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

  ```
  x-amz-meta-<em>name</em>: <em>value</em>
  ```

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

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

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

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

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

"Utilizzo di S3 Object Lock"

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

"Operazioni e limitazioni supportate dall'API REST S3"

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

Opzioni di classe storage

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

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

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

- `STANDARD` (Impostazione predefinita)
  - **Doppio commit**: Se la regola ILM specifica l'opzione doppio commit per il comportamento di Ingest, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita in

un nodo di storage diverso (doppio commit). Una volta valutato l'ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.

  - **Balanced**: Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

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

- `REDUCED_REDUNDANCY`

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

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

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

Specificare `REDUCED_REDUNDANCY` influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto eseguite quando l'oggetto viene valutato dal criterio ILM attivo e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

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

Intestazioni di richiesta per la crittografia lato server

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

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

univoca che si fornisce e si gestisce.

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

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

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

Versione

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

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

Informazioni correlate

"Gestire gli oggetti con ILM"

"Operazioni sui bucket"

"Operazioni S3 registrate nei registri di audit"

"Utilizzo della crittografia lato server"

"Come configurare le connessioni client"

METTI oggetto - Copia

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

Risoluzione dei conflitti

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

Dimensione dell'oggetto

StorageGRID supporta oggetti di dimensioni fino a 5 TB.

UTF-8 caratteri nei metadati dell'utente

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

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

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

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

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

"Utilizzo di S3 Object Lock"

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

- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

"Intestazioni di richiesta per la crittografia lato server"

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

Opzioni di classe storage

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

Se l'origine e la destinazione corrispondono, e il `x-amz-metadata-directive` l'intestazione è specificata

come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non reinserisce l'oggetto. Questo ha due conseguenze importanti:

- Non è possibile utilizzare PUT Object - Copy per crittografare un oggetto esistente o per modificare la crittografia di un oggetto esistente. Se si fornisce `x-amz-server-side-encryption` o il `x-amz-server-side-encryption-customer-algorithm` Intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented`.
- L'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.

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

Intestazioni di richiesta per la crittografia lato server

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

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

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

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

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

Versione

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

Informazioni correlate

"Gestire gli oggetti con ILM"

"Utilizzo della crittografia lato server"

"Operazioni S3 registrate nei registri di audit"

"METTI oggetto"

Operazioni per caricamenti multiparte

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

- "Elenca caricamenti multiparte"
- "Avvia caricamento multiparte"
- "Carica parte"
- "Carica parte - Copia"
- "Caricamento multiparte completo"

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

- Non superare i 1,000 caricamenti simultanei di più parti in un singolo bucket, perché i risultati delle query di upload di List Multipart per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multicpart. I client S3 devono seguire queste linee guida:
  - Ciascuna parte di un caricamento multiparte deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).
  - L'ultima parte può essere inferiore a 5 MiB (5,242,880 byte).
  - In generale, le dimensioni delle parti devono essere il più grandi possibile. Ad esempio, utilizzare le dimensioni delle parti di 5 GiB per un oggetto 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce l'overhead dei metadati StorageGRID.
  - Per gli oggetti di dimensioni inferiori a 5 GiB, prendere in considerazione l'utilizzo di un caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte durante l'acquisizione e per l'oggetto nel suo complesso al termine del caricamento multiparte, se la regola ILM utilizza il comportamento di acquisizione rigoroso o bilanciato. Devi essere consapevole di come questo influisca sul posizionamento di oggetti e parti:
  - Se ILM cambia mentre è in corso un caricamento S3 multiparte, quando il caricamento multiparte

completa alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti. Tutte le parti non posizionate correttamente vengono messe in coda per la rivalutazione ILM e spostate nella posizione corretta in un secondo momento.

  - Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. Quando ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.

- Tutte le operazioni di caricamento multiparte supportano i controlli di coerenza StorageGRID.
- Se necessario, è possibile utilizzare la crittografia lato server con upload multiparte. 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 di avvio caricamento multiparte. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta Initiate Multipart Upload (Avvia caricamento multiparte) e in ogni richiesta successiva di caricamento parte.

Operazione	Implementazione
Elenca caricamenti multiparte	Vedere "Elenca caricamenti multiparte"
Avvia caricamento multiparte	Vedere "Avvia caricamento multiparte"
Carica parte	Vedere "Carica parte"
Carica parte - Copia	Vedere "Carica parte - Copia"
Caricamento multiparte completo	Vedere "Caricamento multiparte completo"
Interrompi caricamento multiparte	Implementato con tutti i comportamenti REST API di Amazon S3
Elencare le parti	Implementato con tutti i comportamenti REST API di Amazon S3

Informazioni correlate

"Controlli di coerenza"

"Utilizzo della crittografia lato server"

Elenca caricamenti multiparte

L'operazione List Multippart Uploads elenca i caricamenti multiparte in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`

- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

Il `delimiter` il parametro della richiesta non è supportato.

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando viene eseguita l'operazione completa di caricamento multiparte, il punto in cui vengono creati gli oggetti (e la versione, se applicabile).

Avvia caricamento multiparte

L'operazione Initiate Multippart Upload (Avvia caricamento multiparte) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

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

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

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

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

    Se StorageGRID è in grado di creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), l' `x-amz-storage-class` l'intestazione non ha alcun effetto.
- `REDUCED_REDUNDANCY`
  - **Commit doppio**: Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
  - **Balanced**: Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. Il `REDUCED_REDUNDANCY` L'opzione è preferibile quando la regola ILM corrispondente

all'oggetto crea una singola copia replicata. In questo caso, utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

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

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

Specificare `REDUCED_REDUNDANCY` influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto eseguite quando l'oggetto viene valutato dal criterio ILM attivo e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

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

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

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

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

  > Aggiunta `creation-time` Poiché i metadati definiti dall'utente non sono consentiti se si aggiunge un oggetto a un bucket che ha abilitato la conformità legacy. Viene restituito un errore.

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

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

"Utilizzo di S3 Object Lock"

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

"Operazioni e limitazioni supportate dall'API REST S3"

> Per informazioni su come StorageGRID gestisce i caratteri UTF-8, consultare la documentazione relativa A PUT Object.

Intestazioni di richiesta per la crittografia lato server

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

- **SSE**: Utilizzare la seguente intestazione nella richiesta di avvio caricamento multiparte se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste di carica parte.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilizzare tutte e tre queste intestazioni nella richiesta Initiate Multipart Upload (e in ogni richiesta successiva di carica parte) se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.

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

Intestazioni di richiesta non supportate

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

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

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Gli oggetti vengono creati (e, se applicabile, con la versione) quando viene eseguita l'operazione completa di caricamento

multiparte.

Informazioni correlate

"Gestire gli oggetti con ILM"

"Utilizzo della crittografia lato server"

"METTI oggetto"

Carica parte

L'operazione carica parte carica una parte in un caricamento multiparte per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Length`
- `Content-MD5`

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta di avvio caricamento multiparte, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta di caricamento parte:

- `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 di avvio caricamento multiparte.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta di avvio caricamento multiparte.

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

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Gli oggetti vengono creati (e, se applicabile, con la versione) quando viene eseguita l'operazione completa di caricamento multiparte.

Informazioni correlate

"Utilizzo della crittografia lato server"

Carica parte - Copia

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

L'operazione carica parte - Copia viene implementata con tutti i comportamenti REST API di Amazon S3.

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

Sono supportate le seguenti intestazioni di richiesta:

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

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta di avvio caricamento multiparte, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta di caricamento parte - Copia:

- `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 di avvio caricamento multiparte.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta di avvio caricamento multiparte.

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

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

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

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Gli oggetti vengono creati (e, se applicabile, con la versione) quando viene eseguita l'operazione completa di caricamento multiparte.

Caricamento multiparte completo

L'operazione completa di caricamento multiparte completa un caricamento multiparte di un oggetto assemblando le parti precedentemente caricate.

Risoluzione dei conflitti

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

Dimensione dell'oggetto

StorageGRID supporta oggetti di dimensioni fino a 5 TB.

Intestazioni delle richieste

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

Versione

Questa operazione completa un caricamento multiparte. Se la versione è abilitata per un bucket, la versione dell'oggetto viene creata al termine del caricamento multiparte.

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

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

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

Replica, notifica o notifica dei metadati non riuscite

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

In questo caso, viene generato un allarme in Grid Manager on Total Events (SMTT). Il messaggio Last Event (ultimo evento) visualizza "Failed to publish notifications for bucket-nameobject key" (Impossibile pubblicare le notifiche per la chiave bucket-nameobject) per l'ultimo oggetto la cui notifica non (Per visualizzare questo messaggio, selezionare **Nodes** > ***Storage Node*** > **Events**. Visualizza ultimo evento nella parte superiore della tabella.) I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

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

Informazioni correlate

"Gestire gli oggetti con ILM"

Risposte agli errori

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

Codici di errore S3 API supportati

Nome	Stato HTTP
Accesso negato	403 proibita
BadDigest	400 richiesta errata
BucketAlreadyExists	409 conflitto
BucketNotEmpty	409 conflitto
IncompleteBody	400 richiesta errata
InternalError	500 errore interno del server
InvalidAccessKeyId	403 proibita

Nome	Stato HTTP
Documento invalidato	400 richiesta errata
InvalidBucketName	400 richiesta errata
InvalidBucketState	409 conflitto
InvalidDigest	400 richiesta errata
InvalidEncryptionAlgorithmError	400 richiesta errata
InvalidPart	400 richiesta errata
InvalidPartOrder	400 richiesta errata
InvalidRange	416 intervallo richiesto non riscontrabile
InvalidRequest	400 richiesta errata
InvalidStorageClass	400 richiesta errata
InvalidTag	400 richiesta errata
InvalidURI	400 richiesta errata
KeyTooLong	400 richiesta errata
MalformedXML	400 richiesta errata
MetadataTooLarge	400 richiesta errata
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
MissingRequestBodyError	400 richiesta errata
MissingSecurityHeader	400 richiesta errata
NoSuchBucket	404 non trovato
NoSuchKey	404 non trovato
NoSuchUpload	404 non trovato

Nome	Stato HTTP
Non soddisfatto	501 non implementato
NoSuchBucketPolicy	404 non trovato
ObjectLockConfigurationNotFoundError	404 non trovato
PrecondizioneFailed	412 precondizione non riuscita
RequestTimeTooSkewed	403 proibita
ServiceUnavailable (Servizio non disponibile)	503 Servizio non disponibile
SignatureDoesNotMatch	403 proibita
TooManyBucket	400 richiesta errata
UserKeyMustBeSpecified	400 richiesta errata

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket compatibile legacy	400 richiesta errata
XBucketPolicyParseException	Impossibile analizzare JSON policy bucket ricevuta.	400 richiesta errata
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 proibita
XComplianceRiduciRedundancyProibita	La ridondanza ridotta non è consentita nel bucket compatibile legacy	400 richiesta errata
XMaxBucketPolicyLengthExceed	La policy supera la lunghezza massima consentita della policy bucket.	400 richiesta errata
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 richiesta errata
Conformità XNoSuchBucketCompliance	Nel bucket specificato non è attivata la compliance legacy.	404 non trovato

Nome	Descrizione	Stato HTTP
XNotAcceptable (XNotAccettabile)	La richiesta contiene una o più intestazioni di accettazione che non possono essere soddisfatte.	406 non accettabile
XNotImplemented	La richiesta fornita implica funzionalità non implementate.	501 non implementato

Informazioni sul copyright

Informazioni sul marchio commerciale