# Utilizzare l'API REST S3

StorageGRID software

NetApp
December 03, 2025

# Sommario

# Utilizzare l'API REST S3

## Versioni e aggiornamenti supportati dall'API REST S3

StorageGRID supporta l'API Simple Storage Service (S3), implementata come un set di servizi Web REST (Representational State Transfer).

Il supporto per l'API REST S3 consente di connettere le applicazioni orientate ai servizi sviluppate per i servizi Web S3 con l'archiviazione di oggetti on-premise che utilizza il sistema StorageGRID . Sono necessarie modifiche minime all'uso attuale delle chiamate API REST S3 da parte di un'applicazione client.

### Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di S3 e HTTP.

| Articolo | Versione |
| --- | --- |
| Specifiche API S3 | "Documentazione di Amazon Web Services (AWS): Riferimento API di Amazon Simple Storage Service" |
| HTTP | 1,1<br><br>Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35).<br><br>"IETF RFC 2616: Protocollo di trasferimento ipertestuale (HTTP/1.1)"<br><br>**Nota**: StorageGRID non supporta il pipelining HTTP/1.1. |

### Aggiornamenti al supporto dell'API REST S3

| Pubblicazione | Commenti |
| --- | --- |
| 11,9 | • Aggiunto supporto per valori di checksum SHA-256 precalcolati per le seguenti richieste e intestazioni supportate. Puoi utilizzare questa funzionalità per verificare l'integrità degli oggetti caricati:<br>◦ Caricamento multiparte completo: `x-amz-checksum-sha256`<br>◦ CreaCaricamentoMultiparte: `x-amz-checksum-algorithm`<br>◦ OttieniOggetto: `x-amz-checksum-mode`<br>◦ OggettoTesta: `x-amz-checksum-mode`<br>◦ ElencoParti<br>◦ MettiOggetto: `x-amz-checksum-sha256`<br>◦ CaricaParte: `x-amz-checksum-sha256`<br>• Aggiunta la possibilità per l'amministratore della griglia di controllare le impostazioni di conservazione e conformità a livello di tenant. Queste impostazioni influiscono sulle impostazioni di Blocco oggetti S3.<br>◦ Modalità di conservazione predefinita del bucket e modalità di conservazione degli oggetti: Governance o Conformità, se consentito dall'amministratore della griglia.<br>◦ Periodo di conservazione predefinito del bucket e data di conservazione dell'oggetto: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.<br>• Supporto migliorato per `aws-chunked` codifica e streaming dei contenuti `x-amz-content-sha256` valori. Limitazioni:<br>◦ Se presente, `chunk-signature` è facoltativo e non convalidato<br>◦ Se presente, `x-amz-trailer` il contenuto viene ignorato |
| 11,8 | Aggiornati i nomi delle operazioni S3 per abbinarli ai nomi utilizzati in "Documentazione di Amazon Web Services (AWS): Riferimento API di Amazon Simple Storage Service" . |
| 11,7 | • Aggiunto"Riferimento rapido: richieste API S3 supportate" .<br>• Aggiunto supporto per l'utilizzo della modalità GOVERNANCE con S3 Object Lock.<br>• Aggiunto supporto per StorageGRID specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta per le richieste GET Object e HEAD Object. Questa intestazione fornisce lo stato di replicazione di un oggetto per la replica tra griglie.<br>• Le richieste SelectObjectContent ora supportano gli oggetti Parquet. |

| Pubblicazione | Commenti |
| --- | --- |
| 11,6 | • Aggiunto supporto per l'utilizzo di `partNumber` parametro di richiesta nelle richieste GET Object e HEAD Object.<br>• Aggiunto il supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock.<br>• Aggiunto supporto per il `s3:object-lock-remaining-retention-days` chiave di condizione della policy per impostare l'intervallo di periodi di conservazione consentiti per i tuoi oggetti.<br>• Modificata la dimensione massima *consigliata* per una singola operazione PUT Object a 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa invece il caricamento multiparte. |
| 11,5 | • Aggiunto supporto per la gestione della crittografia dei bucket.<br>• Aggiunto supporto per S3 Object Lock e richieste di conformità legacy deprecate.<br>• Aggiunto supporto per l'utilizzo di DELETE Multiple Objects su bucket con versione.<br>• IL `Content-MD5` l'intestazione della richiesta è ora supportata correttamente. |
| 11,4 | • Aggiunto supporto per il tagging DELETE Bucket, GET Bucket e PUT Bucket. I tag di allocazione dei costi non sono supportati.<br>• Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le best practice in termini di prestazioni.<br>• Aggiunto supporto per le notifiche bucket su `s3:ObjectRestore:Post` tipo di evento.<br>• Sono ora applicati i limiti dimensionali AWS per le parti multiparte. Ogni parte di un caricamento multiparte deve avere una dimensione compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB.<br>• Aggiunto supporto per TLS 1.3 |
| 11,3 | • Aggiunto supporto per la crittografia lato server dei dati degli oggetti con chiavi fornite dal cliente (SSE-C).<br>• Aggiunto supporto per le operazioni del ciclo di vita del bucket DELETE, GET e PUT (solo azione di scadenza) e per `x-amz-expiration` intestazione di risposta.<br>• Aggiornati PUT Object, PUT Object - Copia e Caricamento multiparte per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione.<br>• I cifrari TLS 1.1 non sono più supportati. |
| 11,2 | Aggiunto supporto per il ripristino di oggetti POST per l'uso con Cloud Storage Pool. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione della policy e variabili della policy nelle policy di gruppo e bucket. Continueranno a essere supportati i criteri di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID .<br><br>**Nota:** gli utilizzi di ARN/URN in altre configurazioni JSON/XML, compresi quelli utilizzati nelle funzionalità StorageGRID personalizzate, non sono cambiati. |

| Pubblicazione | Commenti |
| --- | --- |
| 11,1 | Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per le connessioni client S3 ai nodi della griglia e impostazioni di conformità sui bucket. |
| 11,0 | Aggiunto supporto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. È stato inoltre aggiunto il supporto per i vincoli di posizione del tagging degli oggetti per i bucket e la coerenza disponibile. |
| 10,4 | Aggiunto supporto per le modifiche alla scansione ILM relative al controllo delle versioni, aggiornamenti della pagina Nomi di dominio endpoint, condizioni e variabili nelle policy, esempi di policy e autorizzazione PutOverwriteObject. |
| 10,3 | Aggiunto supporto per il controllo delle versioni. |
| 10,2 | Aggiunto supporto per criteri di accesso a gruppi e bucket e per la copia multiparte (Carica parte - Copia). |
| 10,1 | Aggiunto supporto per caricamento multiparte, richieste in stile virtual hosted e autenticazione v4. |
| 10,0 | Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID. La versione attualmente supportata del *Simple Storage Service API Reference* è 2006-03-01. |

# Riferimento rapido: richieste API S3 supportate

Questa pagina riassume il modo in cui StorageGRID supporta le API di Amazon Simple Storage Service (S3).

Questa pagina include solo le operazioni S3 supportate da StorageGRID.

> Per visualizzare la documentazione AWS per ciascuna operazione, selezionare il collegamento nell'intestazione.

## Parametri di query URI comuni e intestazioni di richiesta

Se non diversamente specificato, sono supportati i seguenti parametri di query URI comuni:

- `versionId`(come richiesto per le operazioni sugli oggetti)

Se non diversamente specificato, sono supportate le seguenti intestazioni di richiesta comuni:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`

- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

**Informazioni correlate**

- "Dettagli di implementazione dell'API REST S3"
- "Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni"

## "Annulla caricamento multiparte"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questo parametro di query URI aggiuntivo:

- `uploadId`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni per caricamenti multiparte"

## "Caricamento multiparte completo"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questo parametro di query URI aggiuntivo:

- `uploadId`
- `x-amz-checksum-sha256`

**Tag XML del corpo della richiesta**

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

**Documentazione StorageGRID**

"Caricamento multiparte completo"

## "CopiaOggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `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-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"CopiaOggetto"

## "CreaBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-bucket-object-lock-enabled`

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "CreaCaricamentoMultiparte"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"CreaCaricamentoMultiparte"

## "EliminaBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "DeleteBucketCors"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "DeleteBucketEncryption"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "DeleteBucketLifecycle"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

- "Operazioni sui bucket"
- "Crea la configurazione del ciclo di vita S3"

## "DeleteBucketPolicy"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "DeleteBucketReplication"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "DeleteBucketTagging"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "EliminaOggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questa intestazione di richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sugli oggetti"

## "EliminaOggetti"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questa intestazione di richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

"Operazioni sugli oggetti"

## "DeleteObjectTagging"

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sugli oggetti"

## "OttieniBucketAcl"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "GetBucketCors"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "Ottieni crittografia dei bucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "GetBucketLifecycleConfiguration"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

- "Operazioni sui bucket"
- "Crea la configurazione del ciclo di vita S3"

## "OttieniPosizioneBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "Configurazione di notifica di GetBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "OttieniPoliticaBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "OttieniReplicazioneBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "OttieniBucketTagging"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "GetBucketVersioning"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "OttieniOggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri di query URI aggiuntivi:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

E queste intestazioni di richiesta aggiuntive:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`

- `If-None-Match`
- `If-Unmodified-Since`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"OttieniOggetto"

## "OttieniOggettoAcl"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sugli oggetti"

## "OttieniOggettoLegaleHold"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

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

## "Ottieni configurazione blocco oggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

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

## "Ottieni conservazione oggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

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

## "OttieniTaggingOggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sugli oggetti"

## "HeadBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "HeadObject"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"HeadObject"

## "ListBuckets"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

**Operazioni sul servizio › ListBuckets**

## "Caricamenti multiparte di List"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

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

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Caricamenti multiparte di List"

## "ElencoOggetti"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "ListObjectsV2"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "ListObjectVersions"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "ElencoParti"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `max-parts`
- `part-number-marker`

- `uploadId`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"Caricamenti multiparte di List"

## "PutBucketCors"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "PutBucketEncryption"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Tag XML del corpo della richiesta**

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "Configurazione del ciclo di vita di PutBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Tag XML del corpo della richiesta**

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `And`
- `Days`
- `Expiration`

- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

**Documentazione StorageGRID**

- "Operazioni sui bucket"
- "Crea la configurazione del ciclo di vita S3"

## "Configurazione della notifica PutBucket"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Tag XML del corpo della richiesta**

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "PutBucketPolicy"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Per i dettagli sui campi del corpo JSON supportati, vedere"Utilizzare criteri di accesso a bucket e gruppi" .

## "PutBucketReplication"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Tag XML del corpo della richiesta**

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "PutBucketTagging"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "PutBucketVersioning"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Parametri del corpo della richiesta**

StorageGRID supporta i seguenti parametri del corpo della richiesta:

- `VersioningConfiguration`
- `Status`

**Documentazione StorageGRID**

"Operazioni sui bucket"

## "MettiOggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

**Corpo della richiesta**

- Dati binari dell'oggetto

**Documentazione StorageGRID**

"MettiOggetto"

## "PutObjectLegalHold"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al

momento dell'implementazione.

**Documentazione StorageGRID**

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

## "PutObjectLockConfiguration"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

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

## "PutObjectRetention"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questa intestazione aggiuntiva:

- `x-amz-bypass-governance-retention`

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

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

## "PutObjectTagging"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

**Documentazione StorageGRID**

"Operazioni sugli oggetti"

## "Ripristina oggetto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Per i dettagli sui campi del corpo supportati, vedere"Ripristina oggetto" .

## "SelezionaOggettoContenuto"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

**Corpo della richiesta**

Per maggiori dettagli sui campi del corpo supportati, vedere quanto segue:

- "Utilizzare S3 Select"
- "SelezionaOggettoContenuto"

## "CaricaParte"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

**Corpo della richiesta**

- Dati binari della parte

**Documentazione StorageGRID**

"CaricaParte"

## "CaricaParteCopia"

**Parametri di query URI e intestazioni di richiesta**

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`

- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `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`

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

"CaricaParteCopia"

# Testare la configurazione dell'API REST S3

È possibile utilizzare l'interfaccia a riga di comando di Amazon Web Services (AWS CLI) per testare la connessione al sistema e verificare di poter leggere e scrivere oggetti.

**Prima di iniziare**

- Hai scaricato e installato AWS CLI da "aws.amazon.com/cli" .
- Facoltativamente, hai"creato un endpoint del bilanciatore del carico" . In caso contrario, è necessario conoscere l'indirizzo IP del nodo di archiviazione a cui si desidera connettersi e il numero di porta da utilizzare. Vedere "Indirizzi IP e porte per le connessioni client" .
- Hai"creato un account tenant S3" .
- Hai effettuato l'accesso al tenant e"ha creato una chiave di accesso" .

Per i dettagli su questi passaggi, vedere"Configurare le connessioni client" .

**Passi**

1. Configura le impostazioni AWS CLI per utilizzare l'account creato nel sistema StorageGRID :
   a. Entra nella modalità di configurazione: `aws configure`
   b. Inserisci l'ID della chiave di accesso per l'account che hai creato.
   c. Inserisci la chiave di accesso segreta per l'account che hai creato.
   d. Inserisci la regione predefinita da utilizzare. Ad esempio, `us-east-1` .
   e. Immettere il formato di output predefinito da utilizzare oppure premere **Invio** per selezionare JSON.
2. Crea un bucket.

   In questo esempio si presuppone che sia stato configurato un endpoint del bilanciatore del carico per utilizzare l'indirizzo IP 10.96.101.17 e la porta 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Se il bucket viene creato correttamente, viene restituita la posizione del bucket, come mostrato nell'esempio seguente:

```
"Location": "/testbucket"
```

3. Carica un oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Se l'oggetto viene caricato correttamente, viene restituito un Etag, ovvero un hash dei dati dell'oggetto.

4. Elenca il contenuto del bucket per verificare che l'oggetto sia stato caricato.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Elimina l'oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Elimina il bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

# Come StorageGRID implementa l'API REST S3

## Richieste dei clienti in conflitto

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins".

La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

## Valori di coerenza

La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti tra diversi nodi di archiviazione e siti. È possibile modificare la coerenza in base alle esigenze dell'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET successivo a un PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture di oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni alla fine risultano coerenti. In genere, la propagazione delle sovrascritture richiede secondi o minuti, ma può richiedere fino a 15 giorni.

Se si desidera eseguire operazioni sugli oggetti con una consistenza diversa, è possibile:

- Specificare una coerenza perogni secchio .
- Specificare una coerenza perogni operazione API .
- Modificare la coerenza predefinita dell'intera griglia eseguendo una delle seguenti attività:
  - In Grid Manager, vai su **CONFIGURAZIONE** > **Sistema** > **Impostazioni di archiviazione** > **Coerenza predefinita**.
  - .

> Una modifica alla coerenza a livello di griglia si applica solo ai bucket creati dopo la modifica dell'impostazione. Per determinare i dettagli di una modifica, consultare il registro di controllo situato in `/var/local/log` (cerca **consistencyLevel**).

### Valori di coerenza

La coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tracciare gli oggetti vengono distribuiti tra i nodi e, di conseguenza, sulla disponibilità degli oggetti per le richieste dei client.

È possibile impostare la coerenza per un bucket o un'operazione API su uno dei seguenti valori:

- **Tutti**: tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
- **Strong-global**: garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti.
- **Strong-site**: garantisce la coerenza di lettura e scrittura per tutte le richieste client all'interno di un sito.
- **Lettura dopo nuova scrittura**: (predefinito) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile**: fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

### Utilizzare la coerenza "Lettura dopo nuova scrittura" e "Disponibile"

Quando un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write", StorageGRID esegue la ricerca in più passaggi, come segue:

- Per prima cosa cerca l'oggetto utilizzando una bassa coerenza.

- Se la ricerca fallisce, la ripete al valore di coerenza successivo finché non raggiunge una coerenza equivalente al comportamento di strong-global.

Se un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write" ma l'oggetto non esiste, la ricerca dell'oggetto raggiungerà sempre una coerenza equivalente al comportamento per strong-global. Poiché questa coerenza richiede che siano disponibili più copie dei metadati dell'oggetto in ogni sito, è possibile ricevere un numero elevato di errori 500 Internal Server se due o più nodi di archiviazione nello stesso sito non sono disponibili.

A meno che non siano necessarie garanzie di coerenza simili ad Amazon S3, è possibile prevenire questi errori per le operazioni HEAD e GET impostando la coerenza su "Disponibile". Quando un'operazione HEAD o GET utilizza la coerenza "Disponibile", StorageGRID fornisce solo la coerenza finale. Non riprova un'operazione non riuscita aumentando la coerenza, quindi non richiede che siano disponibili più copie dei metadati dell'oggetto.

#### Specifica la coerenza per l'operazione API

Per impostare la coerenza per una singola operazione API, i valori di coerenza devono essere supportati per l'operazione ed è necessario specificare la coerenza nell'intestazione della richiesta. In questo esempio la coerenza viene impostata su "Strong-site" per un'operazione GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

È necessario utilizzare la stessa coerenza per entrambe le operazioni PutObject e GetObject.

#### Specifica la coerenza per il bucket

Per impostare la coerenza per il bucket, puoi utilizzare StorageGRID"PUT Consistenza del secchio" richiesta. Oppure puoi"modificare la consistenza di un bucket" dal gestore dell'affitto.

Quando si imposta la consistenza di un bucket, tenere presente quanto segue:

- L'impostazione della coerenza per un bucket determina quale coerenza viene utilizzata per le operazioni S3 eseguite sugli oggetti nel bucket o sulla configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- La coerenza di una singola operazione API prevale sulla coerenza del bucket.
- In generale, i bucket dovrebbero utilizzare la coerenza predefinita, "Lettura dopo nuova scrittura". Se le richieste non funzionano correttamente, modificare, se possibile, il comportamento del client dell'applicazione. Oppure, configura il client in modo che specifichi la coerenza per ogni richiesta API. Impostare la coerenza a livello di bucket solo come ultima risorsa.

#### Come interagiscono la coerenza e le regole ILM per influenzare la protezione dei dati

Sia la scelta della coerenza sia la regola ILM influiscono sul modo in cui gli oggetti vengono protetti. Queste impostazioni possono interagire.

Ad esempio, la coerenza utilizzata quando un oggetto viene archiviato influisce sul posizionamento iniziale dei

metadati dell'oggetto, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie dell'oggetto. Poiché StorageGRID richiede l'accesso sia ai metadati di un oggetto sia ai suoi dati per soddisfare le richieste dei client, la selezione di livelli di protezione corrispondenti per la coerenza e il comportamento di acquisizione può garantire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Il seguente"opzioni di ingestione" sono disponibili per le regole ILM:

**Doppio impegno**

StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce l'esito positivo al client. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

**Rigoroso**

Tutte le copie specificate nella regola ILM devono essere effettuate prima che il successo venga restituito al cliente.

**Equilibrato**

StorageGRID tenta di effettuare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono effettuate copie provvisorie e il client riceve un messaggio di conferma dell'operazione riuscita. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

#### Esempio di come la coerenza e la regola ILM possono interagire

Supponiamo di avere una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM**: creare due copie dell'oggetto, una nel sito locale e una in un sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **coerenza**: Strong-global (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie dell'oggetto e distribuisce i metadati a entrambi i siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati sul sito remoto, ma prima che i metadati dell'oggetto vengano distribuiti lì. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Se hai bisogno di assistenza, contatta NetApp .

## Versionamento degli oggetti

È possibile impostare lo stato di controllo delle versioni di un bucket se si desidera conservare più versioni di ciascun oggetto. Abilitare il controllo delle versioni per un bucket può contribuire a proteggere gli oggetti dall'eliminazione accidentale e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con supporto per la maggior parte delle

funzionalità e con alcune limitazioni. StorageGRID supporta fino a 10.000 versioni di ciascun oggetto.

Il controllo delle versioni degli oggetti può essere combinato con la gestione del ciclo di vita delle informazioni (ILM) StorageGRID o con la configurazione del ciclo di vita del bucket S3. È necessario abilitare esplicitamente il controllo delle versioni per ogni bucket. Quando il controllo delle versioni è abilitato per un bucket, a ogni oggetto aggiunto al bucket viene assegnato un ID versione, generato dal sistema StorageGRID .

L'eliminazione tramite MFA (autenticazione a più fattori) non è supportata.

> Il controllo delle versioni può essere abilitato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

#### ILM e controllo delle versioni

Le policy ILM vengono applicate a ciascuna versione di un oggetto. Un processo di scansione ILM analizza continuamente tutti gli oggetti e li rivaluta in base alla politica ILM corrente. Tutte le modifiche apportate ai criteri ILM vengono applicate a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente acquisite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti precedentemente acquisiti.

Per gli oggetti S3 nei bucket abilitati per il controllo delle versioni, il supporto del controllo delle versioni consente di creare regole ILM che utilizzano "Ora non corrente" come ora di riferimento (selezionare **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti?" in"Passaggio 1 della procedura guidata Crea una regola ILM" ). Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. Utilizzando un filtro "Tempo non corrente" è possibile creare criteri che riducono l'impatto sull'archiviazione delle versioni precedenti degli oggetti.

> Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, il tempo non corrente per la versione originale dell'oggetto riflette il momento in cui è stato creato il caricamento multiparte per la nuova versione, non il momento in cui è stato completato il caricamento multiparte. In casi limitati, l'orario non aggiornato della versione originale potrebbe essere precedente di ore o giorni rispetto all'orario della versione corrente.

#### Informazioni correlate

- "Come vengono eliminati gli oggetti con versione S3"
- "Regole e policy ILM per oggetti con versione S3 (esempio 4)" .

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

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile creare bucket con S3 Object Lock abilitato. È possibile specificare la conservazione predefinita per ogni bucket o le impostazioni di conservazione per ogni versione dell'oggetto.

#### Come abilitare S3 Object Lock per un bucket

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile abilitare facoltativamente S3 Object Lock quando si crea ogni bucket.

S3 Object Lock è un'impostazione permanente che può essere abilitata solo quando si crea un bucket. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket.

Per abilitare S3 Object Lock per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando Tenant Manager. Vedere "Crea bucket S3" .
- Crea il bucket utilizzando una richiesta CreateBucket con `x-amz-bucket-object-lock-enabled` intestazione della richiesta. Vedere "Operazioni sui bucket" .

S3 Object Lock richiede il controllo delle versioni dei bucket, che viene abilitato automaticamente al momento della creazione del bucket. Non è possibile sospendere il controllo delle versioni per il bucket. Vedere "Versionamento degli oggetti" .

### Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è abilitato per un bucket, è possibile abilitare facoltativamente la conservazione predefinita per il bucket e specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito.

#### Modalità di conservazione predefinita

- In modalità CONFORMITÀ:
  - L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
  - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità GOVERNANCE:
  - Utenti con il `s3:BypassGovernanceRetention` il permesso può utilizzare il `x-amz-bypass-governance-retention: true` intestazione della richiesta per ignorare le impostazioni di conservazione.
  - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

#### Periodo di conservazione predefinito

Ogni bucket può avere un periodo di conservazione predefinito specificato in anni o giorni.

### Come impostare la conservazione predefinita per un bucket

Per impostare la conservazione predefinita per un bucket, utilizzare uno dei seguenti metodi:

- Gestisci le impostazioni del bucket da Tenant Manager. Vedere"Crea un bucket S3" E"Aggiorna la conservazione predefinita del blocco degli oggetti S3" .
- Inviare una richiesta PutObjectLockConfiguration al bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

#### PutObjectLockConfiguration

La richiesta PutObjectLockConfiguration consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket in cui è abilitato S3 Object Lock. È anche possibile rimuovere le impostazioni di conservazione predefinite configurate in precedenza.

Quando nuove versioni di oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` E `x-amz-object-lock-retain-until-date` non sono

specificati. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione fino a se `x-amz-object-lock-retain-until-date` non è specificato.

Se il periodo di conservazione predefinito viene modificato dopo l'acquisizione di una versione dell'oggetto, la data di conservazione fino alla versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

Devi avere il `s3:PutBucketObjectLockConfiguration` autorizzazione, oppure essere l'account root, per completare questa operazione.

IL `Content-MD5` l'intestazione della richiesta deve essere specificata nella richiesta PUT.

#### Richiedi esempio

Questo esempio abilita S3 Object Lock per un bucket e imposta la modalità di conservazione predefinita su CONFORMITÀ e il periodo di conservazione predefinito su 6 anni.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

### Come determinare la conservazione predefinita per un bucket

Per determinare se S3 Object Lock è abilitato per un bucket e per visualizzare la modalità di conservazione predefinita e il periodo di conservazione, utilizzare uno di questi metodi:

- Visualizza il bucket in Tenant Manager. Vedere "Visualizza i bucket S3" .
- Inviare una richiesta GetObjectLockConfiguration.

#### Ottieni configurazione blocco oggetto

La richiesta GetObjectLockConfiguration consente di determinare se S3 Object Lock è abilitato per un bucket e, in tal caso, di verificare se sono configurati una modalità di conservazione predefinita e un periodo di

conservazione per il bucket.

Quando nuove versioni di oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` non è specificato. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione fino a se `x-amz-object-lock-retain-until-date` non è specificato.

Devi avere il `s3:GetBucketObjectLockConfiguration` autorizzazione, oppure essere l'account root, per completare questa operazione.

**Richiedi esempio**

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

**Esempio di risposta**

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

**Come specificare le impostazioni di conservazione per un oggetto**

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza impostazioni

di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate tramite l'API REST S3. Le impostazioni di conservazione per un oggetto sostituiscono tutte le impostazioni di conservazione predefinite per il bucket.

Per ogni oggetto è possibile specificare le seguenti impostazioni:

- **Modalità di conservazione**: CONFORMITÀ o GOVERNANCE.
- **Retain-until-date**: data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da StorageGRID.
  - In modalità CONFORMITÀ, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o eliminato. La data di conservazione può essere aumentata, ma questa data non può essere diminuita o rimossa.
  - In modalità GOVERNANCE, gli utenti con autorizzazione speciale possono ignorare l'impostazione di conservazione fino alla data indicata. Possono eliminare una versione di un oggetto prima che scada il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere la data di conservazione.
- **Sospensione legale**: l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente.

  L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla data di conservazione fino alla data di scadenza. Se una versione di un oggetto è sottoposta a blocco legale, nessuno può eliminarla.

Per specificare le impostazioni di blocco degli oggetti S3 quando si aggiunge una versione dell'oggetto a un bucket, emettere un"MettiOggetto" ,"CopiaOggetto" , O"CreaCaricamentoMultiparte" richiesta.

Puoi usare quanto segue:

- `x-amz-object-lock-mode`, che può essere COMPLIANCE o GOVERNANCE (con distinzione tra maiuscole e minuscole).

  > Se specifichi `x-amz-object-lock-mode` , devi anche specificare `x-amz-object-lock-retain-until-date` .

- `x-amz-object-lock-retain-until-date`
  - Il valore retain-til-date deve essere nel formato `2020-08-10T21:46:00Z` . Sono consentite frazioni di secondo, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Altri formati ISO 8601 non sono consentiti.
  - La data di conservazione deve essere futura.
- `x-amz-object-lock-legal-hold`

  Se la conservazione legale è ATTIVA (sensibile alle maiuscole e alle minuscole), l'oggetto viene sottoposto a conservazione legale. Se la conservazione legale è disattivata, non verrà applicata alcuna conservazione legale. 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 PutObject. `Content-MD5` non è richiesto per CopyObject o CreateMultipartUpload.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` Se è presente l'intestazione della richiesta, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta PutObject supporta l'uso di `x-amz-storage-class: REDUCED_REDUNDANCY` per adattarsi al comportamento di AWS. Tuttavia, quando un oggetto viene inserito in un bucket con S3 Object Lock abilitato, StorageGRID eseguirà sempre un inserimento a doppio commit.
- Una successiva risposta alla versione GET o HeadObject 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.

Puoi usare il `s3:object-lock-remaining-retention-days` chiave di condizione della policy per limitare i periodi di conservazione minimi e massimi consentiti per i tuoi oggetti.

**Come aggiornare le impostazioni di conservazione per un oggetto**

Se è necessario aggiornare le impostazioni di conservazione o di blocco legale per una versione esistente di un oggetto, è possibile eseguire le seguenti operazioni sulle sottorisorse dell'oggetto:

- `PutObjectLegalHold`

  Se il nuovo valore di conservazione legale è impostato su ON, l'oggetto viene sottoposto a conservazione legale. Se il valore di sospensione legale è OFF, la sospensione legale viene revocata.

- `PutObjectRetention`
  - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (con distinzione tra maiuscole e minuscole).
  - Il valore retain-til-date deve essere nel formato `2020-08-10T21:46:00Z` . Sono consentite frazioni di secondo, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Altri formati ISO 8601 non sono consentiti.
  - Se una versione di un oggetto ha una data di conservazione (retain-til-date) esistente, è possibile solo aumentarla. Il nuovo valore deve essere nel futuro.

**Come utilizzare la modalità GOVERNANCE**

Gli utenti che hanno il `s3:BypassGovernanceRetention` l'autorizzazione può ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità GOVERNANCE. Tutte le operazioni DELETE o PutObjectRetention devono includere `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire le seguenti operazioni aggiuntive:

- Eseguire le operazioni DeleteObject o DeleteObjects per eliminare una versione dell'oggetto prima che scada il periodo di conservazione.

  Gli oggetti sottoposti a conservazione legale non possono essere eliminati. La conservazione legale deve essere DISATTIVATA.

- Eseguire operazioni PutObjectRetention che modificano la modalità di una versione dell'oggetto da GOVERNANCE a COMPLIANCE prima che sia trascorso il periodo di conservazione dell'oggetto.

  Non è mai consentito cambiare la modalità da COMPLIANCE a GOVERNANCE.

- Eseguire operazioni PutObjectRetention per aumentare, diminuire o rimuovere il periodo di conservazione di una versione dell'oggetto.

**Informazioni correlate**

- "Gestisci gli oggetti con S3 Object Lock"
- "Utilizzare S3 Object Lock per conservare gli oggetti"
- "Guida per l'utente di Amazon Simple Storage Service: blocco degli oggetti"

## Crea la configurazione del ciclo di vita S3

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

Il semplice esempio in questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando determinati oggetti vengono eliminati (scadono) da specifici bucket S3. L'esempio in questa sezione è solo a scopo illustrativo. Per i dettagli completi sulla creazione di configurazioni del ciclo di vita S3, vedere "Guida per l'utente di Amazon Simple Storage Service: gestione del ciclo di vita degli oggetti" . Si noti che StorageGRID supporta solo azioni di scadenza; non supporta azioni di transizione.

### Qual è la configurazione del ciclo di vita?

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in bucket S3 specifici. Ogni regola specifica quali oggetti sono interessati e quando tali oggetti 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: elimina un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dal momento in cui l'oggetto è stato acquisito.
- NoncurrentVersionExpiration: elimina un oggetto quando viene raggiunto un numero di giorni specificato, a partire dal momento in cui l'oggetto è diventato non corrente.
- Filtro (Prefisso, Tag)
- Stato
- ID

Ogni oggetto segue le impostazioni di conservazione del ciclo di vita di un bucket S3 o di una policy ILM. Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita del bucket. Gli oggetti che non corrispondono al filtro del ciclo di vita del bucket utilizzano le impostazioni di conservazione del criterio ILM. Se un oggetto corrisponde a un filtro del ciclo di vita del bucket e non vengono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione del criterio ILM non vengono utilizzate e si implica che le versioni dell'oggetto vengano conservate per sempre. Vedere "Esempio di priorità per il ciclo di vita del bucket S3 e la policy ILM" .

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora valide per l'oggetto. Oppure, un oggetto potrebbe essere mantenuto sulla griglia anche dopo che tutte le istruzioni di posizionamento ILM per l'oggetto sono scadute. Per maggiori dettagli, vedere "Come funziona l'ILM durante la vita di un oggetto" .

La configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

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

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- Configurazione del ciclo di vita di PutBucket

**Crea la configurazione del ciclo di vita**

Come primo passaggio nella creazione di una configurazione del ciclo di vita, si crea un file JSON che include 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 che corrispondono al filtro scadranno a mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2` /. IL `Expiration` Il parametro specifica che gli oggetti che corrispondono al filtro scadranno 100 giorni dopo essere stati acquisiti.

   Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato ingerito. 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` Il parametro specifica che tutte le versioni non correnti degli oggetti corrispondenti scadranno 50 giorni dopo essere diventate non correnti.

```
{
    "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"
        }
    ]
}
```

### Applica la configurazione del ciclo di vita al bucket

Dopo aver creato il file di configurazione del ciclo di vita, puoi applicarlo a un bucket inviando una richiesta PutBucketLifecycleConfiguration.

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

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

Per convalidare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, inviare una richiesta GetBucketLifecycleConfiguration. Per esempio:

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

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

### Convalida che la scadenza del ciclo di vita del bucket si applichi all'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 PutObject, HeadObject o GetObject. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando scade l'oggetto e quale regola di scadenza è stata rispettata.

> Poiché il ciclo di vita del bucket sostituisce ILM, `expiry-date` viene mostrata la data effettiva in cui l'oggetto verrà eliminato. Per maggiori dettagli, vedere "Come viene determinata la ritenzione dell'oggetto" .

Ad esempio, questa richiesta PutObject è stata emessa il 22 giugno 2020 e inserisce un oggetto nel `testbucket` secchio.

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

La risposta di successo 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 HeadObject 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 soddisfa la 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": {}
}
```

Per i bucket abilitati al controllo delle versioni, `x-amz-expiration` l'intestazione di risposta si applica solo alle versioni correnti degli oggetti.

## Raccomandazioni per l'implementazione dell'API REST S3

Quando si implementa l'API REST S3 per l'uso con StorageGRID, è necessario seguire queste raccomandazioni.

### Raccomandazioni per HEAD su oggetti inesistenti

Se la tua applicazione controlla regolarmente se un oggetto esiste in un percorso in cui non ti aspetti che l'oggetto esista effettivamente, dovresti usare "Disponibile""coerenza" . Ad esempio, dovresti usare la coerenza "Disponibile" se la tua applicazione esegue l'HEAD di una posizione prima di eseguirvi un PUT.

In caso contrario, se l'operazione HEAD non trova l'oggetto, è possibile che venga visualizzato un numero elevato di errori 500 Internal Server se due o più nodi di archiviazione nello stesso sito non sono disponibili o un sito remoto non è raggiungibile.

È possibile impostare la coerenza "Disponibile" per ogni bucket utilizzando"PUT Consistenza del secchio"

richiesta oppure è possibile specificare la coerenza nell'intestazione della richiesta per una singola operazione API.

### Raccomandazioni per le chiavi degli oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base al momento in cui il bucket è stato creato per la prima volta.

#### Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi degli oggetti. Ciò è in contrasto con la precedente raccomandazione di AWS per i prefissi delle chiavi. Utilizzare invece prefissi non casuali e non univoci, come ad esempio `image` .
- Se si segue la precedente raccomandazione di AWS di utilizzare caratteri casuali e univoci nei prefissi delle chiavi, aggiungere un nome di directory come prefisso alle chiavi degli oggetti. Cioè, usa questo formato:

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  Invece di questo formato:

  ```
  mybucket/f8e3-image3132.jpg
  ```

#### Bucket creati in StorageGRID 11.4 o versioni successive

Non è necessario limitare i nomi delle chiavi degli oggetti per soddisfare le migliori pratiche in termini di prestazioni. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.

> Un'eccezione è il carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto sulle prestazioni in questo caso d'uso, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa come la data. Ad esempio, supponiamo che un client S3 scriva in genere 2.000 oggetti al secondo e che la policy ILM o del ciclo di vita del bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto sulle prestazioni, potresti denominare le chiavi utilizzando uno schema come questo: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

### Consigli per le "letture di intervallo"

Se il"opzione globale per comprimere gli oggetti memorizzati" è abilitato, le applicazioni client S3 dovrebbero evitare di eseguire operazioni GetObject che specificano un intervallo di byte da restituire. Queste operazioni di "lettura di intervallo" sono inefficienti perché StorageGRID deve effettivamente decomprimere gli oggetti per accedere ai byte richiesti. Le operazioni GetObject che richiedono un intervallo ridotto di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, non è efficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client potrebbero scadere.

> Se è necessario comprimere oggetti e l'applicazione client deve utilizzare letture di intervallo, aumentare il timeout di lettura per l'applicazione.

# Supporto per l'API REST di Amazon S3

## Dettagli di implementazione dell'API REST S3

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

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

### Gestione delle date

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

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

### Intestazioni di richiesta comuni

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

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

### Intestazioni di risposta comuni

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

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

## Autenticare le richieste

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

L'API S3 supporta la versione 2 e la versione 4 della firma per l'autenticazione delle richieste API S3.

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

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

### Utilizzare l'intestazione di autorizzazione HTTP

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

### Utilizzare i parametri di query

È possibile utilizzare i parametri di query per aggiungere informazioni di autenticazione a un URL. Questa operazione è nota come prefirma dell'URL e può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL prefirmato non hanno bisogno di conoscere la chiave di accesso segreta per accedere alla risorsa, il che consente di fornire a terze parti un accesso limitato a una risorsa.

## Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

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

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

## Operazioni sui bucket

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

Ogni griglia può avere un massimo di 100.000 bucket.

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

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

Per maggiori informazioni vedere quanto segue:

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

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

È possibile verificare se gli aggiornamenti all'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket. Vedere "GET Ora dell'ultimo accesso al bucket" .

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

| Operazione | Implementazione |
| --- | --- |
| CreaBucket | Crea un nuovo bucket. Creando il bucket, ne diventi il proprietario.<br><br>• I nomi dei bucket devono rispettare le seguenti regole:<br>◦ Deve essere univoco in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).<br>◦ Deve essere conforme al DNS.<br>◦ Deve contenere almeno 3 e non più di 63 caratteri.<br>◦ Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può contenere solo lettere minuscole, numeri e trattini.<br>◦ Non deve avere l'aspetto di un indirizzo IP formattato come testo.<br>◦ Non utilizzare punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server.<br>• Per impostazione predefinita, i bucket vengono creati in `us-east-1` regione; tuttavia, è possibile utilizzare il `LocationConstraint` elemento di richiesta nel corpo della richiesta per specificare una regione diversa. Quando si utilizza il `LocationConstraint` elemento, è necessario specificare il nome esatto di una regione definita tramite Grid Manager o Grid Management API. Se non conosci il nome della regione da utilizzare, contatta l'amministratore di sistema.<br><br>**Nota**: si verificherà un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID.<br><br>• Puoi includere il `x-amz-bucket-object-lock-enabled` intestazione della richiesta per creare un bucket con S3 Object Lock abilitato. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .<br><br>Quando si crea il bucket, è necessario abilitare S3 Object Lock. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket. S3 Object Lock richiede il controllo delle versioni dei bucket, che viene abilitato automaticamente quando si crea il bucket. |
| EliminaBucket | Elimina il bucket. |
| DeleteBucketCors | Elimina la configurazione CORS per il bucket. |
| DeleteBucketEncryption | Elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma tutti i nuovi oggetti aggiunti al bucket non vengono crittografati. |
| DeleteBucketLifecycle | Elimina la configurazione del ciclo di vita dal bucket. Vedere "Crea la configurazione del ciclo di vita S3" . |
| DeleteBucketPolicy | Elimina la policy associata al bucket. |

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

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

| Operazione | Implementazione |
| --- | --- |
| PutBucketCors | Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire richieste multiorigine. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponiamo di utilizzare un bucket S3 denominato `images` per memorizzare la grafica. Impostando la configurazione CORS per `images` bucket, puoi consentire che le immagini in quel bucket vengano visualizzate sul sito web `http://www.example.com` . |
| PutBucketEncryption | Imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è abilitata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con chiavi gestite StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare `SSEAlgorithm` parametro a `AES256` e non usare il `KMSMasterKeyID` parametro.<br><br>La configurazione di crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include `x-amz-server-side-encryption-*` intestazione della richiesta). |
| Configurazione del ciclo di vita di PutBucket<br><br>(in precedenza denominato ciclo di vita del bucket PUT) | Crea una nuova configurazione del ciclo di vita per il bucket o sostituisce una configurazione del ciclo di vita esistente. StorageGRID supporta fino a 1.000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:<br><br>• Scadenza (Giorni, Data, ExpiredObjectDeleteMarker)<br>• NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays)<br>• Filtro (Prefisso, Tag)<br>• Stato<br>• ID<br><br>StorageGRID non supporta queste azioni:<br><br>• AnnullaIncompletoCaricamento multiparte<br>• Transizione<br><br>Vedere "Crea la configurazione del ciclo di vita S3" . Per comprendere come l'azione di scadenza nel ciclo di vita di un bucket interagisce con le istruzioni di posizionamento ILM, vedere"Come funziona l'ILM durante la vita di un oggetto" .<br><br>**Nota**: la configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy. |

| Operazione | Implementazione |
| --- | --- |
| Configurazione della notifica PutBucket<br><br>(in precedenza denominata notifica PUT Bucket) | Configura le notifiche per il bucket utilizzando l'XML di configurazione delle notifiche incluso nel corpo della richiesta. È necessario conoscere i seguenti dettagli di implementazione:<br><br>• StorageGRID supporta come destinazioni gli argomenti Amazon Simple Notification Service (Amazon SNS) o Kafka. Gli endpoint Simple Queue Service (SQS) o Amazon Lambda non sono supportati.<br>• La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID . Gli endpoint possono essere creati utilizzando Tenant Manager o Tenant Management API.<br><br>Affinché la configurazione della notifica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, un `400 Bad Request` l'errore viene restituito con il codice `InvalidArgument` .<br><br>• Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di eventi **non** sono supportati.<br>◦ `s3:ReducedRedundancyLostObject`<br>◦ `s3:ObjectRestore:Completed`<br>• Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, con la differenza che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente:<br>◦ **fonteevento**<br><br>`sgws:s3`<br><br>◦ **awsRegion**<br><br>non incluso<br><br>◦ **x-amz-id-2**<br><br>non incluso<br><br>◦ **arn**<br><br>`urn:sgws:s3:::bucket_name` |
| PutBucketPolicy | Imposta la policy associata al bucket. Vedere "Utilizzare criteri di accesso a bucket e gruppi" . |

| Operazione | Implementazione |
| --- | --- |
| PutBucketReplication | Configura"Replica StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica CloudMirror, è necessario conoscere i seguenti dettagli di implementazione:<br><br>• StorageGRID supporta solo la versione 1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'uso di `Filter` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per i dettagli, vedere "Guida per l'utente di Amazon Simple Storage Service: configurazione della replica" .<br>• La replica dei bucket può essere configurata su bucket con o senza versione.<br>• È possibile specificare un bucket di destinazione diverso in ogni regola del file XML di configurazione della replica. Un bucket di origine può replicarsi su più di un bucket di destinazione.<br>• I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID come specificato in Tenant Manager o nell'API Tenant Management. Vedere "Configurare la replica di CloudMirror" .<br><br>Affinché la configurazione della replica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, la richiesta fallisce come `400 Bad Request` Il messaggio di errore afferma: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`.<br><br>• Non è necessario specificare un `Role` nell'XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato.<br>• Se si omette la classe di archiviazione dall'XML di configurazione, StorageGRID utilizza `STANDARD` classe di archiviazione predefinita.<br>• Se si elimina un oggetto dal bucket di origine o si elimina il bucket di origine stesso, il comportamento della replica tra regioni è il seguente:<br>◦ Se elimini l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non verrà replicato e non riceverai alcuna notifica.<br>◦ Se si elimina l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento di eliminazione standard di Amazon S3 per la V1 della replica tra regioni. |

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

## Operazioni sugli oggetti

### Operazioni sugli oggetti

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

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

- StorageGRID"valori di coerenza" sono supportati da tutte le operazioni sugli oggetti, ad eccezione delle

seguenti:

  - OttieniOggettoAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelezionaOggettoContenuto

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

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

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

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

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

#### Utilizzare S3 Select

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

Tutti gli elementi non elencati non sono supportati.

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

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

#### Clausole

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

#### Tipi di dati

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

#### Operatori

### Operatori logici

- E
- NON
- O

### Operatori di confronto

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

#### Operatori di corrispondenza di pattern

- COME
- _
- %

#### Operatori unitari

- È NULLO
- NON È NULLO

#### Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

##### Funzioni aggregate

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

##### Funzioni condizionali

- CASO
- COALESCERE
- NULLIF

##### Funzioni di conversione

- CAST (per i tipi di dati supportati)

##### Funzioni di data

- DATA_AGGIUNGI
- DATE_DIFF
- ESTRARRE
- A_STRINGA
- TO_TIMESTAMP

- UTCNOW

#### Funzioni stringa

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

### Utilizzare la crittografia lato server

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

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

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

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

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

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

#### Utilizzare SSE

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

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

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

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

#### Utilizzare SSE-C

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

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

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

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

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

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

- Devi usare https.

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

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

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

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

**Informazioni correlate**

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

### CopiaOggetto

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

#### Risolvere i conflitti

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

#### Dimensione dell'oggetto

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

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

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

#### Caratteri UTF-8 nei metadati utente

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

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

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

#### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

    VedereIntestazioni di richiesta per la crittografia lato server

#### Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

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

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

#### Opzioni di classe di archiviazione

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

#### Utilizzo di x-amz-copy-source in CopyObject

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

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

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

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

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

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

#### Intestazioni di richiesta per la crittografia lato server

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

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

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

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

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

#### Controllo delle versioni

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

### OttieniOggetto

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

#### GetObject e oggetti multipart

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

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

#### Caratteri UTF-8 nei metadati utente

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

#### Intestazione della richiesta supportata

È supportata la seguente intestazione di richiesta:

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

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

#### Intestazione della richiesta non supportata

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

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

#### Controllo delle versioni

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

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

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

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

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

#### Comportamento di GetObject per gli oggetti Cloud Storage Pool

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

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

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

### Oggetti multiparte o segmentati in un pool di archiviazione cloud

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

In questi casi:

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

#### GetObject e replicazione tra griglie

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

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

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

### HeadObject

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

#### HeadObject e oggetti multiparte

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

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

#### Caratteri UTF-8 nei metadati utente

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

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

#### Intestazione della richiesta supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`

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

#### Intestazione della richiesta non supportata

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

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

#### Controllo delle versioni

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

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

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

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

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

#### Risposte HeadObject per gli oggetti Cloud Storage Pool

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

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

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

| Stato dell'oggetto | Risposta a HeadObject |
| --- | --- |
| Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione | `200 OK`(Non viene restituita alcuna intestazione di risposta speciale.) |
| Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`<br><br>Finché l'oggetto non viene portato in uno stato non recuperabile, il valore per `expiry-date` è ambientato in un lontano futuro. Il momento esatto della transizione non è controllato dal sistema StorageGRID . |
| L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche sulla griglia | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`<br><br>Il valore per `expiry-date` è ambientato in un lontano futuro.<br><br>**Nota**: se la copia sulla griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario emettere un"Ripristina oggetto" richiedere di ripristinare la copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto. |
| L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia sulla griglia | `200 OK`<br><br>`x-amz-storage-class: GLACIER` |
| Oggetto in fase di ripristino da uno stato non recuperabile | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="true"` |

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

### Oggetti multiparte o segmentati in Cloud Storage Pool

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

#### HeadObject e replicazione cross-grid

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

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

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

### MettiOggetto

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

#### Risolvere i conflitti

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

#### Dimensione dell'oggetto

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

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

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

#### Dimensione dei metadati utente

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

#### Caratteri UTF-8 nei metadati utente

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

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

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

#### Limiti dei tag degli oggetti

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

#### Proprietà dell'oggetto

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

#### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

- `Content-Encoding`

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

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

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

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

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

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

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

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

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

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

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

  VedereIntestazioni di richiesta per la crittografia lato server

#### Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

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

#### Opzioni di classe di archiviazione

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

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

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

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

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

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

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

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

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

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

#### Intestazioni di richiesta per la crittografia lato server

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

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

    Quando il `x-amz-server-side-encryption` l'intestazione non è inclusa nella richiesta PutObject, la griglia"impostazione di crittografia degli oggetti memorizzati" viene omesso dalla risposta PutObject.
- **SSE-C**: utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo

oggetto.

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

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

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

#### Controllo delle versioni

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

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

#### Calcoli della firma per l'intestazione di autorizzazione

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

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

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

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

#### Informazioni correlate

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

### Ripristina oggetto

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

#### Tipo di richiesta supportato

StorageGRID supporta solo le richieste RestoreObject per ripristinare un oggetto. Non supporta il `SELECT` tipo di restauro. Seleziona le richieste di ritorno `XNotImplemented` .

#### Controllo delle versioni

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

#### Comportamento di RestoreObject sugli oggetti Cloud Storage Pool

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

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

| Stato dell'oggetto | Comportamento di RestoreObject |
|---|---|
| Oggetto inserito in StorageGRID ma non ancora valutato da ILM oppure l'oggetto non si trova in un Cloud Storage Pool | `403 Forbidden` , `InvalidObjectState` |
| Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile | `200 OK`Non vengono apportate modifiche.<br><br>**Nota**: prima che un oggetto sia passato a uno stato non recuperabile, non è possibile modificarne lo stato. `expiry-date` . |
| Oggetto passato a uno stato non recuperabile | `202 Accepted`Ripristina una copia recuperabile dell'oggetto nel Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto torna a uno stato non recuperabile.<br><br>Facoltativamente, utilizzare il `Tier` elemento di richiesta per determinare quanto tempo impiegherà il processo di ripristino per essere completato(`Expedited` , `Standard` , O `Bulk` ). Se non specifichi `Tier` , IL `Standard` viene utilizzato il livello.<br><br>**Importante**: se un oggetto è stato trasferito a S3 Glacier Deep Archive o il pool di archiviazione cloud utilizza l'archiviazione BLOB di Azure, non è possibile ripristinarlo utilizzando `Expedited` livello. Viene restituito il seguente errore `403 Forbidden` , `InvalidTier` : `Retrieval option is not supported by this storage class.` |
| Oggetto in fase di ripristino da uno stato non recuperabile | `409 Conflict` , `RestoreAlreadyInProgress` |

| Stato dell'oggetto | Comportamento di RestoreObject |
| --- | --- |
| Oggetto completamente ripristinato nel Cloud Storage Pool | `200 OK`<br><br>**Nota:** se un oggetto è stato ripristinato in uno stato recuperabile, è possibile modificarne lo stato `expiry-date` riemettendo la richiesta RestoreObject con un nuovo valore per `Days` . La data di ripristino viene aggiornata in base al momento della richiesta. |

#### SelezionaOggettoContenuto

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

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

**Prima di iniziare**

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

**Esempio di sintassi della richiesta CSV**

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

**Esempio di sintassi della richiesta Parquet**

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

#### Esempio di query SQL

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

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

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

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

**Esempio di utilizzo di AWS-CLI (CSV)**

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

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

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

**Esempio di utilizzo di AWS-CLI (Parquet)**

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

Le prime righe del file di output, changes.csv, hanno questo aspetto:

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

## Operazioni per caricamenti multiparte

**Operazioni per caricamenti multiparte**

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

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

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

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

    - Quando si valuta l'ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2 al momento dell'acquisizione. Tuttavia, quando l'ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.

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

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

#### Caricamento multiparte completo

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

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

#### Risolvere i conflitti

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

#### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

#### Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

#### Controllo delle versioni

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

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

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

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

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

#### Replicazione, notifica o notifica dei metadati non riuscita

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

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

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

### CreaCaricamentoMultiparte

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

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

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

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

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

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

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

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

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

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

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

#### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

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

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

stato creato l'oggetto. Per esempio:

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

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

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

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

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

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

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

    Intestazioni di richiesta per la crittografia lato server

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

#### Intestazioni di richiesta per la crittografia lato server

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

- **SSE**: utilizzare la seguente intestazione nella richiesta CreateMultipartUpload se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: utilizzare tutte e tre queste intestazioni nella richiesta CreateMultipartUpload (e in ogni successiva richiesta UploadPart) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo

oggetto.

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

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

#### Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata:

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

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

#### Controllo delle versioni

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

### Caricamenti multiparte di List

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

Sono supportati i seguenti parametri di richiesta:

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

#### Controllo delle versioni

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

### CaricaParte

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

#### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

#### Intestazioni di richiesta per la crittografia lato server

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

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

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

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

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

#### Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

#### Controllo delle versioni

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

### CaricaParteCopia

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

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

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

sistema StorageGRID .

Sono supportate le seguenti intestazioni di richiesta:

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

#### Intestazioni di richiesta per la crittografia lato server

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

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

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

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

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

#### Controllo delle versioni

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

## Risposte di errore

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

**Codici di errore API S3 supportati**

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

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

**Codici di errore personalizzati StorageGRID**

| Nome | Descrizione | Stato HTTP |
| --- | --- | --- |
| XBucketLifecycleNotAllowed | La configurazione del ciclo di vita del bucket non è consentita in un bucket conforme legacy | 400 Richiesta non valida |
| XBucketPolicyParseException | Impossibile analizzare il JSON del criterio del bucket ricevuto. | 400 Richiesta non valida |

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

# Operazioni personalizzate StorageGRID

## Operazioni personalizzate StorageGRID

Il sistema StorageGRID supporta operazioni personalizzate che vengono aggiunte all'API REST S3.

Nella tabella seguente sono elencate le operazioni personalizzate supportate da StorageGRID.

| Operazione | Descrizione |
|---|---|
| "OTTIENI la coerenza del bucket" | Restituisce la coerenza applicata a un determinato bucket. |
| "PUT Consistenza del secchio" | Imposta la coerenza applicata a un determinato bucket. |
| "GET Ora dell'ultimo accesso al bucket" | Restituisce se gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati o disabilitati per un determinato bucket. |
| "Ora dell'ultimo accesso al bucket PUT" | Consente di abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso per un determinato bucket. |
| "ELIMINA la configurazione della notifica dei metadati del bucket" | Elimina l'XML di configurazione delle notifiche dei metadati associato a un determinato bucket. |

| Operazione | Descrizione |
| --- | --- |
| "Configurazione della notifica dei metadati del bucket GET" | Restituisce il file XML di configurazione delle notifiche dei metadati associato a un determinato bucket. |
| "Configurazione della notifica dei metadati del bucket PUT" | Configura il servizio di notifica dei metadati per un bucket. |
| "Utilizzo dello spazio di archiviazione GET" | Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account. |
| "Obsoleto: CreateBucket con impostazioni di conformità" | Obsoleto e non supportato: non è più possibile creare nuovi bucket con la conformità abilitata. |
| "Obsoleto: conformità al bucket GET" | Obsoleto ma supportato: restituisce le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente. |
| "Obsoleto: conformità al bucket PUT" | Obsoleto ma supportato: consente di modificare le impostazioni di conformità per un bucket Compliant legacy esistente. |

## OTTIENI la coerenza del bucket

La richiesta di coerenza del bucket GET consente di determinare la coerenza applicata a un determinato bucket.

La coerenza predefinita è impostata per garantire la lettura dopo la scrittura per gli oggetti appena creati.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketConsistency oppure essere l'account root.

### Richiedi esempio

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

### Risposta

Nella risposta XML, `<Consistency>` restituirà uno dei seguenti valori:

| Coerenza | Descrizione |
| --- | --- |
| Tutto | Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà. |
| forte-globale | Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti. |

| Coerenza | Descrizione |
|---|---|
| sito forte | Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito. |
| lettura dopo nuova scrittura | (Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi. |
| disponibile | Fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool . |

**Esempio di risposta**

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

**Informazioni correlate**

"Valori di coerenza"

## PUT Consistenza del secchio

La richiesta di coerenza PUT Bucket consente di specificare la coerenza da applicare alle operazioni eseguite su un bucket.

La coerenza predefinita è impostata per garantire la lettura dopo la scrittura per gli oggetti appena creati.

**Prima di iniziare**

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketConsistency oppure essere l'account root.

**Richiesta**

IL `x-ntap-sg-consistency` il parametro deve contenere uno dei seguenti valori:

| Coerenza | Descrizione |
| --- | --- |
| Tutto | Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà. |
| forte-globale | Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti. |
| sito forte | Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito. |
| lettura dopo nuova scrittura | (Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi. |
| disponibile | Fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool . |

**Nota:** in generale, dovresti usare la coerenza "Lettura dopo nuova scrittura". Se le richieste non funzionano correttamente, modificare, se possibile, il comportamento del client dell'applicazione. Oppure, configura il client in modo che specifichi la coerenza per ogni richiesta API. Impostare la coerenza a livello di bucket solo come ultima risorsa.

#### Richiedi esempio

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### Informazioni correlate

"Valori di coerenza"

## GET Ora dell'ultimo accesso al bucket

La richiesta GET sull'orario dell'ultimo accesso al bucket consente di determinare se gli aggiornamenti dell'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketLastAccessTime oppure essere l'account root.

#### Richiedi esempio

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

**Esempio di risposta**

Questo esempio mostra che gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati per il bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

## Ora dell'ultimo accesso al bucket PUT

La richiesta dell'orario dell'ultimo accesso al bucket PUT consente di abilitare o disabilitare gli aggiornamenti dell'orario dell'ultimo accesso per singoli bucket. La disattivazione degli aggiornamenti dell'ora dell'ultimo accesso migliora le prestazioni ed è l'impostazione predefinita per tutti i bucket creati con la versione 10.3.0 o successiva.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketLastAccessTime per un bucket oppure essere l'account root.

> A partire dalla versione 10.3 StorageGRID , gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera applicare il nuovo comportamento predefinito, è necessario disabilitare esplicitamente gli aggiornamenti dell'ora dell'ultimo accesso per ciascuno di tali bucket precedenti. È possibile abilitare o disabilitare gli aggiornamenti all'orario dell'ultimo accesso tramite la richiesta dell'orario dell'ultimo accesso al bucket PUT o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedere "Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso" .

Se gli aggiornamenti dell'ora dell'ultimo accesso sono disabilitati per un bucket, alle operazioni sul bucket viene applicato il seguente comportamento:

- Le richieste GetObject, GetObjectAcl, GetObjectTagging e HeadObject non aggiornano l'ora dell'ultimo accesso. L'oggetto non viene aggiunto alle code per la valutazione della gestione del ciclo di vita delle informazioni (ILM).

- Le richieste CopyObject e PutObjectTagging che aggiornano solo i metadati aggiornano anche l'ora dell'ultimo accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per il bucket di origine, le richieste CopyObject non aggiornano l'ora dell'ultimo accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM per il bucket di origine. Tuttavia, per la destinazione, le richieste CopyObject aggiornano sempre l'ora dell'ultimo accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- Le richieste CompleteMultipartUpload aggiornano l'orario dell'ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

**Esempi di richiesta**

Questo esempio abilita l'orario dell'ultimo accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Questo esempio disabilita l'orario dell'ultimo accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## ELIMINA la configurazione della notifica dei metadati del bucket

La richiesta di configurazione della notifica dei metadati DELETE Bucket consente di disabilitare il servizio di integrazione della ricerca per singoli bucket eliminando l'XML di configurazione.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket oppure essere l'account root.

**Richiedi esempio**

Questo esempio mostra come disabilitare il servizio di integrazione della ricerca per un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## Configurazione della notifica dei metadati del bucket GET

La richiesta di configurazione della notifica dei metadati del bucket GET consente di recuperare l'XML di configurazione utilizzato per configurare l'integrazione della ricerca per i singoli bucket.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketMetadataNotification oppure essere l'account root.

### Richiedi esempio

Questa richiesta recupera la configurazione della notifica dei metadati per il bucket denominato `bucket` .

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

### Risposta

Il corpo della risposta include la configurazione della notifica dei metadati per il bucket. La configurazione della notifica dei metadati consente di determinare come configurare il bucket per l'integrazione della ricerca. Ciò significa che è possibile determinare quali oggetti sono indicizzati e a quali endpoint vengono inviati i metadati degli oggetti.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione a cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID .

| Nome | Descrizione | Necessario |
| --- | --- | --- |
| MetadatiNotificaConfigurazione | Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati.<br><br>Contiene uno o più elementi Rule. | SÌ |
| Regola | Tag contenitore per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato.<br><br>Le regole con prefissi sovrapposti vengono rifiutate.<br><br>Incluso nell'elemento MetadataNotificationConfiguration. | SÌ |
| ID | Identificatore univoco per la regola.<br><br>Incluso nell'elemento Regola. | NO |
| Stato | Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate.<br><br>Incluso nell'elemento Regola. | SÌ |
| Prefisso | Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata.<br><br>Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto.<br><br>Incluso nell'elemento Regola. | SÌ |
| Destinazione | Tag contenitore per la destinazione di una regola.<br><br>Incluso nell'elemento Regola. | SÌ |

| Nome | Descrizione | Necessario |
| --- | --- | --- |
| Urna | URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà:<br>• `es`deve essere il terzo elemento.<br>• L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato `domain-name/myindex/mytype` .<br>Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma:<br>• `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br>L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404.<br>L'urna è inclusa nell'elemento Destinazione. | SÌ |

**Esempio di risposta**

L'XML incluso tra `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra come l'integrazione con un endpoint di integrazione della ricerca è configurata per il bucket. In questo esempio, i metadati dell'oggetto vengono inviati a un indice Elasticsearch denominato `current` e digita denominato `2017` che è ospitato in un dominio AWS denominato `records` .

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**Informazioni correlate**

"Utilizzare un account tenant"

## Configurazione della notifica dei metadati del bucket PUT

La richiesta di configurazione della notifica dei metadati del bucket PUT consente di abilitare il servizio di integrazione della ricerca per singoli bucket. Il codice XML di configurazione della notifica dei metadati fornito nel corpo della richiesta specifica gli oggetti i cui metadati vengono inviati all'indice di ricerca di destinazione.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketMetadataNotification per un bucket oppure essere l'account root.

### Richiesta

La richiesta deve includere la configurazione della notifica dei metadati nel corpo della richiesta. Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione a cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, potresti inviare metadati per oggetti con il prefisso `/images` verso una destinazione e oggetti con il prefisso `/videos` all'altro.

Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che includeva una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non sarebbe consentito.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID . L'endpoint deve esistere quando viene inviata la configurazione della notifica dei metadati, altrimenti la richiesta fallisce come

`400 Bad Request` Il messaggio di errore afferma: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

La tabella descrive gli elementi presenti nel file XML di configurazione delle notifiche dei metadati.

| Nome | Descrizione | Necessario |
|---|---|---|
| MetadatiNotificaConfigurazione | Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati.<br><br>Contiene uno o più elementi Rule. | SÌ |
| Regola | Tag contenitore per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato.<br><br>Le regole con prefissi sovrapposti vengono rifiutate.<br><br>Incluso nell'elemento MetadataNotificationConfiguration. | SÌ |
| ID | Identificatore univoco per la regola.<br><br>Incluso nell'elemento Regola. | NO |
| Stato | Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate.<br><br>Incluso nell'elemento Regola. | SÌ |

| Nome | Descrizione | Necessario |
| --- | --- | --- |
| Prefisso | Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata.<br><br>Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto.<br><br>Incluso nell'elemento Regola. | SÌ |
| Destinazione | Tag contenitore per la destinazione di una regola.<br><br>Incluso nell'elemento Regola. | SÌ |
| Urna | URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà:<br><br>• `es`deve essere il terzo elemento.<br>• L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato `domain-name/myindex/mytype` .<br><br>Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma:<br><br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br><br>L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404.<br><br>L'urna è inclusa nell'elemento Destinazione. | SÌ |

**Esempi di richiesta**

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati di tutti gli oggetti vengono inviati alla stessa destinazione.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

In questo esempio, metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti corrispondono al prefisso `/videos` viene inviato a una seconda destinazione.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**JSON generato dal servizio di integrazione della ricerca**

Quando si abilita il servizio di integrazione della ricerca per un bucket, ogni volta che vengono aggiunti, aggiornati o eliminati metadati o tag di un oggetto, viene generato un documento JSON che viene inviato all'endpoint di destinazione.

Questo esempio mostra un esempio del JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test` . IL `test` il bucket non è sottoposto a versioning, quindi `versionId` il tag è vuoto.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

**Metadati degli oggetti inclusi nelle notifiche dei metadati**

Nella tabella sono elencati tutti i campi inclusi nel documento JSON inviato all'endpoint di destinazione quando è abilitata l'integrazione della ricerca.

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

| Tipo | Nome dell'articolo | Descrizione |
|---|---|---|
| Informazioni su bucket e oggetti | secchio | Nome del bucket |
| Informazioni su bucket e oggetti | chiave | Nome chiave oggetto |
| Informazioni su bucket e oggetti | ID versione | Versione dell'oggetto, per gli oggetti nei bucket con versione |
| Informazioni su bucket e oggetti | regione | Regione del bucket, ad esempio `us-east-1` |
| Metadati di sistema | misurare | Dimensione dell'oggetto (in byte) visibile a un client HTTP |
| Metadati di sistema | md5 | Hash dell'oggetto |
| Metadati utente | metadati *`key:value`* | Tutti i metadati utente per l'oggetto, come coppie chiave-valore |
| Etichette | etichette *`key:value`* | Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore |

Per i tag e i metadati utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. È necessario abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

**Informazioni correlate**

"Utilizzare un account tenant"

## Richiesta di utilizzo dello spazio di archiviazione GET

La richiesta GET Storage Usage indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.

La quantità di spazio di archiviazione utilizzata da un account e dai suoi bucket può essere ottenuta tramite una richiesta ListBuckets modificata con `x-ntap-sg-usage` parametro di query. L'utilizzo dello spazio di archiviazione del bucket viene monitorato separatamente dalle richieste PUT e DELETE elaborate dal sistema. Potrebbe verificarsi un ritardo prima che i valori di utilizzo corrispondano ai valori previsti in base all'elaborazione delle richieste, in particolare se il sistema è sottoposto a un carico elevato.

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando la coerenza globale forte. Se non è possibile ottenere una coerenza globale forte, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una coerenza del sito forte.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:ListAllMyBuckets oppure essere l'account root.

**Richiedi esempio**

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

**Esempio di risposta**

Questo esempio mostra un account con quattro oggetti e 12 byte di dati in due bucket. Ogni bucket contiene due oggetti e sei byte di dati.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

#### Controllo delle versioni

Ogni versione dell'oggetto memorizzata contribuirà a `ObjectCount` E `DataBytes` valori nella risposta. I marcatori di eliminazione non vengono aggiunti al `ObjectCount` totale.

#### Informazioni correlate

"Valori di coerenza"

## Richieste di bucket deprecate per la conformità legacy

#### Richieste di bucket deprecate per la conformità legacy

Potrebbe essere necessario utilizzare l'API REST StorageGRID S3 per gestire i bucket creati utilizzando la funzionalità di conformità legacy.

##### Funzionalità di conformità deprecata

La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock.

Se in precedenza è stata abilitata l'impostazione Conformità globale, in StorageGRID 11.6 è abilitata l'impostazione Blocco oggetto S3 globale. Non è più possibile creare nuovi bucket con la conformità abilitata; tuttavia, se necessario, è possibile utilizzare l'API REST StorageGRID S3 per gestire eventuali bucket conformi legacy esistenti.

- "Utilizzare l'API REST S3 per configurare S3 Object Lock"
- "Gestire gli oggetti con ILM"
- "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Richieste di conformità deprecate:

- "Obsoleto - Modifiche alla richiesta PUT Bucket per conformità"

  L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML facoltativo delle richieste PUT Bucket per creare un bucket conforme.

- "Obsoleto - Conformità al bucket GET"

  La richiesta di conformità del bucket GET è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Conforme legacy esistente.

- "Obsoleto - Conformità al bucket PUT"

  La richiesta di conformità del bucket PUT è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket Conforme legacy esistente. Ad esempio, è possibile mettere in attesa per motivi legali un bucket esistente o aumentarne il periodo di conservazione.

**Obsoleto: modifiche alla richiesta CreateBucket per conformità**

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML facoltativa delle richieste CreateBucket per creare un bucket conforme.

> La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:
>
> - "Utilizzare l'API REST S3 per configurare S3 Object Lock"
> - "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Non è più possibile creare nuovi bucket con la Conformità abilitata. Se si tenta di utilizzare le modifiche alla richiesta CreateBucket per la conformità per creare un nuovo bucket conforme, viene restituito il seguente messaggio di errore:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

### Obsoleto: richiesta di conformità del bucket GET

La richiesta di conformità del bucket GET è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Conforme legacy esistente.

> La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:
>
> - "Utilizzare l'API REST S3 per configurare S3 Object Lock"
> - "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketCompliance oppure essere l'account root.

#### Richiedi esempio

Questa richiesta di esempio consente di determinare le impostazioni di conformità per il bucket denominato `mybucket` .

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### Esempio di risposta

Nella risposta XML, `<SGCompliance>` elenca le impostazioni di conformità in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di conformità per un bucket in cui ogni oggetto verrà conservato per un anno (525.600 minuti), a partire dal momento in cui l'oggetto viene inserito nella griglia. Al momento non esiste alcun blocco legale su questo bucket. Ogni oggetto verrà automaticamente eliminato dopo un anno.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| Nome | Descrizione |
| --- | --- |
| Periodo di conservazioneMinuti | Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia. |
| LegalHold | • Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto.<br>• Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione. |
| Eliminazione automatica | • Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale.<br>• Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente. |

#### Risposte di errore

Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è `404 Not Found` , con un codice di errore S3 di `XNoSuchBucketCompliance` .

### Obsoleto: richiesta di conformità del bucket PUT

La richiesta di conformità del bucket PUT è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket Conforme legacy esistente. Ad esempio, è possibile mettere in attesa per motivi legali un bucket esistente o aumentarne il periodo di conservazione.

> La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:
>
> • "Utilizzare l'API REST S3 per configurare S3 Object Lock"
> • "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketCompliance oppure essere l'account root.

Quando si invia una richiesta di conformità del bucket PUT, è necessario specificare un valore per ogni campo delle impostazioni di conformità.

#### Richiedi esempio

Questa richiesta di esempio modifica le impostazioni di conformità per il bucket denominato `mybucket` . In questo esempio, gli oggetti in `mybucket` verranno ora conservati per due anni (1.051.200 minuti) anziché uno, a partire dal momento in cui l'oggetto viene inserito nella griglia. Non esiste alcun vincolo legale su questo

secchio. Ogni oggetto verrà automaticamente eliminato dopo due anni.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| Nome | Descrizione |
|---|---|
| Periodo di conservazioneMinuti | Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia.<br><br>**Importante** Quando si specifica un nuovo valore per RetentionPeriodMinutes, è necessario specificare un valore uguale o maggiore del periodo di conservazione corrente del bucket. Dopo aver impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore; è possibile solo aumentarlo. |
| LegalHold | • Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto.<br>• Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione. |
| Eliminazione automatica | • Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale.<br>• Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente. |

#### Coerenza per le impostazioni di conformità

Quando si aggiornano le impostazioni di conformità per un bucket S3 con una richiesta di conformità del bucket PUT, StorageGRID tenta di aggiornare i metadati del bucket in tutta la griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **Strong-global** per garantire che tutti i siti dei data center e tutti i nodi di archiviazione che contengono metadati dei bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere la coerenza **Strong-global** perché un sito del data center o più nodi di archiviazione in un sito non sono disponibili, il codice di stato HTTP per la risposta è `503 Service Unavailable.`

Se si riceve questa risposta, è necessario contattare l'amministratore della rete per assicurarsi che i servizi di archiviazione richiesti siano resi disponibili il prima possibile. Se l'amministratore della rete non è in grado di rendere disponibili sufficienti nodi di archiviazione in ciascun sito, il supporto tecnico potrebbe consigliarti di riprovare la richiesta non riuscita forzando la coerenza **Strong-site**.

> Non forzare mai la coerenza **Strong-site** per la conformità del bucket PUT, a meno che non ti sia stato chiesto di farlo dal supporto tecnico e a meno che tu non comprenda le potenziali conseguenze dell'utilizzo di questo livello.

Quando la coerenza viene ridotta a **Strong-site**, StorageGRID garantisce che le impostazioni di conformità aggiornate avranno coerenza di lettura dopo scrittura solo per le richieste client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe avere temporaneamente più impostazioni incoerenti per questo bucket finché tutti i siti e i nodi di archiviazione non saranno disponibili. Impostazioni incoerenti possono dare luogo a comportamenti inaspettati e indesiderati. Ad esempio, se si sottopone un bucket a un blocco legale e si impone una minore coerenza, le precedenti impostazioni di conformità del bucket (ovvero il blocco legale) potrebbero continuare a essere valide in alcuni siti di data center. Di conseguenza, gli oggetti che ritieni siano in sospeso a fini legali potrebbero essere eliminati alla scadenza del periodo di conservazione, dall'utente o tramite l'eliminazione automatica, se abilitata.

Per forzare l'uso della coerenza **Strong-site**, riemettere la richiesta di conformità del bucket PUT e includere `Consistency-Control` Intestazione della richiesta HTTP, come segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

#### Risposte di errore

- Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è `404 Not Found`.
- Se `RetentionPeriodMinutes` nella richiesta è inferiore al periodo di conservazione corrente del bucket, il codice di stato HTTP è `400 Bad Request`.

#### Informazioni correlate

"Obsoleto: modifiche alla richiesta PUT Bucket per conformità"

# Criteri di accesso a bucket e gruppi

## Utilizzare criteri di accesso a bucket e gruppi

StorageGRID utilizza il linguaggio delle policy di Amazon Web Services (AWS) per consentire ai tenant S3 di controllare l'accesso ai bucket e agli oggetti all'interno di tali bucket. Il sistema StorageGRID implementa un sottoinsieme del linguaggio di policy dell'API REST S3. Le policy di accesso per l'API S3 sono scritte in JSON.

### Panoramica della politica di accesso

StorageGRID supporta due tipi di criteri di accesso.

- **Politiche bucket**, gestite tramite le operazioni API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy oppure tramite l'API Tenant Manager o Tenant Management. I criteri dei bucket sono associati ai bucket e sono quindi configurati per controllare l'accesso degli utenti nell'account proprietario del bucket o di altri account al bucket e agli oggetti in esso contenuti. Una policy basata su bucket si applica a un solo bucket e, possibilmente, a più gruppi.
- **Criteri di gruppo**, configurati tramite Tenant Manager o Tenant Management API. I criteri di gruppo sono associati a un gruppo nell'account e sono quindi configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Un criterio di gruppo si applica a un solo gruppo e, possibilmente, a più bucket.

Non vi è alcuna differenza di priorità tra i criteri di gruppo e quelli di bucket.

I criteri di gruppo e bucket StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy e ciascuna dichiarazione contiene i seguenti elementi:

- ID dichiarazione (Sid) (facoltativo)
- Effetto
- Principale/Non Principale
- Risorsa/Non Risorsa
- Azione/Non azione
- Condizione (facoltativa)

Le istruzioni di policy vengono create utilizzando questa struttura per specificare le autorizzazioni: Concedi <Effetto> per consentire/negare a <Principale> di eseguire <Azione> su <Risorsa> quando si applica <Condizione>.

Ogni elemento della policy viene utilizzato per una funzione specifica:

| Elemento | Descrizione |
|---|---|
| Sid | L'elemento Sid è facoltativo. Il Sid è inteso solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID . |
| Effetto | Utilizzare l'elemento Effetto per stabilire se le operazioni specificate sono consentite o negate. È necessario identificare le operazioni consentite (o negate) sui bucket o sugli oggetti utilizzando le parole chiave dell'elemento Azione supportate. |

| Elemento | Descrizione |
| --- | --- |
| Principale/Non Principale | È possibile consentire a utenti, gruppi e account di accedere a risorse specifiche ed eseguire azioni specifiche. Se nella richiesta non è inclusa alcuna firma S3, l'accesso anonimo è consentito specificando il carattere jolly (*) come principale. Per impostazione predefinita, solo l'account root ha accesso alle risorse di proprietà dell'account.<br><br>È sufficiente specificare l'elemento Principal in un criterio bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito. |
| Risorsa/Non Risorsa | L'elemento Risorsa identifica bucket e oggetti. È possibile concedere o negare autorizzazioni a bucket e oggetti utilizzando l'Amazon Resource Name (ARN) per identificare la risorsa. |
| Azione/Non azione | Gli elementi Azione ed Effetto sono i due componenti delle autorizzazioni. Quando un gruppo richiede una risorsa, gli viene concesso o negato l'accesso alla risorsa. L'accesso viene negato a meno che non si assegnino autorizzazioni specifiche, ma è possibile utilizzare la negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio. |
| Condizione | L'elemento Condizione è facoltativo. Le condizioni consentono di creare espressioni per determinare quando applicare una policy. |

Nell'elemento Azione, è possibile utilizzare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde ad autorizzazioni quali s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Risorsa è possibile utilizzare i caratteri jolly (*) e (?). Mentre l'asterisco (*) corrisponde a 0 o più caratteri, il punto interrogativo (?) corrisponde a qualsiasi singolo carattere.

Nell'elemento Principal, i caratteri jolly non sono supportati, tranne che per impostare l'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, si imposta il carattere jolly (*) come valore Principale.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effetto, Principale, Azione e Risorsa. Questo esempio mostra un'istruzione completa della policy del bucket che utilizza l'effetto "Consenti" per fornire ai Principals, il gruppo di amministrazione `federated-group/admin` e il gruppo finanziario `federated-group/finance` , autorizzazioni per eseguire l'azione `s3:ListBucket` sul secchio denominato `mybucket` e l'azione `s3:GetObject` su tutti gli oggetti all'interno di quel contenitore.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

Il criterio del bucket ha un limite di dimensione di 20.480 byte, mentre il criterio del gruppo ha un limite di dimensione di 5.120 byte.

**Coerenza per le politiche**

Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche potrebbero richiedere altri 15 minuti per diventare effettive, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri dei bucket sono fortemente coerenti.

Se necessario, è possibile modificare le garanzie di coerenza per gli aggiornamenti dei criteri dei bucket. Ad esempio, potresti voler rendere disponibile una modifica ai criteri di un bucket durante un'interruzione del sito.

In questo caso, è possibile impostare il `Consistency-Control` intestazione nella richiesta PutBucketPolicy oppure puoi utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio di bucket diventa coerente, le modifiche potrebbero richiedere altri 8 secondi per diventare effettive, a causa della memorizzazione nella cache dei criteri.

> Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di ripristinare l'impostazione a livello di bucket al valore originale al termine dell'operazione. In caso contrario, tutte le future richieste di bucket utilizzeranno l'impostazione modificata.

**Utilizzare ARN nelle dichiarazioni di policy**

Nelle dichiarazioni di policy, l'ARN viene utilizzato negli elementi Principal e Resource.

- Utilizzare questa sintassi per specificare l'ARN della risorsa S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilizzare questa sintassi per specificare l'ARN della risorsa identità (utenti e gruppi):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Altre considerazioni:

- È possibile utilizzare l'asterisco (*) come carattere jolly per trovare la corrispondenza con zero o più caratteri all'interno della chiave dell'oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave dell'oggetto, devono essere codificati utilizzando JSON UTF-8 o sequenze di escape JSON \u. La codifica percentuale non è supportata.

  "Sintassi URN RFC 2141"

  Il corpo della richiesta HTTP per l'operazione PutBucketPolicy deve essere codificato con charset=UTF-8.

**Specificare le risorse in una policy**

Nelle istruzioni dei criteri, è possibile utilizzare l'elemento Risorsa per specificare il bucket o l'oggetto per cui sono concesse o negate le autorizzazioni.

- Ogni dichiarazione di policy richiede un elemento Risorsa. In una policy, le risorse sono indicate dall'elemento `Resource` , o in alternativa, `NotResource` per l'esclusione.
- È possibile specificare le risorse con un ARN di risorsa S3. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- È anche possibile utilizzare variabili di policy all'interno della chiave dell'oggetto. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Il valore della risorsa può specificare un bucket che non esiste ancora al momento della creazione di un criterio di gruppo.

### Specificare i principi in una policy

Utilizzare l'elemento Principal per identificare l'utente, il gruppo o l'account tenant a cui è consentito/negato l'accesso alla risorsa in base all'istruzione di policy.

- Ogni istruzione di policy in una policy di bucket deve includere un elemento Principal. Le istruzioni di policy in un criterio di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In una policy, i mandanti sono indicati dall'elemento "Manager" o, in alternativa, "NotManager" per l'esclusione.
- Le identità basate sull'account devono essere specificate utilizzando un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- In questo esempio viene utilizzato l'ID account tenant 27233906934684427525, che include l'account root e tutti gli utenti nell'account:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- È possibile specificare solo l'account root:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- È possibile specificare un utente federato specifico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- È possibile specificare un gruppo federato specifico ("Manager"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- È possibile specificare un'entità anonima:

```
"Principal": "*"
```

- Per evitare ambiguità, è possibile utilizzare l'UUID dell'utente anziché il nome utente:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

Ad esempio, supponiamo che Alex lasci l'organizzazione e il nome utente `Alex` viene eliminato. Se un nuovo Alex si unisce all'organizzazione e gli viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe ereditare involontariamente i permessi concessi all'utente originale.

- Il valore principale può specificare un nome di gruppo/utente che non esiste ancora al momento della creazione di un criterio bucket.

### Specificare le autorizzazioni in una policy

In una policy, l'elemento Azione viene utilizzato per concedere/negare le autorizzazioni a una risorsa. Esiste una serie di autorizzazioni che è possibile specificare in una policy, contrassegnate dall'elemento "Azione" o, in alternativa, "NonAzione" per l'esclusione. Ciascuno di questi elementi è mappato a specifiche operazioni dell'API REST S3.

Nelle tabelle sono elencate le autorizzazioni che si applicano ai bucket e le autorizzazioni che si applicano agli oggetti.

Amazon S3 ora utilizza l'autorizzazione s3:PutReplicationConfiguration per entrambe le azioni PutBucketReplication e DeleteBucketReplication. StorageGRID utilizza autorizzazioni separate per ogni azione, in linea con le specifiche originali di Amazon S3.

Un'operazione di eliminazione viene eseguita quando si utilizza un'istruzione put per sovrascrivere un valore esistente.

#### Autorizzazioni applicabili ai bucket

| Permessi | Operazioni API REST S3 | Personalizzato per StorageGRID |
|---|---|---|
| s3:CreaBucket | CreaBucket | Sì.<br><br>**Nota**: utilizzare solo nei criteri di gruppo. |
| s3:EliminaBucket | EliminaBucket | |
| s3:DeleteBucketMetadataNotification | ELIMINA la configurazione della notifica dei metadati del bucket | SÌ |
| s3:EliminaBucketPolicy | DeleteBucketPolicy | |
| s3:EliminaConfigurazioneReplicazione | DeleteBucketReplication | Sì, autorizzazioni separate per PUT e DELETE |
| s3:GetBucketAcl | OttieniBucketAcl | |
| s3:GetBucketCompliance | Conformità GET Bucket (obsoleto) | SÌ |
| s3:GetBucketConsistency | OTTIENI la coerenza del bucket | SÌ |

| Permessi | Operazioni API REST S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:GetBucketCORS | GetBucketCors | |
| s3:Ottieni configurazione crittografia | Ottieni crittografia dei bucket | |
| s3:GetBucketLastAccessTime | GET Ora dell'ultimo accesso al bucket | SÌ |
| s3:OttieniPosizioneBucket | OttieniPosizioneBucket | |
| s3:GetBucketMetadataNotification | Configurazione della notifica dei metadati del bucket GET | SÌ |
| s3:OttieniNotificaBucket | Configurazione di notifica di GetBucket | |
| s3:GetBucketObjectLockConfiguration | Ottieni configurazione blocco oggetto | |
| s3:GetBucketPolicy | OttieniPoliticaBucket | |
| s3:OttieniTaggingBucket | OttieniBucketTagging | |
| s3:GetBucketVersioning | GetBucketVersioning | |
| s3:GetLifecycleConfiguration | GetBucketLifecycleConfiguration | |
| s3:OttieniConfigurazioneReplicazione | OttieniReplicazioneBucket | |
| s3:ElencaTuttiIMieBucket | • ListBuckets<br>• Utilizzo dello spazio di archiviazione GET | Sì, per l'utilizzo dello spazio di archiviazione GET.<br><br>**Nota**: utilizzare solo nei criteri di gruppo. |
| s3:ElencoBucket | • ElencoOggetti<br>• HeadBucket<br>• Ripristina oggetto | |
| s3:ListBucketMultipartUploads | • Caricamenti multiparte di List<br>• Ripristina oggetto | |
| s3:ListBucketVersions | Versioni GET Bucket | |
| s3:PutBucketCompliance | Conformità al bucket PUT (obsoleto) | SÌ |

| Permessi | Operazioni API REST S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:PutBucketConsistency | PUT Consistenza del secchio | SÌ |
| s3:PutBucketCORS | • DeleteBucketCors†<br>• PutBucketCors | |
| s3:PutEncryptionConfiguration | • DeleteBucketEncryption<br>• PutBucketEncryption | |
| s3:PutBucketLastAccessTime | Ora dell'ultimo accesso al bucket PUT | SÌ |
| s3:PutBucketMetadataNotification | Configurazione della notifica dei metadati del bucket PUT | SÌ |
| s3:PutBucketNotification | Configurazione della notifica PutBucket | |
| s3:PutBucketObjectLockConfiguration | • CreateBucket con il `x-amz-bucket-object-lock-enabled: true` intestazione della richiesta (richiede anche l'autorizzazione s3:CreateBucket)<br>• PutObjectLockConfiguration | |
| s3:PoliticaPutBucket | PutBucketPolicy | |
| s3:PutBucketTagging | • EliminaBucketTagging†<br>• PutBucketTagging | |
| s3:PutBucketVersioning | PutBucketVersioning | |
| s3:PutLifecycleConfiguration | • DeleteBucketLifecycle†<br>• Configurazione del ciclo di vita di PutBucket | |
| s3:PutReplicationConfiguration | PutBucketReplication | Sì, autorizzazioni separate per PUT e DELETE |

**Autorizzazioni applicabili agli oggetti**

| Permessi | Operazioni API REST S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:AnnullaCaricamentoMultipart | • Annulla caricamento multiparte<br>• Ripristina oggetto | |
| s3:BypassGovernanceRetention | • EliminaOggetto<br>• EliminaOggetti<br>• PutObjectRetention | |
| s3:EliminaOggetto | • EliminaOggetto<br>• EliminaOggetti<br>• Ripristina oggetto | |
| s3:EliminaTaggingOggetto | DeleteObjectTagging | |
| s3:EliminaObjectVersionTagging | DeleteObjectTagging (una versione specifica dell'oggetto) | |
| s3:EliminaVersioneOggetto | DeleteObject (una versione specifica dell'oggetto) | |
| s3:OttieniOggetto | • OttieniOggetto<br>• HeadObject<br>• Ripristina oggetto<br>• SelezionaOggettoContenuto | |
| s3:GetObjectAcl | OttieniOggettoAcl | |
| s3:GetObjectLegalHold | OttieniOggettoLegaleHold | |
| s3:OttieniRitenzioneOggetto | Ottieni conservazione oggetto | |
| s3:OttieniTaggingOggetto | OttieniTaggingOggetto | |
| s3:GetObjectVersionTagging | GetObjectTagging (una versione specifica dell'oggetto) | |
| s3:GetObjectVersion | GetObject (una versione specifica dell'oggetto) | |
| s3:ListMultipartUploadParts | ListParts, RestoreObject | |

| Permessi | Operazioni API REST S3 | Personalizzato per StorageGRID |
|---|---|---|
| s3:PutObject | • MettiOggetto<br>• CopiaOggetto<br>• Ripristina oggetto<br>• CreaCaricamentoMultiparte<br>• Caricamento multiparte completo<br>• CaricaParte<br>• CaricaParteCopia | |
| s3:PutObjectLegalHold | PutObjectLegalHold | |
| s3:PutObjectRetention | PutObjectRetention | |
| s3:PutObjectTagging | PutObjectTagging | |
| s3:PutObjectVersionTagging | PutObjectTagging (una versione specifica dell'oggetto) | |
| s3:PutOverwriteObject | • MettiOggetto<br>• CopiaOggetto<br>• PutObjectTagging<br>• DeleteObjectTagging<br>• Caricamento multiparte completo | SÌ |
| s3:RipristinaOggetto | Ripristina oggetto | |

**Utilizzare l'autorizzazione PutOverwriteObject**

L'autorizzazione s3:PutOverwriteObject è un'autorizzazione StorageGRID personalizzata che si applica alle operazioni che creano o aggiornano oggetti. L'impostazione di questa autorizzazione determina se il client può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging degli oggetti S3.

Le possibili impostazioni per questa autorizzazione includono:

- **Consenti**: il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega**: Il client non può sovrascrivere un oggetto. Se impostato su Nega, l'autorizzazione PutOverwriteObject funziona come segue:
  - Se un oggetto esistente viene trovato nello stesso percorso:
    - I dati dell'oggetto, i metadati definiti dall'utente o i tag degli oggetti S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se è abilitato il controllo delle versioni S3, l'impostazione Nega impedisce alle operazioni

PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le sue versioni non correnti.

    - Se non viene trovato un oggetto esistente, questa autorizzazione non ha effetto.
- Quando questa autorizzazione non è presente, l'effetto è lo stesso che si avrebbe se fosse impostato Consenti.

> Se l'attuale policy S3 consente la sovrascrittura e l'autorizzazione PutOverwriteObject è impostata su Nega, il client non può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o i tag degli oggetti. Inoltre, se è selezionata la casella di controllo **Impedisci modifica client** (**CONFIGURAZIONE** > **Impostazioni di sicurezza** > **Rete e oggetti**), tale impostazione sostituisce l'impostazione dell'autorizzazione PutOverwriteObject.

### Specificare le condizioni in una policy

Le condizioni definiscono quando una politica entrerà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condizione può contenere più condizioni e ogni condizione può contenere più coppie chiave-valore. Il blocco di condizione utilizza il seguente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Nell'esempio seguente, la condizione IpAddress utilizza la chiave di condizione SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

#### Operatori di condizione supportati

Gli operatori condizionali sono classificati come segue:

- Corda
- Numerico
- Booleano
- indirizzo IP
- Controllo nullo

| Operatori di condizione | Descrizione |
| --- | --- |
| StringEquals | Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole). |
| Stringa non uguale | Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole). |
| StringEqualsIgnoreCase | Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora la distinzione tra maiuscole e minuscole). |
| StringNotEqualsIgnoreCase | Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora la distinzione tra maiuscole e minuscole). |
| StringLike | Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole). Può includere i caratteri jolly * e ?. |
| Stringa non piace | Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole). Può includere i caratteri jolly * e ?. |
| NumericEquals | Confronta una chiave con un valore numerico in base alla corrispondenza esatta. |
| NumericoNonUguale | Confronta una chiave con un valore numerico in base alla corrispondenza negata. |
| NumericoMaggioreDi | Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di". |
| NumericoMaggioreDiUguale | Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a". |
| NumericoMenoDi | Confronta una chiave con un valore numerico in base alla corrispondenza "minore di". |
| NumericoMinoreUguale | Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale". |
| Bool | Confronta una chiave con un valore booleano in base alla corrispondenza "vero o falso". |
| Indirizzo IP | Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP. |
| NonIndirizzoIP | Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata. |

| Operatori di condizione | Descrizione |
| --- | --- |
| Nullo | Controlla se una chiave di condizione è presente nel contesto della richiesta corrente. |

**Chiavi di condizione supportate**

| Chiavi di condizione | Azioni | Descrizione |
| --- | --- | --- |
| aws:SourceIp | operatori IP | Verrà confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti.<br><br>**Nota:** se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi amministrativi e sui nodi gateway, questa verrà confrontata con l'indirizzo IP a monte del servizio Load Balancer.<br><br>**Nota**: se viene utilizzato un bilanciatore del carico di terze parti non trasparente, questo verrà confrontato con l'indirizzo IP di tale bilanciatore del carico. Qualunque `X-Forwarded-For` l'intestazione verrà ignorata perché non è possibile accertarne la validità. |
| aws:nome utente | Risorsa/Identità | Verrà confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti. |
| s3:delimitatore | s3:ListBucket e<br><br>s3:permessi ListBucketVersions | Verrà confrontato con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions. |

| Chiavi di condizione | Azioni | Descrizione |
| --- | --- | --- |
| s3:ExistingObjectTag/<chiave-tag> | s3:EliminaTaggingOggetto<br><br>s3:EliminaObjectVersionTagging<br><br>s3:OttieniOggetto<br><br>s3:GetObjectAcl<br><br>3: Ottieni tag oggetto<br><br>s3:GetObjectVersion<br><br>s3:GetObjectVersionAcl<br><br>s3:GetObjectVersionTagging<br><br>s3:PutObjectAcl<br><br>s3:PutObjectTagging<br><br>s3:PutObjectVersionAcl<br><br>s3:PutObjectVersionTagging | Richiederà che l'oggetto esistente abbia la chiave e il valore del tag specifici. |
| s3:max-chiavi | s3:ListBucket e<br><br>s3:permessi ListBucketVersions | Verrà confrontato con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions. |
| s3:giorni di conservazione rimanenti del blocco dell'oggetto | s3:PutObject | Confronta con la data di conservazione specificata in `x-amz-object-lock-retain-until-date` intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori siano compresi nell'intervallo consentito per le seguenti richieste:<br><br>• MettiOggetto<br>• CopiaOggetto<br>• CreaCaricamentoMultiparte |
| s3:giorni di conservazione rimanenti del blocco dell'oggetto | s3:PutObjectRetention | Confronta con la retain-until-date specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito. |

| Chiavi di condizione | Azioni | Descrizione |
|---|---|---|
| s3:prefisso | s3:ListBucket e<br><br>s3:permessi ListBucketVersions | Verrà confrontato con il parametro prefisso specificato in una richiesta ListObjects o ListObjectVersions. |
| s3:RequestObjectTag/<chiave-tag> | s3:PutObject<br><br>s3:PutObjectTagging<br><br>s3:PutObjectVersionTagging | Richiederà una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging. |

**Specificare le variabili in una policy**

È possibile utilizzare le variabili nelle policy per popolare le informazioni sulle policy quando sono disponibili. È possibile utilizzare le variabili di policy in `Resource` elemento e nei confronti di stringhe in `Condition` elemento.

In questo esempio, la variabile `${aws:username}` fa parte dell'elemento Risorsa:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore della condizione nel blocco di condizioni:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

| Variabile | Descrizione |
|---|---|
| `${aws:SourceIp}` | Utilizza la chiave SourceIp come variabile fornita. |
| `${aws:username}` | Utilizza la chiave nome utente come variabile fornita. |
| `${s3:prefix}` | Utilizza la chiave del prefisso specifico del servizio come variabile fornita. |
| `${s3:max-keys}` | Utilizza la chiave max-keys specifica del servizio come variabile fornita. |

| Variabile | Descrizione |
| --- | --- |
| `${*}` | Carattere speciale. Utilizza il carattere come carattere letterale *. |
| `${?}` | Carattere speciale. Utilizza il carattere come carattere ? letterale. |
| `${$}` | Carattere speciale. Utilizza il carattere come carattere $ letterale. |

**Creare politiche che richiedono una gestione speciale**

Talvolta una policy può concedere autorizzazioni pericolose per la sicurezza o per il proseguimento delle operazioni, ad esempio bloccando l'utente root dell'account. L'implementazione dell'API REST S3 StorageGRID è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

| Descrizione della politica | Tipo di polizza | Comportamento di Amazon | Comportamento StorageGRID |
| --- | --- | --- | --- |
| Nega a te stesso qualsiasi autorizzazione all'account root | Secchio | Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3 | Stesso |
| Nega a te stesso qualsiasi autorizzazione all'utente/gruppo | Gruppo | Valido e applicato | Stesso |
| Consentire qualsiasi autorizzazione a un gruppo di account esteri | Secchio | Principale non valido | Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy |
| Consentire a un account esterno root o utente qualsiasi autorizzazione | Secchio | Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy | Stesso |

| Descrizione della politica | Tipo di polizza | Comportamento di Amazon | Comportamento StorageGRID |
|---|---|---|---|
| Consenti a tutti i permessi per tutte le azioni | Secchio | Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito per l'account esterno root e gli utenti | Stesso |
| Nega a tutti i permessi per tutte le azioni | Secchio | Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3 | Stesso |
| Il principale è un utente o un gruppo inesistente | Secchio | Principale non valido | Valido |
| La risorsa è un bucket S3 inesistente | Gruppo | Valido | Stesso |
| Principal è un gruppo locale | Secchio | Principale non valido | Valido |
| La policy concede a un account non proprietario (inclusi gli account anonimi) l'autorizzazione a inserire oggetti. | Secchio | Valido. Gli oggetti sono di proprietà dell'account del creatore e la policy del bucket non si applica. L'account del creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL degli oggetti. | Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la politica dei bucket. |

**Protezione WORM (Write-once-read-many)**

È possibile creare bucket WORM (write-once-read-many) per proteggere i dati, i metadati degli oggetti definiti dall'utente e il tagging degli oggetti S3. È possibile configurare i bucket WORM per consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione di contenuti esistenti. Utilizzare uno degli approcci descritti qui.

Per garantire che le sovrascritture vengano sempre negate, puoi:

- Da Grid Manager, vai su **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza** > **Rete e oggetti** e seleziona la casella di controllo **Impedisci modifiche client**.
- Applicare le seguenti regole e policy S3:
  - Aggiungere un'operazione PutOverwriteObject DENY al criterio S3.
  - Aggiungere un'operazione DeleteObject DENY al criterio S3.
  - Aggiungere un'operazione PutObject ALLOW al criterio S3.

L'impostazione di DeleteObject su DENY in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".

Anche quando vengono applicate tutte queste regole e policy, non proteggono dalle scritture simultanee (vedere Situazione A). Proteggono dalle sovrascritture sequenziali completate (vedere Situazione B).

**Situazione A**: Scritture simultanee (non protette)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

**Situazione B**: Sovrascritture sequenziali completate (protette contro)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

**Informazioni correlate**

- "Come le regole StorageGRID ILM gestiscono gli oggetti"
- "Criteri di esempio per i bucket"
- "Criteri di gruppo di esempio"
- "Gestire gli oggetti con ILM"
- "Utilizzare un account tenant"

## Criteri di esempio per i bucket

Utilizzare gli esempi in questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri dei bucket specificano le autorizzazioni di accesso per il bucket a cui è associato il criterio. È possibile configurare un criterio bucket utilizzando l'API S3 PutBucketPolicy tramite uno di questi strumenti:

- "Responsabile degli inquilini" .
- AWS CLI utilizzando questo comando (fare riferimento a"Operazioni sui bucket" ):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

**Esempio: consentire a tutti l'accesso in sola lettura a un bucket**

In questo esempio, a tutti, incluso l'utente anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni saranno negate. Si noti che questa policy potrebbe non essere particolarmente utile perché nessuno, eccetto l'account root, ha i permessi per

scrivere nel bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

**Esempio: consentire a tutti gli utenti di un account l'accesso completo e a tutti gli utenti di un altro account l'accesso in sola lettura a un bucket**

In questo esempio, a tutti gli utenti di un account specificato è consentito l'accesso completo a un bucket, mentre a tutti gli utenti di un altro account specificato è consentito solo di elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket a partire da `shared/` prefisso della chiave dell'oggetto.

> In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. A questi oggetti si applica la policy bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

**Esempio: consentire a tutti l'accesso in sola lettura a un bucket e l'accesso completo al gruppo specificato**

In questo esempio, a tutti, incluso l'utente anonimo, è consentito elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti al gruppo `Marketing` nell'account specificato è consentito l'accesso completo.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

**Esempio: consentire a tutti l'accesso in lettura e scrittura a un bucket se il client è nell'intervallo IP**

In questo esempio, a tutti, compresi gli utenti anonimi, è consentito elencare il bucket ed eseguire qualsiasi operazione sugli oggetti su tutti gli oggetti nel bucket, a condizione che le richieste provengano da un intervallo IP specificato (da 54.240.143.0 a 54.240.143.255, eccetto 54.240.143.188). Tutte le altre operazioni verranno negate e tutte le richieste al di fuori dell'intervallo IP verranno negate.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

**Esempio: consentire l'accesso completo a un bucket esclusivamente a un utente federato specificato**

In questo esempio, all'utente federato Alex è consentito l'accesso completo a `examplebucket` secchio e i suoi oggetti. A tutti gli altri utenti, compreso 'root', viene esplicitamente negata qualsiasi operazione. Si noti tuttavia che a 'root' non vengono mai negati i permessi per Put/Get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

**Esempio: autorizzazione PutOverwriteObject**

In questo esempio, il `Deny` L'effetto di PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging dell'oggetto S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

## Criteri di gruppo di esempio

Utilizzare gli esempi in questa sezione per creare criteri di accesso StorageGRID per i gruppi.

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non c'è `Principal` elemento nella politica perché è implicito. I criteri di gruppo vengono configurati tramite Tenant Manager o API.

### Esempio: impostare i criteri di gruppo utilizzando Tenant Manager

Quando aggiungi o modifichi un gruppo in Tenant Manager, puoi selezionare un criterio di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedere "Creare gruppi per un tenant S3" .

- **Nessun accesso S3**: opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non venga concesso tramite un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
- **Accesso di sola lettura**: gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi modificare questa stringa.
- **Accesso completo**: gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo con accesso completo. Non puoi modificare questa stringa.
- **Mitigazione del ransomware**: questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare definitivamente gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti.

  Gli utenti Tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono ignorare questo criterio di gruppo. Limitare l'autorizzazione Gestisci tutti i bucket agli utenti attendibili e utilizzare l'autenticazione a più fattori (MFA) laddove disponibile.

- **Personalizzato**: agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

### Esempio: consentire al gruppo l'accesso completo a tutti i bucket

In questo esempio, a tutti i membri del gruppo è consentito l'accesso completo a tutti i bucket di proprietà dell'account tenant, a meno che non venga esplicitamente negato dalla policy del bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

### Esempio: consentire al gruppo l'accesso in sola lettura a tutti i bucket

In questo esempio, tutti i membri del gruppo hanno accesso in sola lettura alle risorse S3, a meno che non venga esplicitamente negato dai criteri del bucket. Ad esempio, gli utenti di questo gruppo possono elencare oggetti e leggere dati, metadati e tag degli oggetti.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

**Esempio: consentire ai membri del gruppo l'accesso completo solo alla loro "cartella" in un bucket**

In questo esempio, ai membri del gruppo è consentito solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Si noti che quando si determina la privacy di queste cartelle, è necessario prendere in considerazione le autorizzazioni di accesso provenienti da altri criteri di gruppo e dai criteri del bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

# Operazioni S3 tracciate nei registri di controllo

I messaggi di controllo vengono generati dai servizi StorageGRID e archiviati in file di registro di testo. È possibile esaminare i messaggi di controllo specifici di S3 nel registro di controllo per ottenere dettagli sulle operazioni di bucket e oggetti.

## Operazioni del bucket monitorate nei log di controllo

- CreaBucket
- EliminaBucket
- DeleteBucketTagging
- EliminaOggetti
- OttieniBucketTagging
- HeadBucket
- ElencoOggetti
- ListObjectVersions
- Conformità del bucket PUT
- PutBucketTagging
- PutBucketVersioning

## Operazioni sugli oggetti tracciate nei registri di controllo

- Caricamento multiparte completo
- CopiaOggetto
- EliminaOggetto
- OttieniOggetto
- HeadObject
- MettiOggetto
- Ripristina oggetto
- SelezionaOggetto
- UploadPart (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)
- UploadPartCopy (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)

**Informazioni correlate**

- "Accedi al file di registro di controllo"
- "Il cliente scrive messaggi di audit"
- "Il cliente ha letto i messaggi di controllo"