



# UTILIZZARE L'API REST S3

StorageGRID 11.7

NetApp  
April 12, 2024

# Sommario

- UTILIZZARE L'API REST S3 ..... 1
  - Versioni e aggiornamenti supportati dall'API REST S3 ..... 1
  - Riferimento rapido: Richieste API S3 supportate ..... 3
  - Configurare gli account e le connessioni del tenant ..... 22
  - Supporto per i servizi della piattaforma StorageGRID ..... 26
  - Come StorageGRID implementa l'API REST S3 ..... 27
  - Supporto per Amazon S3 REST API ..... 44
  - Richieste StorageGRID S3 ..... 94
  - Policy di accesso a bucket e gruppi ..... 115
  - Configurare la sicurezza per l'API REST ..... 141
  - Monitorare e controllare le operazioni ..... 143
  - Vantaggi delle connessioni HTTP attive, inattive e simultanee ..... 146

# UTILIZZARE L'API REST S3

## Versioni e aggiornamenti supportati dall'API REST S3

StorageGRID supporta l'API S3 (Simple Storage Service), implementata come 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 lo storage a oggetti on-premise che utilizza il sistema StorageGRID. Sono necessarie modifiche minime all'utilizzo corrente delle chiamate API REST S3 da parte di un'applicazione client.

### Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di S3 e HTTP.

Elemento	Versione
Specifica S3	<i>Riferimento API Simple Storage Service 2006-03-01</i>
HTTP	1.1  Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35).  <b>Nota:</b> StorageGRID non supporta la pipelining HTTP/1.1.

### Informazioni correlate

["IETF RFC 2616: Protocollo di trasferimento ipertestuale \(HTTP/1.1\)"](#)

["Documentazione Amazon Web Services \(AWS\): Riferimento API Amazon Simple Storage Service"](#)

### Aggiornamenti al supporto delle API REST S3

Rilasciare	Commenti
11.7	<ul style="list-style-type: none"><li>• Aggiunto <a href="#">"Riferimento rapido: Richieste API S3 supportate"</a>.</li><li>• Aggiunto supporto per l'utilizzo della modalità DI GOVERNANCE con S3 Object Lock.</li><li>• Aggiunto supporto per StorageGRID specifico <code>x-ntap-sg-cgr-replication-status</code> Intestazione di risposta per le richieste DI oggetti GET e HEAD. Questa intestazione fornisce lo stato di replica di un oggetto per la replica cross-grid.</li><li>• Le richieste <code>SelectObjectContent</code> ora supportano gli oggetti Parquet.</li></ul>

Rilasciare	Commenti
11.6	<ul style="list-style-type: none"> <li>• Aggiunto supporto per l'utilizzo di <code>partNumber</code> Parametro di richiesta in GET object e HEAD object requests.</li> <li>• Aggiunto supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock.</li> <li>• Aggiunto supporto per <code>s3:object-lock-remaining-retention-days</code> policy condition key (chiave condizione policy) per impostare l'intervallo di periodi di conservazione consentiti per gli oggetti.</li> <li>• Modifica della dimensione massima <i>consigliata</i> per un'operazione di singolo oggetto PUT in 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.</li> </ul>
11.5	<ul style="list-style-type: none"> <li>• Aggiunto supporto per la gestione della crittografia bucket.</li> <li>• Aggiunto supporto per S3 Object Lock e richieste legacy di Compliance obsolete.</li> <li>• Aggiunto il supporto per l'utilizzo DELL'ELIMINAZIONE di più oggetti nei bucket con versione.</li> <li>• Il <code>Content-MD5</code> l'intestazione della richiesta è ora supportata correttamente.</li> </ul>
11.4	<ul style="list-style-type: none"> <li>• Aggiunto supporto per L'ELIMINAZIONE di tag bucket, L'AGGIUNTA DI tag bucket E L'AGGIUNTA di tag bucket. I tag di allocazione dei costi non sono supportati.</li> <li>• Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance.</li> <li>• Aggiunto supporto per le notifiche bucket su <code>s3:ObjectRestore:Post</code> tipo di evento.</li> <li>• I limiti di dimensione AWS per le parti multipart vengono ora applicati. Ogni parte di un caricamento multiparte deve essere compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB.</li> <li>• Aggiunto supporto per TLS 1.3</li> </ul>
11.3	<ul style="list-style-type: none"> <li>• Aggiunto supporto per la crittografia lato server dei dati a oggetti con chiavi fornite dal cliente (SSE-C).</li> <li>• Supporto aggiunto per LE operazioni DI eliminazione, GET e PUT del ciclo di vita del bucket (solo azione di scadenza) e per <code>x-amz-expiration</code> intestazione della risposta.</li> <li>• Aggiornamento DI PUT object, PUT object - Copy e Multipart Upload per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione.</li> <li>• Le crittografia TLS 1.1 non sono più supportate.</li> </ul>

Rilasciare	Commenti
11.2	<p>Aggiunto supporto per il ripristino POST-oggetto da utilizzare con i Cloud Storage Pools. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione dei criteri e variabili dei criteri in policy di gruppo e bucket. Le policy di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID continueranno a essere supportate.</p> <p><b>Nota:</b> gli utilizzi di ARN/URN in altre configurazioni JSON/XML, inclusi quelli utilizzati nelle funzionalità personalizzate di StorageGRID, non sono cambiati.</p>
11.1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per connessioni client S3 ai nodi di rete e impostazioni di conformità sui bucket.
11.0	Supporto aggiunto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. Inoltre, è stato aggiunto il supporto per i vincoli di posizione per il tag degli oggetti per i bucket e l'impostazione di controllo della coerenza disponibile.
10.4	Aggiunto supporto per le modifiche di scansione ILM alle versioni, agli aggiornamenti delle pagine dei nomi di dominio degli endpoint, alle condizioni e alle variabili nei criteri, agli esempi di policy e all'autorizzazione PutOverwriteObject.
10.3	Aggiunto supporto per il controllo delle versioni.
10.2	Aggiunto supporto per policy di accesso di gruppo e bucket e per copia multiparte (carica parte - Copia).
10.1	Aggiunto supporto per upload multiparte, richieste virtuali in stile host e autenticazione v4.
10.0	Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID. La versione attualmente supportata del <i>riferimento API del servizio di storage semplice</i> è 2006-03-01.

## Riferimento rapido: Richieste API S3 supportate

In questa pagina viene riepilogato 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 relativa a ciascuna operazione, selezionare il collegamento nell'intestazione.

### Parametri di query URI comuni e intestazioni di richiesta

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

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

Se non 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 sull'implementazione dell'API REST S3"](#)
- ["Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"](#)

## "AbortMultipartUpload"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) Per questa richiesta, più questo parametro di query URI aggiuntivo:

- uploadId

#### Corpo della richiesta

Nessuno

#### Documentazione StorageGRID

["Operazioni per caricamenti multiparte"](#)

## "CompleteMultipartUpload"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) Per questa richiesta, più questo parametro di query URI aggiuntivo:

- uploadId

#### Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- CompleteMultipartUpload
- Part
- ETag
- PartNumber

## Documentazione StorageGRID

["Caricamento multiparte completo"](#)

## "Oggetto CopyObject"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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

["PUT Object-Copy \(COPIA oggetto\)"](#)

## "CreateBucket"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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"](#)

## "CreateMultipartUpload"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più queste intestazioni aggiuntive:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- 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

["Avvia caricamento multiparte"](#)



## "DeleteBucket"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "DeleteBucketCors"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

## "DeleteBucketPolicy"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

#### Corpo della richiesta

Nessuno

## Documentazione StorageGRID

["Operazioni sui bucket"](#)

### "DeleteObject (Elimina oggetto)"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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"](#)

### "DeleteObjects"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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" (ELIMINA più oggetti)

### "DeleteObjectTagging"

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

#### Corpo della richiesta

Nessuno

## Documentazione StorageGRID

"Operazioni sugli oggetti"

### "GetBucketAcl"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

#### Corpo della richiesta

Nessuno

## Documentazione StorageGRID

"Operazioni sui bucket"

### "GetBucketEncryption"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

- ["Operazioni sui bucket"](#) (OTTIENI ciclo di vita del bucket)
- ["Creare la configurazione del ciclo di vita S3"](#)

## "GetBucketLocation"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "GetBucketNotificationConfiguration"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Operazioni sui bucket"](#) (OTTIENI notifica bucket)

## "GetBucketPolicy"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "GetBucketReplication"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "GetBucketTagging"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "GetObject"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) Per questa richiesta, più i seguenti parametri di query URI aggiuntivi:

- `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**

["OTTIENI oggetto"](#)

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

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

["Operazioni sugli oggetti"](#)

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

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

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

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

**Corpo della richiesta**

Nessuno

**Documentazione StorageGRID**

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

## "GetObjectRetention"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

## "GetObjectTagging"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "HeadObject (oggetto intestazione)"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più queste intestazioni aggiuntive:

- 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

["Oggetto TESTA"](#)

## "ListBucket"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

[Operazioni sul servizio](#) > [ASSISTENZA](#)

## "ListMultipartUploads"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

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

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Elenca caricamenti multiparte"](#)

## "ListObjects (oggetti elenco)"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- delimiter
- encoding-type
- marker
- max-keys



- `prefix`

#### Corpo della richiesta

Nessuno

#### Documentazione StorageGRID

["Operazioni sui bucket"](#) (OTTIENI bucket)

### "ListObjectsV2"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

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

#### Corpo della richiesta

Nessuno

#### Documentazione StorageGRID

["Operazioni sui bucket"](#) (OTTIENI bucket)

### "ListObjectVersions"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

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

#### Corpo della richiesta

Nessuno

#### Documentazione StorageGRID

["Operazioni sui bucket"](#) (OTTIENI versioni oggetto bucket)

## "ListParts"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- max-parts
- part-number-marker
- uploadId

### Corpo della richiesta

Nessuno

### Documentazione StorageGRID

["Elenca caricamenti multiparte"](#)

## "PutBucketCors"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- ServerSideEncryptionConfiguration
- Rule
- ApplyServerSideEncryptionByDefault
- SSEAlgorithm

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "PutBucketLifecycleConfiguration"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- NewerNoncurrentVersions
- LifecycleConfiguration
- Rule
- Expiration
- Days
- Filter
- And
- Prefix
- Tag
- Key
- Value
- Prefix
- Tag
- Key
- Value
- ID
- NoncurrentVersionExpiration
- NoncurrentDays
- Prefix
- Status

### Documentazione StorageGRID

- ["Operazioni sui bucket"](#) (CICLO di vita DEL bucket PUT)
- ["Creare la configurazione del ciclo di vita S3"](#)

## "PutBucketNotificationConfiguration"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

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

## Documentazione StorageGRID

["Operazioni sui bucket"](#) (METTI notifica bucket)

### "PutBucketPolicy"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

#### Corpo della richiesta

Per ulteriori informazioni sui campi corpo JSON supportati, vedere ["Utilizza policy di accesso a bucket e gruppi"](#).

### "PutBucketReplication"

#### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

#### Tag XML del corpo della richiesta

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

## Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "PutBucketTagging"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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 tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Parametri del corpo della richiesta

StorageGRID supporta questi parametri del corpo della richiesta:

- VersioningConfiguration
- Status

### Documentazione StorageGRID

["Operazioni sui bucket"](#)

## "PutObject"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, più queste intestazioni aggiuntive:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- 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**

["METTI oggetto"](#)

### **"PutObjectLegalHold"**

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

StorageGRID supporta tutti [parametri 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 il blocco oggetti S3"](#)

### **"PutObjectLockConfiguration"**

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

StorageGRID supporta tutti [parametri 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 il blocco oggetti S3"](#)

### **"PutObjectRetention"**

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

StorageGRID supporta tutti [parametri 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 il blocco oggetti S3"](#)

## "PutObjectTagging"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri 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"](#)

## "SelectObjectContent"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

### Corpo della richiesta

Per ulteriori informazioni sui body field supportati, vedere quanto segue:

- ["USA S3 Select"](#)
- ["Selezionare contenuto oggetto"](#)

## "UploadPart"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) Per questa richiesta, più i seguenti parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `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

["Carica parte"](#)

## "UploadPartCopy"

### Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) Per questa richiesta, più i seguenti 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

["Carica parte - Copia"](#)

## Configurare gli account e le connessioni del tenant

La configurazione di StorageGRID per accettare connessioni da applicazioni client richiede la creazione di uno o più account tenant e la configurazione delle connessioni.

### Creare e configurare account tenant S3

È necessario un account tenant S3 prima che i client API S3 possano memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, gruppi, utenti, bucket e oggetti.

Gli account del tenant S3 vengono creati da un amministratore del grid StorageGRID utilizzando l'API Gestione griglia o Gestione griglia. Vedere ["Gestire i tenant"](#) per ulteriori informazioni. Dopo la creazione di un account tenant S3, gli utenti tenant possono accedere a tenant Manager per gestire gruppi, utenti, chiavi di accesso e bucket. Vedere ["Utilizzare un account tenant"](#) per ulteriori informazioni.



Mentre gli utenti del tenant S3 possono creare e gestire chiavi di accesso S3 e bucket con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Vedere ["UTILIZZARE L'API REST S3"](#) per ulteriori informazioni.



## Come configurare le connessioni client

Un amministratore di grid effettua scelte di configurazione che influiscono sul modo in cui i client S3 si connettono a StorageGRID per memorizzare e recuperare i dati. Esistono quattro passaggi fondamentali per collegare StorageGRID a qualsiasi applicazione S3:

- Eseguire attività preliminari in StorageGRID, in base al modo in cui l'applicazione client si conetterà a StorageGRID.
- Utilizzare StorageGRID per ottenere i valori necessari all'applicazione per connettersi alla griglia. È possibile farlo ["Utilizzare l'installazione guidata S3"](#) Oppure configurare manualmente ogni entità StorageGRID.
- Utilizzare l'applicazione S3 per completare la connessione a StorageGRID. Creare voci DNS per associare gli indirizzi IP ai nomi di dominio che si intende utilizzare.
- Eseguire attività in corso nell'applicazione e in StorageGRID per gestire e monitorare lo storage a oggetti nel tempo.

Per ulteriori informazioni su questi passaggi, vedere ["Configurare le connessioni client"](#).

### Informazioni richieste per le connessioni client

Per memorizzare o recuperare oggetti, le applicazioni client S3 si connettono al servizio Load Balancer, incluso in tutti i nodi Admin e Gateway, o al servizio Local Distribution Router (LDR), incluso in tutti i nodi Storage.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta del servizio su tale nodo. Facoltativamente, è possibile creare gruppi ad alta disponibilità (ha) di nodi di bilanciamento del carico per fornire connessioni ad alta disponibilità che utilizzano indirizzi IP virtuali (VIP). Se si desidera connettersi a StorageGRID utilizzando un nome di dominio completo (FQDN) invece di un indirizzo IP o VIP, è possibile configurare le voci DNS.

Vedere ["Riepilogo: Indirizzi IP e porte per le connessioni client"](#) per ulteriori informazioni.

### Decidere di utilizzare connessioni HTTPS o HTTP

Quando le connessioni client vengono eseguite utilizzando un endpoint Load Balancer, le connessioni devono essere effettuate utilizzando il protocollo (HTTP o HTTPS) specificato per tale endpoint. Per utilizzare HTTP per le connessioni client ai nodi di storage, è necessario abilitarne l'utilizzo.

Per impostazione predefinita, quando le applicazioni client si connettono ai nodi di storage, devono utilizzare HTTPS crittografato per tutte le connessioni. In alternativa, è possibile attivare connessioni HTTP meno sicure selezionando **CONFIGURAZIONE > Impostazioni di sicurezza > rete e oggetti > attiva HTTP per connessioni nodo di storage** in Grid Manager. Ad esempio, un'applicazione client potrebbe utilizzare il protocollo HTTP quando si verifica la connessione a un nodo di storage in un ambiente non di produzione.



Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste e le risposte verranno inviate senza crittografia.

### Informazioni correlate

["Amministrare StorageGRID"](#)

["Vantaggi delle connessioni HTTP attive, inattive e simultanee"](#)

## Nomi di dominio degli endpoint S3 per le richieste S3

Prima di poter utilizzare i nomi di dominio degli endpoint S3 per le richieste dei client, un amministratore di StorageGRID deve configurare il sistema in modo che accetti le connessioni che utilizzano i nomi di dominio degli endpoint S3 nelle richieste in stile percorso S3 e in stile host virtuale S3.

### A proposito di questa attività

Per consentire l'utilizzo delle richieste di stile in hosting virtuale S3, un amministratore di grid deve eseguire le seguenti attività:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il certificato utilizzato dal client per le connessioni HTTPS a StorageGRID sia firmato per tutti i nomi di dominio richiesti dal client.

Ad esempio, se l'endpoint del dominio dell'endpoint del servizio API S3 è `s3.company.com`, l'amministratore della griglia deve assicurarsi che il certificato utilizzato per le connessioni HTTPS abbia `s3.company.com` Come nome comune del soggetto e nei nomi alternativi del soggetto, e.  
`*.s3.company.com` Nei nomi alternativi del soggetto.

- **"Configurare il server DNS"** Utilizzato dal client per includere record DNS che corrispondono ai nomi di dominio degli endpoint S3, inclusi i record con caratteri jolly richiesti.

Se il client si connette utilizzando il servizio Load Balancer, il certificato configurato dall'amministratore della griglia è il certificato per l'endpoint del bilanciamento del carico utilizzato dal client.



Ogni endpoint di bilanciamento del carico dispone di un proprio certificato e ciascun endpoint può essere configurato in modo da riconoscere nomi di dominio degli endpoint S3 diversi.

Se il client si connette ai nodi di storage, il certificato configurato dall'amministratore della griglia è il singolo certificato server personalizzato utilizzato per la griglia.

Consultare le istruzioni per **"Amministrazione di StorageGRID"** per ulteriori informazioni.

Una volta completate queste fasi, è possibile utilizzare richieste virtuali in stile host.

## Verificare la configurazione dell'API REST S3

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

### Prima di iniziare

- È stata scaricata e installata la CLI AWS dal sito ["aws.amazon.com/cli"](https://aws.amazon.com/cli).
- Hai creato un account tenant S3 nel sistema StorageGRID.
- È stata creata una chiave di accesso nell'account tenant.

### Fasi

1. Configurare le impostazioni dell'interfaccia utente di AWS per utilizzare l'account creato nel sistema StorageGRID:
  - a. Accedere alla modalità di configurazione: `aws configure`
  - b. Inserire l'ID della chiave di accesso per l'account creato.

- c. Inserire la chiave di accesso segreta per l'account creato.
- d. Immettere 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. Creare un bucket.

In questo esempio si presuppone che sia stato configurato un endpoint del bilanciamento 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. Caricare 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 che rappresenta un hash dei dati dell'oggetto.

## 4. Elencare i contenuti 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. Eliminare l'oggetto.

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

## 6. Eliminare il bucket.

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

# Supporto per i servizi della piattaforma StorageGRID

I servizi della piattaforma StorageGRID consentono agli account tenant StorageGRID di sfruttare servizi esterni come un bucket S3 remoto, un endpoint SNS (Simple Notification Service) o un cluster Elasticsearch per estendere i servizi forniti da un grid.

Nella tabella seguente sono riepilogati i servizi della piattaforma disponibili e le API S3 utilizzate per configurarli.

Servizio di piattaforma	Scopo	S3 API utilizzata per configurare il servizio
Replica di CloudMirror	Replica gli oggetti da un bucket StorageGRID di origine al bucket S3 remoto configurato.	METTI la replica del bucket (vedere <a href="#">"Operazioni sui bucket"</a> )
Notifiche	Invia notifiche sugli eventi in un bucket StorageGRID di origine a un endpoint configurato per il servizio di notifica semplice (SNS).	NOTIFICA DEL bucket (vedere <a href="#">"Operazioni sui bucket"</a> )
Integrazione della ricerca	Invia i metadati degli oggetti memorizzati in un bucket StorageGRID a un indice Elasticsearch configurato.	<a href="#">"INSERIRE la configurazione della notifica dei metadati del bucket"</a>  <b>Nota:</b> questa è un'API S3 personalizzata di StorageGRID.

Un amministratore di grid deve abilitare l'utilizzo dei servizi della piattaforma per un account tenant prima di poter essere utilizzato. Vedere ["Amministrare StorageGRID"](#). Quindi, un amministratore del tenant deve creare un endpoint che rappresenti il servizio remoto nell'account tenant. Questa fase è necessaria prima di poter configurare un servizio. Vedere ["Utilizzare un account tenant"](#).

## Consigli per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, è necessario conoscere i seguenti consigli:

- NetApp consiglia di non consentire più di 100 tenant attivi con richieste S3 che richiedono la replica CloudMirror, le notifiche e l'integrazione della ricerca. La presenza di più di 100 tenant attivi può rallentare le performance del client S3.
- Se un bucket S3 nel sistema StorageGRID ha attivato sia la versione che la replica CloudMirror, NetApp consiglia di abilitare anche il controllo delle versioni del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica di CloudMirror di generare versioni di oggetti simili sull'endpoint.
- La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.
- La replica di CloudMirror non riesce e viene visualizzato un errore AccessDenied se nel bucket di destinazione è attivata la conformità legacy.

# Come StorageGRID implementa l'API REST S3

## Richieste client in conflitto

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite".

La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

## Controlli di coerenza

I controlli di coerenza forniscono un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage, come richiesto dall'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET che segue UN PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

Se si desidera eseguire operazioni a oggetti a un livello di coerenza diverso, è possibile specificare un controllo di coerenza per ciascun bucket o per ciascuna operazione API.

### Controlli di coerenza

Il controllo della coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tenere traccia degli oggetti vengono distribuiti tra i nodi e, di conseguenza, sulla disponibilità degli oggetti per le richieste dei client.

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

- **All:** Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non avrà esito positivo.
- **Strong-Global:** Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Site:** Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write:** (Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available:** Fornisce una 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 raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

### Utilizzare i controlli di coerenza "read-after-new-write" e "available"

Quando un'operazione HEAD o GET utilizza il controllo di 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 non riesce, ripete la ricerca al livello di coerenza successivo fino a raggiungere un livello di coerenza equivalente al comportamento per un livello globale-forte.

Se un'operazione HEAD o GET utilizza il controllo di coerenza "read-after-new-write" ma l'oggetto non esiste, la ricerca dell'oggetto raggiungerà sempre un livello di coerenza equivalente al comportamento per strong-Global. Poiché questo livello di coerenza richiede la disponibilità di più copie dei metadati dell'oggetto in ciascun sito, è possibile ricevere un numero elevato di errori 500 interni del server se due o più nodi di storage nello stesso sito non sono disponibili.

A meno che non necessiti di garanzie di coerenza simili a Amazon S3, puoi evitare questi errori per LE operazioni HEAD and GET impostando il controllo di coerenza su "Available". Quando un'operazione HEAD o GET utilizza il controllo di coerenza "Available", StorageGRID fornisce solo la coerenza finale. Non riprova un'operazione non riuscita a livelli di coerenza crescenti, quindi non richiede la disponibilità di più copie dei metadati dell'oggetto.

### Specificare il controllo di coerenza per il funzionamento API

Per impostare il controllo di coerenza per una singola operazione API, i controlli di coerenza devono essere supportati per l'operazione e occorre specificare il controllo di coerenza nell'intestazione della richiesta. Questo esempio imposta il controllo di coerenza su "strong-site" per un'operazione GET Object.

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



È necessario utilizzare lo stesso controllo di coerenza per le operazioni PUT object e GET object.

### Specificare il controllo di coerenza per il bucket

Per impostare il controllo di coerenza per il bucket, è possibile utilizzare la richiesta di coerenza PUT bucket StorageGRID e LA richiesta di coerenza GET bucket. In alternativa, puoi utilizzare l'API di gestione tenant o tenant Manager.

Quando si impostano i controlli di coerenza per un bucket, tenere presente quanto segue:

- L'impostazione del controllo di coerenza per un bucket determina quale controllo di coerenza viene utilizzato per le operazioni S3 eseguite sugli oggetti nel bucket o sulla configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- Il controllo di coerenza per una singola operazione API sovrascrive il controllo di coerenza per il bucket.
- In generale, i bucket devono utilizzare il controllo di coerenza predefinito, "read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare il controllo di coerenza per ogni richiesta API. Impostare il controllo di coerenza a livello di bucket solo come ultima risorsa.

### come interagiscono i controlli di coerenza e le regole ILM per influire sulla protezione dei dati

La scelta del controllo di coerenza e la regola ILM influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il controllo di coerenza utilizzato quando un oggetto viene memorizzato 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 che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Doppio commit:** StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Strict:** Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.
- **Balanced:** StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.



Prima di selezionare il comportamento di acquisizione per una regola ILM, leggere la descrizione completa di queste impostazioni nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

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

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di coerenza:

- **ILM rule:** Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **Livello di 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 degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece sono state utilizzate la stessa regola ILM e il livello di coerenza "strong-site", il client potrebbe ricevere un messaggio di successo dopo la replica dei dati dell'oggetto nel sito remoto, ma prima della distribuzione dei metadati dell'oggetto. 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 poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interconnessione tra i livelli di coerenza e le regole ILM può essere complessa. Contattare NetApp per assistenza.

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["COERENZA del bucket"](#)

["METTI la coerenza del bucket"](#)

## Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID

L'amministratore del grid crea regole ILM (Information Lifecycle Management) per gestire i dati degli oggetti acquisiti nel sistema StorageGRID dalle applicazioni client API REST S3. Queste regole vengono quindi aggiunte al criterio ILM per determinare come e dove i dati degli oggetti vengono memorizzati nel tempo.

Le impostazioni ILM determinano i seguenti aspetti di un oggetto:

- **Geografia**

La posizione dei dati di un oggetto, all'interno del sistema StorageGRID (pool di storage) o in un pool di storage cloud.

- **Grado di storage**

Il tipo di storage utilizzato per memorizzare i dati dell'oggetto, ad esempio flash o disco rotante.

- **Protezione contro le perdite**

Quante copie vengono eseguite e i tipi di copie create: Replica, erasure coding o entrambe.

- **Conservazione**

Il cambia nel tempo in base alla modalità di gestione dei dati di un oggetto, alla posizione in cui sono memorizzati e al modo in cui sono protetti dalla perdita.

- **Protezione durante l'acquisizione**

Metodo utilizzato per proteggere i dati degli oggetti durante l'acquisizione: Posizionamento sincrono (utilizzando le opzioni bilanciate o rigide per il comportamento di Ingest) o creazione di copie intermedie (utilizzando l'opzione Dual Commit).

Le regole ILM possono filtrare e selezionare gli oggetti. Per gli oggetti acquisiti tramite S3, le regole ILM possono filtrare gli oggetti in base ai seguenti metadati:

- Account tenant
- Nome bucket
- Tempo di acquisizione
- Chiave
- Ora dell'ultimo accesso



Per impostazione predefinita, gli aggiornamenti dell'ultimo tempo di accesso sono disattivati per tutti i bucket S3. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione ultimo tempo di accesso, è necessario abilitare gli aggiornamenti per l'ultimo tempo di accesso per i bucket S3 specificati in tale regola. Utilizza LA richiesta PUT bucket Last access time, il tenant manager (vedere ["Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso"](#)) O l'API di gestione tenant. Quando si abilitano gli ultimi aggiornamenti del tempo di accesso, tenere presente che le prestazioni di StorageGRID potrebbero essere ridotte, soprattutto nei sistemi con oggetti di piccole dimensioni.



- Vincolo di posizione
- Dimensione dell'oggetto
- Metadati dell'utente
- Tag oggetto

### Informazioni correlate

["Utilizzare un account tenant"](#)

["Gestire gli oggetti con ILM"](#)

["TEMPO ULTIMO accesso bucket"](#)

## Versione degli oggetti

È possibile utilizzare il controllo delle versioni per conservare più versioni di un oggetto, che protegge dall'eliminazione accidentale di oggetti e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con il supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 1,000 versioni di ciascun oggetto.

La versione degli oggetti può essere combinata con la gestione del ciclo di vita delle informazioni di StorageGRID (ILM) o con la configurazione del ciclo di vita del bucket S3. Per attivare questa funzionalità per il bucket, è necessario abilitare esplicitamente il controllo delle versioni per ciascun bucket. A ciascun oggetto del bucket viene assegnato un ID di versione, generato dal sistema StorageGRID.

L'utilizzo dell'autenticazione MFA (multi-factor Authentication) Delete non è supportato.



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

### ILM e versione

I criteri ILM vengono applicati a ogni versione di un oggetto. Un processo di scansione ILM esegue una scansione continua di tutti gli oggetti e li rivaluti in base al criterio ILM corrente. Qualsiasi modifica apportata ai criteri ILM viene applicata a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente ingerite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti acquisiti in precedenza.

Per gli oggetti S3 nei bucket abilitati per il controllo delle versioni, il supporto delle versioni consente di creare regole ILM che utilizzano "ora non corrente" come ora di riferimento (selezionare **Sì** per la domanda, "applicare questa regola solo alle versioni di oggetti precedenti?" poll ["Fase 1 della creazione guidata di una regola ILM"](#)). Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro "Noncurrent Time" consente di creare policy che riducono l'impatto sullo storage delle versioni precedenti degli oggetti.



Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, l'ora non corrente per la versione originale dell'oggetto si riflette quando il caricamento multiparte è stato creato per la nuova versione, non quando il caricamento multiparte è stato completato. In casi limitati, il tempo non corrente per la versione originale potrebbe essere di ore o giorni prima del tempo per la versione corrente.

Vedere ["Regole e criteri ILM per gli oggetti con versione S3 \(esempio 4\)"](#).

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

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato. È possibile specificare la conservazione predefinita per ogni bucket o impostazioni di conservazione per ciascuna versione dell'oggetto.

### Come attivare il blocco oggetti S3 per un bucket

Se l'impostazione globale di blocco oggetti S3 è attivata per il sistema StorageGRID, è possibile attivare il blocco oggetti S3 quando si crea ciascun bucket.

S3 Object Lock è un'impostazione permanente che può essere attivata solo quando si crea un bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

Per attivare il blocco oggetti S3 per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager. Vedere ["Creare un bucket S3"](#).
- Creare il bucket utilizzando una richiesta PUT bucket con `x-amz-bucket-object-lock-enabled` intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando viene creato il bucket. Non puoi sospendere il controllo delle versioni per il bucket. Vedere ["Versione degli oggetti"](#).

### Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è attivato per un bucket, è possibile attivare 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 COMPLIANCE:
  - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
  - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità GOVERNANCE:
  - Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione.
  - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

#### 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:

- Gestire le impostazioni del bucket da Tenant Manager. Vedere ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).
- Inviare una richiesta DI configurazione PUT Object Lock per il bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

### PUT Object Lock Configuration (CONFIGURAZIONE blocco oggetto)

La richiesta PUT Object Lock Configuration consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket con S3 Object Lock attivato. È inoltre possibile rimuovere le impostazioni di conservazione predefinite precedentemente configurate.

Quando le nuove versioni degli 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 il periodo di conservazione fino alla data se `x-amz-object-lock-retain-until-date` non specificato.

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

È necessario disporre di `s3:PutBucketObjectLockConfiguration` autorizzazione, o essere root dell'account, per completare questa operazione.

Il `Content-MD5` L'intestazione della richiesta deve essere specificata nella richiesta PUT.

### Esempio di richiesta

Questo esempio attiva il blocco oggetti S3 per un bucket e imposta la modalità di conservazione predefinita su COMPLIANCE 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 attivato per un bucket e per visualizzare la modalità di conservazione e il periodo di conservazione predefiniti, utilizzare uno dei seguenti metodi:

- Visualizza il bucket nel tenant manager. Vedere ["Visualizza i bucket S3"](#).
- Eseguire una richiesta GET Object Lock Configuration.

### OTTIENI configurazione blocco oggetto

La richiesta GET Object Lock Configuration (OTTIENI configurazione blocco oggetto) consente di determinare se S3 Object Lock (blocco oggetto S3) è attivato per un bucket e, se è attivato, di verificare se sono configurate una modalità di conservazione predefinita e un periodo di conservazione per il bucket.

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

È necessario disporre di `s3:GetBucketObjectLockConfiguration` autorizzazione, o essere root dell'account, per completare questa operazione.

### Esempio di richiesta

```
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/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
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 le impostazioni di conservazione S3 Object Lock.

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

È possibile specificare le seguenti impostazioni per ciascun oggetto:

- **Modalità di conservazione:** CONFORMITÀ o GOVERNANCE.
- **Conserva-fino-data:** Una data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da StorageGRID.

- In modalità COMPLIANCE, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. È possibile aumentare la data di conservazione fino alla data prevista, ma non è possibile ridurla o rimuoverla.
- In modalità GOVERNANCE, gli utenti con autorizzazioni speciali possono ignorare l'impostazione di conservazione fino alla data odierna. Possono eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere il mantenimento fino ad oggi.

- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa.

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

Per specificare le impostazioni di blocco oggetti S3 quando si aggiunge una versione di oggetto a un bucket, eseguire un **"METTI oggetto"**, **"METTI oggetto - Copia"**, o **"Avvia caricamento multiparte"** richiesta.

È possibile utilizzare quanto segue:

- `x-amz-object-lock-mode`, Che può essere COMPLIANCE o GOVERNANCE (sensibile al maiuscolo/minuscolo).



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

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

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

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

- Il `Content-MD5` l'intestazione della richiesta è obbligatoria, se presente `x-amz-object-lock-*` L'intestazione della richiesta è presente nella richiesta DELL'oggetto PUT. `Content-MD5` Non è richiesto per METTERE oggetto - copiare o avviare caricamento multiparte.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` L'intestazione della richiesta è presente, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta DI oggetti PUT supporta l'utilizzo di `x-amz-storage-class: REDUCED_REDUNDANCY` Per far corrispondere il comportamento di AWS. Tuttavia, quando un oggetto viene acquisito in un bucket con il blocco oggetti S3 attivato, StorageGRID eseguirà sempre un ingest a doppio commit.

- Una risposta successiva ALLA versione DELL'oggetto GET o HEAD includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e. `x-amz-object-lock-legal-hold`, se configurato e se il mittente della richiesta ha il corretto `s3:Get*` permessi.

È possibile utilizzare `s3:object-lock-remaining-retention-days` chiave di condizione dei criteri per limitare i periodi di conservazione minimi e massimi consentiti per gli oggetti.

## Come aggiornare le impostazioni di conservazione per un oggetto

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

- `PUT Object legal-hold`

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

- `PUT Object retention`
  - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (distinzione tra maiuscole e minuscole).
  - Il valore di conservazione fino alla data deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
  - Se una versione a oggetti ha un valore di conservazione esistente fino alla data odierna, è possibile aumentarlo. Il nuovo valore deve essere in futuro.

## Come utilizzare LA modalità DI GOVERNANCE

Utenti che dispongono di `s3:BypassGovernanceRetention` L'autorizzazione può ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità DI GOVERNANCE. Tutte le operazioni DI eliminazione o CONSERVAZIONE degli oggetti PUT devono includere `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire queste operazioni aggiuntive:

- Eseguire operazioni DI ELIMINAZIONE di oggetti o DI ELIMINAZIONE di oggetti multipli per eliminare una versione di oggetti prima che sia trascorso il periodo di conservazione.

Non è possibile eliminare gli oggetti che si trovano sotto un blocco legale. La sospensione legale deve essere disattivata.

- Eseguire operazioni DI conservazione degli oggetti PUT 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 dalla CONFORMITÀ alla GOVERNANCE.

- Eseguire operazioni DI conservazione DEGLI oggetti PUT per aumentare, ridurre o rimuovere il periodo di conservazione di una versione dell'oggetto.

## Informazioni correlate

- ["Gestire gli oggetti con S3 Object Lock"](#)
- ["USA il blocco oggetti S3 per conservare gli oggetti"](#)

- ["Amazon Simple Storage Service User Guide \(Guida utente di Amazon Simple Storage Service\): Utilizzo di S3 Object Lock"](#)

## Creare la configurazione del ciclo di vita S3

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

Il semplice esempio di questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando alcuni oggetti vengono cancellati (scaduti) da specifici bucket S3. L'esempio in questa sezione è a solo scopo illustrativo. Per informazioni dettagliate sulla creazione di configurazioni del ciclo di vita S3, vedere ["Amazon Simple Storage Service Developer Guide: Gestione del ciclo di vita degli oggetti"](#). Nota: StorageGRID supporta solo le azioni di scadenza e non le azioni di transizione.

### Che cos'è la configurazione del ciclo di vita

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

StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:

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

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

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora applicabili all'oggetto. Oppure, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni di posizionamento ILM per l'oggetto. Per ulteriori informazioni, vedere ["Come ILM opera per tutta la vita di un oggetto"](#).



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

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

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



## Creare la configurazione del ciclo di vita

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

1. La regola 1 si applica solo agli oggetti che corrispondono al prefisso `category1/` e che hanno un `key2` valore di `tag2`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno alla mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2/`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno 100 giorni dopo l'acquisizione.



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

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

```

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

```

## Applica la configurazione del ciclo di vita al bucket

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

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

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

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

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

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

## Verificare 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 DI oggetto PUT, HEAD o GET. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata associata.



Poiché il ciclo di vita del bucket ha la priorità su ILM, il sistema `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere ["Come viene determinata la conservazione degli oggetti"](#).

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

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

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

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

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

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

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

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

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

Seguire questi consigli quando si implementa l'API REST S3 per l'utilizzo con StorageGRID.

### Raccomandazioni per la gestione di oggetti inesistenti

Se l'applicazione verifica regolarmente l'esistenza di un oggetto in un percorso in cui non si prevede l'effettiva esistenza dell'oggetto, utilizzare il controllo di coerenza "Available". Ad esempio, è necessario utilizzare il controllo di coerenza "Available" se l'applicazione dirige una posizione prima DI INSERIRVI.

In caso contrario, se l'operazione HEAD non trova l'oggetto, potrebbe essere visualizzato un numero elevato di errori 500 nel server interno se uno o più nodi di storage non sono disponibili.

È possibile impostare il controllo di coerenza "Available" per ciascun bucket utilizzando LA richiesta di coerenza PUT bucket oppure specificare il controllo di coerenza nell'intestazione della richiesta per una singola operazione API.

## Raccomandazioni per le chiavi a oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base alla prima volta che il bucket è stato creato.

### Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Utilizzare invece prefissi non casuali e non univoci, ad esempio `image`.
- Se si segue la precedente raccomandazione AWS per utilizzare caratteri casuali e univoci nei prefissi delle chiavi, inserire un prefisso tra le chiavi degli oggetti e il nome della directory. Ovvero, utilizzare 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 Best practice di performance. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.



Un'eccezione è rappresentata da un carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto delle performance per questo caso d'utilizzo, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa di simile alla data. Si supponga, ad esempio, che un client S3 scriva in genere 2,000 oggetti al secondo e che il criterio del ciclo di vita di ILM o bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto delle performance, è possibile assegnare un nome alle chiavi utilizzando un modello come questo:

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

## Raccomandazioni per "range reads"

Se il ["opzione globale per comprimere gli oggetti memorizzati"](#) È attivato, le applicazioni client S3 dovrebbero evitare di eseguire operazioni GET Object che specificano un intervallo di byte da restituire. Queste operazioni "range Read" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente 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 possono scadere.



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

### Informazioni correlate

- ["Controlli di coerenza"](#)
- ["METTI la coerenza del bucket"](#)
- ["Amministrare StorageGRID"](#)

# Supporto per Amazon S3 REST API

## Dettagli sull'implementazione dell'API REST S3

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

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

### Gestione della data

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

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

### Intestazioni di richiesta comuni

Il sistema StorageGRID supporta le intestazioni di richiesta comuni definite da ["Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"](#), con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per firma AWS versione 2  Supporto per firma AWS versione 4, con le seguenti eccezioni: <ul style="list-style-type: none"><li>Il valore SHA256 non viene calcolato per il corpo della richiesta. Il valore inviato dall'utente viene accettato senza convalida, come se il valore <code>UNSIGNED-PAYLOAD</code> è stato fornito per <code>x-amz-content-sha256</code> intestazione.</li></ul>
<code>x-amz-security-token</code>	Non implementato. Ritorno <code>XNotImplemented</code> .

### Intestazioni di risposta comuni

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

Intestazione della risposta	Implementazione
<code>x-amz-id-2</code>	Non utilizzato

## Autenticare le richieste

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

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

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

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

### Utilizzare l'intestazione autorizzazione HTTP

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

### Utilizzare i parametri di query

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

## Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

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

### Informazioni correlate

["OTTIENI l'utilizzo dello storage"](#)

## Operazioni sui bucket

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

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

Per ulteriori informazioni, vedere quanto segue:

- ["Documentazione di Amazon Web Services \(AWS\): Limitazioni e limitazioni del bucket"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

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

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

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

Operazione	Implementazione
ELIMINA bucket	Questa operazione elimina il bucket.
ELIMINA cors bucket	Questa operazione elimina la configurazione CORS per il bucket.
ELIMINA crittografia bucket	Questa operazione elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non vengono crittografati.
ELIMINA ciclo di vita bucket	Questa operazione elimina la configurazione del ciclo di vita dal bucket. Vedere <a href="#">"Creare la configurazione del ciclo di vita S3"</a> .
ELIMINA policy bucket	Questa operazione elimina la policy associata al bucket.
ELIMINA replica bucket	Questa operazione elimina la configurazione di replica collegata al bucket.
ELIMINA tag bucket	Questa operazione utilizza <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un bucket.



Operazione	Implementazione
OTTIENI bucket (ListObjects) (ListObjectsV2)	<p>Questa operazione restituisce alcuni o tutti (fino a 1,000) gli oggetti in un bucket. La classe Storage per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con REDUCED_REDUNDANCY opzione classe di storage:</p> <ul style="list-style-type: none"> <li>• STANDARD, Che indica che l'oggetto è memorizzato in un pool di storage costituito da nodi di storage.</li> <li>• GLACIER, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool.</li> </ul> <p>Se il bucket contiene un numero elevato di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune CommonPrefixes che non contengono chiavi.</p>
SCARICA le versioni degli oggetti bucket (ListObjectVersions)	Con l'accesso IN LETTURA su un bucket, questa operazione con versions la sottomisura elenca i metadati di tutte le versioni degli oggetti nel bucket.
OTTIENI acl bucket	Questa operazione restituisce una risposta positiva e l'ID, il DisplayName e il permesso del proprietario del bucket, indicando che il proprietario ha pieno accesso al bucket.
OTTIENI bucket cors	Questa operazione restituisce il cors configurazione per il bucket.
OTTIENI la crittografia bucket	Questa operazione restituisce la configurazione di crittografia predefinita per il bucket.
OTTIENI il ciclo di vita del bucket (GetBucketLifecycleConfiguration)	Questa operazione restituisce la configurazione del ciclo di vita del bucket. Vedere <a href="#">"Creare la configurazione del ciclo di vita S3"</a> .
OTTIENI posizione bucket	Questa operazione restituisce la regione impostata utilizzando LocationConstraint Elemento nella richiesta PUT bucket. Se l'area del bucket è us-east-1, viene restituita una stringa vuota per la regione.
OTTIENI notifica bucket (GetBucketNotificationConfiguration)	Questa operazione restituisce la configurazione di notifica allegata al bucket.
OTTIENI la policy bucket	Questa operazione restituisce la policy allegata al bucket.
OTTIENI la replica bucket	Questa operazione restituisce la configurazione di replica collegata al bucket.

Operazione	Implementazione
OTTIENI il contrassegno bucket	Questa operazione utilizza <code>tagging</code> sottorisorsa per restituire tutti i tag per un bucket.
SCARICA la versione di bucket	<p>Questa implementazione utilizza <code>versioning</code> sottorisorsa per restituire lo stato di versione di un bucket.</p> <ul style="list-style-type: none"> <li>• <i>Blank</i>: Il controllo delle versioni non è mai stato abilitato (bucket "Unversioned")</li> <li>• <i>Enabled</i> (attivato): Il controllo delle versioni è attivato</li> <li>• <i>Suspended</i> (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso</li> </ul>
OTTIENI configurazione blocco oggetto	<p>Questa operazione restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurato.</p> <p>Vedere <a href="#">"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"</a>.</p>
BENNA PER LA TESTA	<p>Questa operazione determina se esiste un bucket e se si dispone dell'autorizzazione per accedervi.</p> <p>Questa operazione restituisce:</p> <ul style="list-style-type: none"> <li>• <code>x-ntap-sg-bucket-id</code>: UUID del bucket in formato UUID.</li> <li>• <code>x-ntap-sg-trace-id</code>: L'ID di traccia univoco della richiesta associata.</li> </ul>

Operazione	Implementazione
METTI bucket	<p>Questa operazione crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket.</p> <ul style="list-style-type: none"> <li>• I nomi dei bucket devono rispettare le seguenti regole: <ul style="list-style-type: none"> <li>◦ Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).</li> <li>◦ Deve essere conforme al DNS.</li> <li>◦ Deve contenere almeno 3 e non più di 63 caratteri.</li> <li>◦ Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini.</li> <li>◦ Non deve essere simile a un indirizzo IP formattato con testo.</li> <li>◦ Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server.</li> </ul> </li> <li>• Per impostazione predefinita, i bucket vengono creati in <code>us-east-1</code> regione; tuttavia, è possibile utilizzare <code>LocationConstraint</code> elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza <code>LocationConstraint</code> È necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API Grid Management. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare.</li> </ul> <p><b>Nota:</b> Si verifica un errore se la richiesta PUT bucket utilizza un'area non definita in StorageGRID.</p> <ul style="list-style-type: none"> <li>• È possibile includere <code>x-amz-bucket-object-lock-enabled</code> Richiedi intestazione per creare un bucket con blocco oggetti S3 attivato. Vedere <a href="#">"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"</a>.</li> </ul> <p>È necessario attivare il blocco oggetti S3 quando si crea il bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea il bucket.</p>
METTI cors bucket	<p>Questa operazione imposta la configurazione del CORS per un bucket in modo che il bucket possa gestire le richieste di origine incrociata. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Si supponga, ad esempio, di utilizzare un bucket S3 denominato <code>images</code> per memorizzare le immagini. Impostando la configurazione CORS per <code>images</code> bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito web <code>http://www.example.com</code>.</p>

Operazione	Implementazione
METTI la crittografia bucket	<p>Questa operazione imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è attivata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con le chiavi gestite da StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare SSEAlgorithm parametro a AES256`e non utilizzare `KMSTMasterKeyID parametro.</p> <p>La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento degli oggetti specifica già la crittografia, ovvero se la richiesta include x-amz-server-side-encryption-* intestazione della richiesta).</p>
METTI IL ciclo di vita del bucket (PutBucketLifecycleConfiguration)	<p>Questa operazione crea una nuova configurazione del ciclo di vita per il bucket o sostituisce una configurazione del ciclo di vita esistente. StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:</p> <ul style="list-style-type: none"> <li>• Scadenza (giorni, data)</li> <li>• Non currentVersionExpiration (non currentDays)</li> <li>• Filtro (prefisso, tag)</li> <li>• Stato</li> <li>• ID</li> </ul> <p>StorageGRID non supporta queste azioni:</p> <ul style="list-style-type: none"> <li>• AbortIncompleteMultipartUpload</li> <li>• ExpiredObjectDeleteMarker</li> <li>• Transizione</li> </ul> <p>Vedere "<a href="#">Creare la configurazione del ciclo di vita S3</a>". Per comprendere come l'azione di scadenza in un ciclo di vita del bucket interagisce con le istruzioni di posizionamento ILM, vedere "<a href="#">Come ILM opera per tutta la vita di un oggetto</a>".</p> <p><b>Nota:</b> La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.</p>

Operazione	Implementazione
NOTIFICA DEL bucket  (PutBucketNotificationConfiguration)	<p>Questa operazione configura le notifiche per il bucket utilizzando l'XML di configurazione delle notifiche incluso nel corpo della richiesta. È necessario conoscere i seguenti dettagli di implementazione:</p> <ul style="list-style-type: none"> <li>• StorageGRID supporta gli argomenti del servizio di notifica semplice (SNS) come destinazioni. Gli endpoint SQS (Simple Queue Service) o Amazon Lambda non sono supportati.</li> <li>• La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID. Gli endpoint possono essere creati utilizzando il tenant Manager o l'API di gestione tenant.</li> </ul> <p>L'endpoint deve esistere perché la configurazione della notifica abbia esito positivo. Se l'endpoint non esiste, un 400 Bad Request viene restituito un errore con il codice <code>InvalidArgument</code>.</p> <ul style="list-style-type: none"> <li>• Non è possibile configurare una notifica per i seguenti tipi di evento. Questi tipi di evento sono <b>non</b> supportati. <ul style="list-style-type: none"> <li>◦ <code>s3:ReducedRedundancyLostObject</code></li> <li>◦ <code>s3:ObjectRestore:Completed</code></li> </ul> </li> <li>• Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ad eccezione del fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente: <ul style="list-style-type: none"> <li>◦ <b>EventSource</b>  <code>sgws:s3</code></li> <li>◦ <b>AwsRegion</b>  non incluso</li> <li>◦ <b>x-amz-id-2</b>  non incluso</li> <li>◦ <b>arn</b>  <code>urn:sgws:s3:::bucket_name</code></li> </ul> </li> </ul>
METTI la policy bucket	Questa operazione imposta la policy associata al bucket.

Operazione	Implementazione
METTI la replica del bucket	<p>Questa operazione viene configurata "<a href="#">Replica di StorageGRID CloudMirror</a>" Per il bucket che utilizza l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica di CloudMirror, è necessario conoscere i seguenti dettagli di implementazione:</p> <ul style="list-style-type: none"> <li>• StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo di <code>Filter</code> Per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, vedere "<a href="#">Documentazione di Amazon S3 sulla configurazione della replica</a>".</li> <li>• La replica del bucket può essere configurata su bucket con versione o senza versione.</li> <li>• È possibile specificare un bucket di destinazione diverso in ciascuna regola dell'XML di configurazione della replica. Un bucket di origine può replicare in più di un bucket di destinazione.</li> <li>• I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID, come specificato in Gestione tenant o nell'API di gestione tenant. Vedere "<a href="#">Configurare la replica di CloudMirror</a>".</li> </ul> <p>L'endpoint deve esistere per il successo della configurazione della replica. Se l'endpoint non esiste, la richiesta fallisce come a. 400 Bad Request. Il messaggio di errore indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> <li>• Non è necessario specificare un <code>Role</code> Nel file XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato.</li> <li>• Se si omette la classe di storage dall'XML di configurazione, StorageGRID utilizza <code>STANDARD</code> classe di storage per impostazione predefinita.</li> <li>• Se si elimina un oggetto dal bucket di origine o si elimina lo stesso bucket di origine, il comportamento della replica tra regioni è il seguente: <ul style="list-style-type: none"> <li>◦ Se si elimina l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non viene replicato e non viene inviata alcuna notifica.</li> <li>◦ Se elimini l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento standard di eliminazione di Amazon S3 per V1 della replica tra regioni.</li> </ul> </li> </ul>
INSERIRE il contrassegno bucket	<p>Questa operazione utilizza <code>tagging</code> sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni:</p> <ul style="list-style-type: none"> <li>• StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket.</li> <li>• Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode.</li> <li>• I valori dei tag possono contenere fino a 256 caratteri Unicode.</li> <li>• Chiave e valori distinguono tra maiuscole e minuscole.</li> </ul>

Operazione	Implementazione
METTERE il bucket in versione	<p>Questa implementazione utilizza <code>versioning</code> sottorisorsa per impostare lo stato di versione di un bucket esistente. È possibile impostare lo stato di versione con uno dei seguenti valori:</p> <ul style="list-style-type: none"> <li>• <b>Enabled (attivato):</b> Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco.</li> <li>• <b>Suspended (sospeso):</b> Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione <code>null</code>.</li> </ul>
PUT Object Lock Configuration (CONFIGURAZIONE blocco oggetto)	<p>Questa operazione consente di configurare o rimuovere la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito.</p> <p>Se il periodo di conservazione predefinito viene modificato, la data di conservazione delle versioni degli oggetti esistenti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.</p> <p>Vedere <a href="#">"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"</a> per informazioni dettagliate.</p>

#### Informazioni correlate

["Controlli di coerenza"](#)

["OTTIENI l'ultimo tempo di accesso a bucket"](#)

["Utilizza policy di accesso a bucket e gruppi"](#)

["Operazioni S3 monitorate nei registri di audit"](#)

#### Operazioni personalizzate sui bucket

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

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

Operazione	Descrizione	Per ulteriori informazioni
COERENZA del bucket	Restituisce il livello di coerenza applicato a un determinato bucket.	<a href="#">"COERENZA del bucket"</a>
METTI la coerenza del bucket	Imposta il livello di coerenza applicato a un bucket specifico.	<a href="#">"METTI la coerenza del bucket"</a>
OTTIENI l'ultimo tempo di accesso a bucket	Restituisce se gli ultimi aggiornamenti dell'ora di accesso sono attivati o disattivati per un bucket specifico.	<a href="#">"OTTIENI l'ultimo tempo di accesso a bucket"</a>

Operazione	Descrizione	Per ulteriori informazioni
TEMPO ULTIMO accesso bucket	Consente di attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso per un determinato bucket.	<a href="#">"TEMPO ULTIMO accesso bucket"</a>
ELIMINA la configurazione di notifica dei metadati del bucket	Elimina l'XML di configurazione della notifica dei metadati associato a un bucket specifico.	<a href="#">"ELIMINA la configurazione di notifica dei metadati del bucket"</a>
OTTIENI la configurazione della notifica dei metadati del bucket	Restituisce l'XML di configurazione della notifica dei metadati associato a un bucket specifico.	<a href="#">"OTTIENI la configurazione della notifica dei metadati del bucket"</a>
INSERIRE la configurazione della notifica dei metadati del bucket	Configura il servizio di notifica dei metadati per un bucket.	<a href="#">"INSERIRE la configurazione della notifica dei metadati del bucket"</a>
METTI il bucket con le impostazioni di conformità	Obsoleto e non supportato: Non è più possibile creare nuovi bucket con Compliance abilitata.	<a href="#">"Deprecato: METTI il bucket con le impostazioni di conformità"</a>
OTTIENI la compliance del bucket	Obsoleto ma supportato: Restituisce le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.	<a href="#">"Obsoleto: OTTIENI la compliance del bucket"</a>
METTI la compliance del bucket	Obsoleto ma supportato: Consente di modificare le impostazioni di conformità per un bucket compatibile esistente.	<a href="#">"Obsoleto: METTI la compliance del bucket"</a>

#### Informazioni correlate

["Operazioni S3 registrate nei registri di audit"](#)

## Operazioni sugli oggetti

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

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

- StorageGRID ["controlli di coerenza"](#) sono supportate da tutte le operazioni sugli oggetti, ad eccezione di quanto segue:
  - GET Object ACL (OTTIENI ACL oggetto)
  - OPTIONS /
  - METTERE in attesa legale l'oggetto



- METTI la conservazione degli oggetti
- SELEZIONARE il contenuto dell'oggetto
- Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione "ultimi successi" si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.
- Impossibile accedere agli oggetti dati acquisiti nel sistema StorageGRID tramite Swift tramite S3.

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

Operazione	Implementazione
ELIMINA oggetto	<p data-bbox="589 163 1479 226">Autenticazione multifattore (MFA) e intestazione della risposta <code>x-amz-mfa</code> non sono supportati.</p> <p data-bbox="589 268 1479 541">Durante l'elaborazione di una richiesta DI ELIMINAZIONE degli oggetti, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.</p> <p data-bbox="589 573 708 604"><b>Versione</b></p> <p data-bbox="630 615 1479 825">Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare <code>versionId</code> sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il <code>versionId</code> corrisponde a un indicatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene restituito impostato su <code>true</code>.</p> <ul data-bbox="654 867 1479 1297" style="list-style-type: none"> <li>• Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket abilitato alla versione, si ottiene la generazione di un indicatore di eliminazione. Il <code>versionId</code> per il contrassegno di eliminazione viene restituito utilizzando <code>x-amz-version-id</code> intestazione della risposta e la <code>x-amz-delete-marker</code> l'intestazione della risposta viene restituita impostata su <code>true</code>.</li> <li>• Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket sospeso della versione, si ottiene una cancellazione permanente di una versione 'null' già esistente o di un marker di eliminazione 'null' e la generazione di un nuovo marker di eliminazione 'null'. Il <code>x-amz-delete-marker</code> l'intestazione della risposta viene restituita impostata su <code>true</code>.</li> </ul> <p data-bbox="678 1339 1406 1402"><b>Nota:</b> In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione.</p> <p data-bbox="589 1455 1463 1549">Vedere <a href="#">"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"</a> Per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.</p>
ELIMINARE più oggetti (DeleteObjects)	<p data-bbox="589 1612 1479 1675">Autenticazione multifattore (MFA) e intestazione della risposta <code>x-amz-mfa</code> non sono supportati.</p> <p data-bbox="589 1707 1430 1738">È possibile eliminare più oggetti nello stesso messaggio di richiesta.</p> <p data-bbox="589 1780 1463 1875">Vedere <a href="#">"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"</a> Per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.</p>

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

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

#### Informazioni correlate

["Operazioni S3 monitorate nei registri di audit"](#)

## USA S3 Select

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



Gli elementi non elencati non sono supportati.

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

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

### Clausole

- SELEZIONARE l'elenco
- CLAUSOLA FROM
- Clausola WHERE
- Clausola LIMIT

### Tipi di dati

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

### Operatori

#### Operatori logici

- E.
- NO
- OPPURE

#### Operatori di confronto

- <
- >
- <=
- >=
- =
- =
- <>

- !=
- TRA
- POLL

### **Operatori di corrispondenza dei modelli**

- MI PIACE
- \_
- %

### **Operatori unitari**

- È NULL
- NON È NULL

### **Operatori matematici**

- +
- -
- \*
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

### **Funzioni di aggregazione**

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

### **Funzioni condizionali**

- CASO
- COALESCE
- NULLIF

### **Funzioni di conversione**

- CAST (per il tipo di dati supportato)

### **Funzioni di data**

- DATA\_ADD
- DATA\_DIFF

- ESTRARRE
- TO\_STRING
- TO\_TIMESTAMP
- UTCNOW

#### Funzioni di stringa

- CHAR\_LENGTH, CHARACTER\_LENGTH
- ABBASSARE
- SOTTOSTRINGA
- TAGLIARE
- SUPERIORE

#### Utilizzare la crittografia lato server

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

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

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

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



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



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

#### Utilizzare SSE

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

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

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

- "METTI oggetto"

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

#### Utilizzare SSE-C.

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

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

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

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

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

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

- È necessario utilizzare https.



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

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



versione dell'oggetto.

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



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

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

#### Informazioni correlate

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

#### OTTIENI oggetto

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

#### OTTIENI oggetti oggetto e multiparte

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

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

#### UTF-8 caratteri nei metadati dell'utente

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

#### Intestazione della richiesta non supportata

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

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

#### Versione

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

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

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

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



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

### Comportamento di GET Object per gli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in ["Pool di cloud storage"](#), Il comportamento di una richiesta DI oggetto GET dipende dallo stato dell'oggetto. Vedere ["Oggetto TESTA"](#) per ulteriori dettagli.



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

Stato dell'oggetto	Comportamento dell'oggetto GET
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK  Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK  Viene recuperata una copia dell'oggetto.
Oggetto sottoposto a transizione in uno stato non recuperabile	403 Forbidden, InvalidObjectState  Utilizzare un <a href="#">"RIPRISTINO POST-oggetto"</a> richiesta di ripristino dell'oggetto in uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden, InvalidObjectState  Attendere il completamento della richiesta DI ripristino dell'oggetto POST.
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK  Viene recuperata una copia dell'oggetto.

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

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

o quando alcune parti dell'oggetto non sono ancora state ripristinate.

In questi casi:

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

#### OTTIENI replica di oggetti e cross-grid

Se si utilizza ["federazione di grid"](#) e ["replica cross-grid"](#) È attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta DI oggetto GET. La risposta include lo specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	<ul style="list-style-type: none"><li>• <b>SUCCESSO</b>: La replica è riuscita.</li><li>• <b>PENDING</b>: L'oggetto non è stato ancora replicato.</li><li>• <b>ERRORE</b>: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.</li></ul>
Destinazione	<b>REPLICA</b> : L'oggetto è stato replicato dalla griglia di origine.



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

#### Informazioni correlate

["Operazioni S3 monitorate nei registri di audit"](#)

#### Oggetto TESTA

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

#### OGGETTI TESTA e multiparte

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

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

#### UTF-8 caratteri nei metadati dell'utente

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

## Intestazione della richiesta non supportata

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

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

## Versione

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

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

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

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



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

## Risposte DEGLI oggetti HEAD per gli oggetti del Cloud Storage Pool

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

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

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

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

Stato dell'oggetto	Risposta all'oggetto HEAD
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Fino a quando l'oggetto non passa a uno stato non recuperabile, il valore per <code>expiry-date</code> è impostato su un periodo di tempo lontano in futuro. L'ora esatta della transizione non è controllata dal sistema StorageGRID.</p>
L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella griglia	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Il valore per <code>expiry-date</code> è impostato su un periodo di tempo lontano in futuro.</p> <p><b>Nota:</b> Se la copia sulla griglia non è disponibile (ad esempio, un nodo di storage non è disponibile), è necessario eseguire una <a href="#">"RIPRISTINO POST-oggetto"</a> Richiesta di ripristino della copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.</p>
L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella griglia	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Oggetto in fase di ripristino da uno stato non recuperabile	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

Stato dell'oggetto	Risposta all'oggetto HEAD
Oggetto completamente ripristinato nel Cloud Storage Pool	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT"</p> <p>Il expiry-date Indica quando l'oggetto nel Cloud Storage Pool verrà riportato in uno stato non recuperabile.</p>

### Oggetti multiparte o segmentati nel Cloud Storage Pool

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

### Replica di oggetti HEAD e cross-grid

Se si utilizza ["federazione di grid"](#) e ["replica cross-grid"](#) È abilitato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta di oggetto HEAD. La risposta include lo specifico StorageGRID x-ntap-sg-cgr-replication-status intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	<ul style="list-style-type: none"> <li>• <b>SUCCESSO:</b> La replica è riuscita.</li> <li>• <b>PENDING:</b> L'oggetto non è stato ancora replicato.</li> <li>• <b>ERRORE:</b> La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.</li> </ul>
Destinazione	<b>REPLICA:</b> L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta x-amz-replication-status intestazione.

### Informazioni correlate

["Operazioni S3 monitorate nei registri di audit"](#)

### RIPRISTINO POST-oggetto

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

## Tipo di richiesta supportato

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

## Versione

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

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

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



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

Stato dell'oggetto	Comportamento del ripristino degli oggetti POST
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	403 Forbidden, InvalidObjectState
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Non vengono apportate modifiche.  <b>Nota:</b> Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificarne lo stato <code>expiry-date</code> .
Oggetto sottoposto a transizione in uno stato non recuperabile	202 Accepted Ripristina una copia recuperabile dell'oggetto nel Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto viene riportato in uno stato non recuperabile.  In alternativa, utilizzare <code>Tier</code> elemento request per determinare il tempo necessario per il completamento del processo di ripristino ( <code>Expedited</code> , <code>Standard</code> , o <code>Bulk</code> ). Se non si specifica <code>Tier</code> , il <code>Standard</code> viene utilizzato il tier.  <b>Importante:</b> Se un oggetto è stato spostato in S3 Glacier Deep Archive o il Cloud Storage Pool utilizza lo storage Azure Blob, non è possibile ripristinarlo utilizzando <code>Expedited tier</code> . Viene visualizzato il seguente errore 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Oggetto in fase di ripristino da uno stato non recuperabile	409 Conflict, RestoreAlreadyInProgress

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

## Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Oggetto TESTA"](#)

["Operazioni S3 monitorate nei registri di audit"](#)

## METTI oggetto

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

### Risolvi i conflitti

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

### Dimensione dell'oggetto

La dimensione massima *consigliata* per un'operazione di singolo oggetto PUT è 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.

La dimensione massima *supportata* per un'operazione a singolo oggetto PUT è 5 TiB (5,497,558,138,880 byte). Tuttavia, l'avviso **S3 PUT object size too large** (DIMENSIONE oggetto ECCESSIVA) viene attivato se si tenta di caricare un oggetto che supera i 5 GiB.

### Dimensione dei metadati dell'utente

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

### UTF-8 caratteri nei metadati dell'utente

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

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

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



valore della chiave include caratteri non stampabili.

### Limiti tag oggetto

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

### Proprietà degli oggetti

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

### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

- StorageGRID non verifica `chunk-signature` rispetto ai dati del blocco.
- StorageGRID non verifica il valore fornito `x-amz-decoded-content-length` rispetto all'oggetto.

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

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

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

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

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

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

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

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



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

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

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

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

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

### Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

### Opzioni di classe storage

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

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

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

- STANDARD (Impostazione predefinita)

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

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

- **REDUCED\_REDUNDANCY**

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

Utilizzando il `REDUCED_REDUNDANCY` l'opzione non è consigliata in altre circostanze.

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



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

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



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

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

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

- **SSE:** Utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca

gestita da StorageGRID.

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

- **SSE-C:** Utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.

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

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

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



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



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

## Versione

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

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

## Calcoli della firma per l'intestazione autorizzazione

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

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



Come Best practice generale, includere sempre queste intestazioni all'interno di `CanonicalHeaders` Per verificare che siano state verificate, tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce alcun errore.

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

## Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Operazioni sui bucket"](#)

["Operazioni S3 monitorate nei registri di audit"](#)

## METTI oggetto - Copia

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

### Risolvi i conflitti

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

### Dimensione dell'oggetto

La dimensione massima *consigliata* per un'operazione di singolo oggetto PUT è 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.

La dimensione massima *supportata* per un'operazione a singolo oggetto PUT è 5 TiB (5,497,558,138,880 byte). Tuttavia, l'avviso **S3 PUT object size too large** (DIMENSIONE oggetto ECCESSIVA) viene attivato se si tenta di caricare un oggetto che supera i 5 GiB.

### UTF-8 caratteri nei metadati dell'utente

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

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

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

### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

- Intestazioni della richiesta di blocco oggetti S3:

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

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

- Intestazioni di richiesta SSE:

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

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

### Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

### Opzioni di classe storage

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

commit o bilanciato.

- STANDARD

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

- REDUCED\_REDUNDANCY

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



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

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

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

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

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

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

### Intestazioni di richiesta per la crittografia lato server

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

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

- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto di origine.
- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca che si fornisce e si gestisce, includere le seguenti tre intestazioni:
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
  - `x-amz-server-side-encryption-customer-key`: Specificare una nuova chiave di crittografia per l'oggetto di destinazione.
  - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della nuova chiave di crittografia.



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

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



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

## Versione

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

## Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Operazioni S3 monitorate nei registri di audit"](#)

["METTI oggetto"](#)

## SelectObjectContent

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

Per ulteriori informazioni, consultare ["Documentazione AWS per SelectObjectContent"](#).

## Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.



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



L'utilizzo di ScanRange non è supportato.

#### Esempio di sintassi per le richieste CSV

```

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

```

#### Esempio di sintassi della richiesta di parquet

```

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

```

### Esempio di query SQL

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

```

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

```

Le prime righe del file da interrogare, SUB-EST2020\_ALL.csv, ad esempio:

```
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, ad esempio:

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

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

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

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

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

## Operazioni per caricamenti multiparte

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

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

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

corretta in un secondo momento.

- Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. Quando ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.
- Tutte le operazioni di caricamento multiparte supportano i controlli di coerenza StorageGRID.
- Se necessario, è possibile utilizzare la crittografia lato server con upload multiparte. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere `x-amz-server-side-encryption` Intestazione della richiesta solo nella richiesta di avvio caricamento multiparte. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta Initiate Multipart Upload (Avvia caricamento multiparte) e in ogni richiesta successiva di caricamento parte.

Operazione	Implementazione
Elenca carichi multiparte	Vedere <a href="#">"Elenca carichi multiparte"</a>
Avvia caricamento multiparte	Vedere <a href="#">"Avvia caricamento multiparte"</a>
Carica parte	Vedere <a href="#">"Carica parte"</a>
Carica parte - Copia	Vedere <a href="#">"Carica parte - Copia"</a>
Caricamento multiparte completo	Vedere <a href="#">"Caricamento multiparte completo"</a>
Interrompi caricamento multiparte	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
Elencare le parti	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.

#### Informazioni correlate

- ["Controlli di coerenza"](#)
- ["Utilizzare la crittografia lato server"](#)

#### Elenca carichi multiparte

L'operazione List Multipart Uploads elenca i carichi multiparte in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `key-marker`

- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

## Versione

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

## Avvia caricamento multipart

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

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

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

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

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

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

- **REDUCED\_REDUNDANCY**
  - **Commit doppio:** Se la regola ILM specifica l'opzione commit doppio per il comportamento di `Ingest`, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
  - **Balanced:** Se la regola ILM specifica l'opzione `Balanced`, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha

alcun effetto. Il `REDUCED_REDUNDANCY` L'opzione è preferibile quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

Utilizzando il `REDUCED_REDUNDANCY` l'opzione non è consigliata in altre circostanze.

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



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

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



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

Sono supportate le seguenti intestazioni di richiesta:

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

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

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

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

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

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



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



- Intestazioni della richiesta di blocco oggetti S3:

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

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

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

- Intestazioni di richiesta SSE:

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

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



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

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

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

- **SSE:** Utilizzare la seguente intestazione nella richiesta di avvio caricamento multiparte se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste di carica parte.

- x-amz-server-side-encryption

- **SSE-C:** Utilizzare tutte e tre queste intestazioni nella richiesta Initiate Multipart Upload (e in ogni richiesta successiva di carica parte) se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.

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



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

### Intestazioni di richiesta non supportate

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

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

### Versione

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

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["METTI oggetto"](#)

### Carica parte

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

### Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

### Intestazioni di richiesta per la crittografia lato server

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

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



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

### Versione

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

### Informazioni correlate

## Carica parte - Copia

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

L'operazione carica parte - Copia viene implementata con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.

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

Sono supportate le seguenti intestazioni di richiesta:

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

### Intestazioni di richiesta per la crittografia lato server

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

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

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

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



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

### Versione

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

multiparte.

## Caricamento multiparte completo

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

### Risolvi i conflitti

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

### Intestazioni delle richieste

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

- STANDARD

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

- REDUCED\_REDUNDANCY

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



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



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



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

### Versione

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

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

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



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

#### Replica, notifica o notifica dei metadati non riuscite

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

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

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

#### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

## Risposte agli errori

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

#### Codici di errore S3 API supportati

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

Nome	Stato HTTP
InvalidBucketName	400 richiesta errata
InvalidBucketState	409 conflitto
InvalidDigest	400 richiesta errata
InvalidEncryptionAlgorithmError	400 richiesta errata
InvalidPart	400 richiesta errata
InvalidPartOrder	400 richiesta errata
InvalidRange	416 intervallo richiesto non riscontrabile
InvalidRequest	400 richiesta errata
InvalidStorageClass	400 richiesta errata
InvalidTag	400 richiesta errata
InvalidURI	400 richiesta errata
KeyTooLong	400 richiesta errata
MalformedXML	400 richiesta errata
MetadataTooLarge	400 richiesta errata
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
MissingRequestBodyError	400 richiesta errata
MissingSecurityHeader	400 richiesta errata
NoSuchBucket	404 non trovato
NoSuchKey	404 non trovato
NoSuchUpload	404 non trovato
Non soddisfatto	501 non implementato

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

#### Codici di errore personalizzati StorageGRID

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

Nome	Descrizione	Stato HTTP
XNotImplemented	La richiesta fornita implica funzionalità non implementate.	501 non implementato

## Richieste StorageGRID S3

### COERENZA del bucket

La richiesta DI coerenza GET Bucket consente di determinare il livello di coerenza applicato a un determinato bucket.

I controlli di coerenza predefiniti sono impostati in modo da garantire la lettura dopo la scrittura degli oggetti creati di recente.

Per completare questa operazione, si dispone dell'autorizzazione s3:GetBucketConsistency o si è root dell'account.

### Esempio di richiesta

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

### Risposta

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

Controllo della coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.



Controllo della coerenza	Descrizione
disponibile	Fornisce una 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 raramente letti o per operazioni HEAD o GET su chiavi che non esistono). 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

["Controlli di coerenza"](#)

## METTI la coerenza del bucket

La richiesta DI coerenza PUT bucket consente di specificare il livello di coerenza da applicare alle operazioni eseguite su un bucket.

I controlli di coerenza predefiniti sono impostati in modo da garantire la lettura dopo la scrittura degli oggetti creati di recente.

### Prima di iniziare

Per completare questa operazione, si dispone dell'autorizzazione s3:PutBucketConsistency o si è root dell'account.

### Richiesta

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

Controllo della coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.

Controllo della coerenza	Descrizione
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
disponibile	Fornisce una 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 raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

**Nota:** in generale, utilizzare il valore del controllo di coerenza “read-after-new-write”. Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare il controllo di coerenza per ogni richiesta API. Impostare il controllo di coerenza a livello di bucket solo come ultima risorsa.

### Esempio di richiesta

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

### Informazioni correlate

["Controlli di coerenza"](#)

## OTTIENI l'ultimo tempo di accesso a bucket

La richiesta GET bucket last access time (OTTIENI bucket ultimo accesso) consente di determinare se gli ultimi aggiornamenti dell'orario di accesso sono attivati o disattivati per i singoli bucket.

Per completare questa operazione, si dispone dell'autorizzazione s3:GetBucketLastAccessTime o si è root dell'account.

### Esempio di richiesta

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

### Esempio di risposta

Questo esempio mostra che gli ultimi aggiornamenti dell'ora di accesso sono attivati 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>
```

## TEMPO ULTIMO accesso bucket

La richiesta PUT bucket Last access time consente di attivare o disattivare gli ultimi aggiornamenti del tempo di accesso per i singoli bucket. La disattivazione degli ultimi aggiornamenti dell'orario di 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, si dispone dell'autorizzazione s3:PutBucketLastAccessTime per un bucket o si è root dell'account.



A partire dalla versione 10.3 di StorageGRID, gli aggiornamenti all'ultimo tempo di accesso sono disattivati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera che corrispondano al nuovo comportamento predefinito, è necessario disattivare esplicitamente gli ultimi aggiornamenti del tempo di accesso per ciascuno di questi bucket precedenti. È possibile attivare o disattivare gli aggiornamenti per l'ultimo accesso utilizzando LA richiesta PUT bucket last access time, la casella di controllo **S3 > Bucket > Change Last Access Setting** (Modifica impostazione ultimo accesso) in Tenant Manager o l'API di gestione tenant.

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

- LE richieste GET Object, GET Object ACL, GET Object Tagging e HEAD Object non aggiornano l'ultimo tempo di accesso. L'oggetto non viene aggiunto alle code per la valutazione ILM (Information Lifecycle Management).

- PUT Object (INSERISCI oggetto) - le richieste di tag degli oggetti di copia e INSERIMENTO che aggiornano solo i metadati aggiornano anche l'ultimo tempo di accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti dell'ultimo tempo di accesso sono disattivati per il bucket di origine, LE richieste PUT object - Copy non aggiornano l'ultimo tempo di accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM del bucket di origine. Tuttavia, per la destinazione, PUT Object - le richieste di copia aggiornano sempre l'ultimo tempo di accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- Le richieste complete di caricamento Multipart aggiornano l'ultimo tempo di accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

## Richiedi esempi

In questo esempio viene attivato l'ultimo tempo di accesso per un bucket.

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

Questo esempio disattiva l'ultimo tempo di accesso per un bucket.

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

## Informazioni correlate

["Utilizzare un account tenant"](#)

## ELIMINA la configurazione di notifica dei metadati del bucket

La richiesta di configurazione DELLA notifica dei metadati DEL bucket DELETE consente di disattivare il servizio di integrazione della ricerca per i singoli bucket eliminando il file XML di configurazione.

Per completare questa operazione, si dispone dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket o si è account root.

## Esempio di richiesta

Questo esempio mostra la disattivazione del 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
```

## OTTIENI la configurazione della notifica dei metadati del bucket

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

Per completare questa operazione, si dispone dell'autorizzazione `s3:GetBucketMetadataNotification` o si è root dell'account.

### Esempio di richiesta

Questa richiesta recupera la configurazione di 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 la configurazione del bucket per l'integrazione della ricerca. Ciò consente di determinare quali oggetti vengono 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 in cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	<p>Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati.</p> <p>Contiene uno o più elementi della regola.</p>	Sì
Regola	<p>Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato.</p> <p>Le regole con prefissi sovrapposti vengono rifiutate.</p> <p>Incluso nell'elemento MetadataNotificationConfiguration.</p>	Sì
ID	<p>Identificatore univoco della regola.</p> <p>Incluso nell'elemento Rule.</p>	No
Stato	<p>Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate.</p> <p>Incluso nell'elemento Rule.</p>	Sì

Nome	Descrizione	Obbligatorio
Prefisso	<p>Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata.</p> <p>Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Destinazione	<p>Tag container per la destinazione di una regola.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Urna	<p>URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà:</p> <ul style="list-style-type: none"> <li>• <code>es</code> deve essere il terzo elemento.</li> <li>• L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form <code>domain-name/myindex/mytype</code>.</li> </ul> <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> <li>• <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code></li> <li>• <code>urn:mysite:es:::mydomain/myindex/mytype</code></li> </ul> <p>L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404.</p> <p>L'urn è incluso nell'elemento Destination.</p>	Sì

## Esempio di risposta

L'XML incluso tra

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tag mostra come è configurata l'integrazione con un endpoint di integrazione della ricerca per il bucket. In questo esempio, i metadati degli oggetti vengono inviati a un indice Elasticsearch denominato `current` e digitare `named 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"](#)

## INSERIRE la configurazione della notifica dei metadati del bucket

La richiesta di configurazione DELLA notifica dei metadati PUT bucket consente di attivare il servizio di integrazione della ricerca per i singoli bucket. L'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, si dispone dell'autorizzazione `s3:PutBucketMetadataNotification` per un bucket o si è root dell'account.

### 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 in cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per oggetti con il prefisso `/images` a una destinazione e agli oggetti con il prefisso `/videos` a un 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 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, oppure la richiesta non riesce come a. 400 Bad Request. Il messaggio di errore indica: 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 contenuti nel file XML di configurazione per la notifica dei metadati.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfi guration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati.  Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato.  Le regole con prefissi sovrapposti vengono rifiutate.  Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola.  Incluso nell'elemento Rule.	No

Nome	Descrizione	Obbligatorio
Stato	<p>Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Prefisso	<p>Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata.</p> <p>Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Destinazione	<p>Tag container per la destinazione di una regola.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Urna	<p>URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà:</p> <ul style="list-style-type: none"> <li>• <code>es</code> deve essere il terzo elemento.</li> <li>• L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form <code>domain-name/myindex/mytype</code>.</li> </ul> <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> <li>• <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code></li> <li>• <code>urn:mysite:es:::mydomain/myindex/mytype</code></li> </ul> <p>L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404.</p> <p>L'urn è incluso nell'elemento Destination.</p>	Sì

### Richiedi esempi

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati degli oggetti per 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, i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti per gli oggetti che 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-1:33333333: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 attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` bucket non è configurato, quindi il `versionId` tag 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

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando è attivata 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'elemento	Descrizione
Informazioni su bucket e oggetti	bucket	Nome del bucket
Informazioni su bucket e oggetti	chiave	Nome chiave oggetto
Informazioni su bucket e oggetti	ID versione	Versione oggetto, per gli oggetti nei bucket con versione
Informazioni su bucket e oggetti	regione	Area bucket, ad esempio <code>us-east-1</code>
Metadati di sistema	dimensione	Dimensione dell'oggetto (in byte) come visibile a un client HTTP
Metadati di sistema	md5	Hash di oggetto
Metadati dell'utente	metadati <i>key:value</i>	Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore

Tipo	Nome dell'elemento	Descrizione
Tag	tag <i>key:value</i>	Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore



Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

## Informazioni correlate

["Utilizzare un account tenant"](#)

## OTTIENI la richiesta di utilizzo dello storage

La richiesta GET Storage Usage indica la quantità totale di storage in uso da un account e per ciascun bucket associato all'account.

La quantità di storage utilizzata da un account e dai relativi bucket può essere ottenuta tramite una richiesta GET Service modificata con `x-ntap-sg-usage` parametro di query. L'utilizzo dello storage bucket viene monitorato separatamente dalle richieste DI PUT ed ELIMINAZIONE 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 pesante.

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

Per completare questa operazione, si dispone dell'autorizzazione `s3:ListAllMyBucket` o si è root dell'account.

## Esempio di richiesta

```
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>
```

## Versione

Ogni versione dell'oggetto memorizzata contribuirà a. ObjectCount e. DataBytes valori nella risposta. I contrassegni di eliminazione non vengono aggiunti a ObjectCount totale.

## Informazioni correlate

["Controlli di coerenza"](#)

## Richieste bucket obsolete per conformità legacy

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

## Funzionalità di compliance obsoleta

La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

Se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale viene attivata in StorageGRID 11.6. Non è più possibile creare nuovi bucket con la conformità abilitata;

tuttavia, se necessario, è possibile utilizzare l'API REST di StorageGRID S3 per gestire qualsiasi bucket compatibile esistente.

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Richieste di conformità obsolete:

- ["Deprecato - CONSENTE DI APPORTARE modifiche alla richiesta di conformità al bucket"](#)

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML opzionale di PUT bucket Requests per creare un bucket conforme.

- ["Obsoleto - CONFORMITÀ bucket"](#)

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

- ["Deprecato - METTERE la compliance del bucket"](#)

La richiesta DI compliance DEL bucket PUT è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.

#### **Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket**

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML opzionale di PUT bucket Requests per creare un bucket conforme.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["Gestire gli oggetti con ILM"](#)

["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Non è più possibile creare nuovi bucket con Compliance abilitata. Il seguente messaggio di errore viene visualizzato se si tenta di utilizzare LE modifiche DELLA richiesta PUT bucket per la conformità per creare un nuovo bucket Compliance:

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



## Deprecato: OTTIENI una richiesta di conformità bucket

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["Gestire gli oggetti con ILM"](#)

["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Per completare questa operazione, si dispone dell'autorizzazione s3:GetBucketCompliance o si è root dell'account.

### Esempio di richiesta

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 compliance in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di compliance per un bucket in cui ciascun oggetto verrà conservato per un anno (525,600 minuti), a partire da quando l'oggetto viene acquisito nella griglia. Attualmente non esiste un blocco legale in questo bucket. Ogni oggetto verrà automaticamente cancellato 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
RetentionPeriodMinutes	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia.
LegalHold	<ul style="list-style-type: none"> <li>• Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto.</li> <li>• Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.</li> </ul>
Eliminazione automatica	<ul style="list-style-type: none"> <li>• Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale.</li> <li>• Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.</li> </ul>

### Risposte agli errori

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.

### Deprecato: INSERIRE la richiesta di conformità del bucket

La richiesta DI compliance DEL bucket PUT è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["Gestire gli oggetti con ILM"](#)

["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Per completare questa operazione, si dispone dell'autorizzazione `s3:PutBucketCompliance` o si è root dell'account.

È necessario specificare un valore per ogni campo delle impostazioni di compliance quando si invia una richiesta DI compliance PUT bucket.

#### Esempio di richiesta

Questa richiesta di esempio modifica le impostazioni di compliance per il bucket denominato `mybucket`. In questo esempio, gli oggetti in `mybucket` verrà ora conservato per due anni (1,051,200 minuti) invece di un anno, a partire dal momento in cui l'oggetto viene acquisito nella griglia. Questo bucket non ha alcuna tenuta legale. Ogni oggetto verrà automaticamente cancellato 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
RetentionPeriodMinutes	<p>La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia.</p> <p><b>Importante</b> quando si specifica un nuovo valore per <code>RetentionPeriodMinutes</code>, è necessario specificare un valore uguale o superiore al periodo di conservazione corrente del bucket. Una volta impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore, ma solo aumentarlo.</p>

Nome	Descrizione
LegalHold	<ul style="list-style-type: none"> <li>• Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto.</li> <li>• Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.</li> </ul>
Eliminazione automatica	<ul style="list-style-type: none"> <li>• Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale.</li> <li>• Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.</li> </ul>

#### Livello di coerenza per le impostazioni di conformità

Quando aggiorni le impostazioni di compliance per un bucket S3 con una richiesta DI compliance PUT bucket, StorageGRID tenta di aggiornare i metadati del bucket nella griglia. Per impostazione predefinita, StorageGRID utilizza il livello di coerenza **strong-Global** per garantire che tutti i siti del data center e tutti i nodi di storage che contengono metadati bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere il livello di coerenza **strong-Global** perché un sito del data center o più nodi di storage 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 del grid per assicurarsi che i servizi di storage richiesti siano resi disponibili il prima possibile. Se l'amministratore del grid non è in grado di rendere disponibile una quantità sufficiente di nodi di storage in ogni sito, il supporto tecnico potrebbe richiedere di riprovare la richiesta non riuscita forzando il livello di coerenza **strong-Site**.



Non forzare mai il livello di coerenza **strong-site** per LA compliance DEL bucket PUT, a meno che non sia stato richiesto dal supporto tecnico e a meno che non si comprendano le potenziali conseguenze dell'utilizzo di questo livello.

Quando il livello di coerenza viene ridotto a **strong-Site**, StorageGRID garantisce che le impostazioni di conformità aggiornate avranno una coerenza di lettura dopo scrittura solo per le richieste dei client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe disporre temporaneamente di più impostazioni incoerenti per questo bucket fino a quando non saranno disponibili tutti i siti e i nodi di storage. Le impostazioni incoerenti possono causare comportamenti imprevisti e indesiderati. Ad esempio, se si colloca un bucket sotto un blocco legale e si forza un livello di coerenza inferiore, le impostazioni di conformità precedenti del bucket (ovvero, blocco legale) potrebbero continuare a essere in vigore in alcuni siti del data center. Di conseguenza, gli oggetti che si ritiene siano in stato di conservazione a fini giudiziari potrebbero essere eliminati allo scadere del periodo di conservazione, dall'utente o mediante eliminazione automatica, se attivata.

Per forzare l'utilizzo del livello di coerenza **strong-site**, emettere nuovamente la richiesta DI conformità PUT bucket e includere `Consistency-Control` Intestazione della richiesta HTTP, come segue:

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

### Risposte agli errori

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

### Informazioni correlate

"[Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket](#)"

## Policy di accesso a bucket e gruppi

### Utilizza policy 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 dei criteri delle API REST S3. I criteri di accesso per l'API S3 sono scritti in JSON.

### Panoramica dei criteri di accesso

StorageGRID supporta due tipi di policy di accesso.

- **Le policy bucket**, configurate utilizzando le policy GET bucket, PUT bucket e DELETE Bucket Policy S3 API Operations. Le policy del bucket sono collegate ai bucket, quindi sono configurate per controllare l'accesso degli utenti nell'account del proprietario del bucket o altri account al bucket e agli oggetti in esso contenuti. Una policy di bucket si applica a un solo bucket ed eventualmente a più gruppi.
- **Criteri di gruppo**, configurati utilizzando l'API di gestione tenant Manager o tenant. I criteri di gruppo sono associati a un gruppo dell'account, quindi sono configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Una policy di gruppo si applica a un solo gruppo e possibilmente a più bucket.



Non vi è alcuna differenza di priorità tra le policy di gruppo e quelle di bucket.

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

- ID dichiarazione (Sid) (opzionale)
- Effetto
- Principal/NotPrincipal
- Risorsa/NotResource
- Azione/Notazione

- Condizione (opzionale)

Le istruzioni dei criteri vengono create utilizzando questa struttura per specificare le autorizzazioni: Grant <Effect> per consentire/negare a <Principal> di eseguire <Action> su <Resource> quando viene applicato <Condition>.

Ciascun elemento di policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
SID	L'elemento Sid è opzionale. Il Sid deve essere utilizzato solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID.
Effetto	Utilizzare l'elemento Effect per stabilire se le operazioni specificate sono consentite o rifiutate. È necessario identificare le operazioni consentite (o negate) su bucket o oggetti utilizzando le parole chiave dell'elemento Action supportate.
Principal/NotPrincipal	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.  È sufficiente specificare l'elemento Principal in una policy bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.
Risorsa/NotResource	L'elemento Resource identifica bucket e oggetti. Puoi consentire o negare le autorizzazioni per bucket e oggetti utilizzando il nome risorsa Amazon (ARN) per identificare la risorsa.
Azione/Notazione	Gli elementi Action e Effect 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 specificamente autorizzazioni, ma è possibile utilizzare la funzione di negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condition è opzionale. Le condizioni consentono di creare espressioni per determinare quando applicare un criterio.

Nell'elemento Action, è possibile utilizzare il carattere jolly (\*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde a permessi come s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Resource, 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, ad eccezione dell'impostazione dell'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, impostare il carattere jolly (\*) come valore Principal.

```
"Principal": "*"

```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. Questo esempio mostra un'istruzione completa di policy bucket che utilizza l'effetto "allow" per assegnare i Principal, il gruppo di amministrazione federated-group/admin e il gruppo finanziario federated-group/finance, Autorizzazioni per eseguire l'azione s3:ListBucket sul bucket denominato mybucket E l'azione s3:GetObject su tutti gli oggetti all'interno del bucket.

```
{
  "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:iam:s3::mybucket",
        "arn:aws:iam:s3::mybucket/*"
      ]
    }
  ]
}
```

Il criterio bucket ha un limite di dimensione di 20,480 byte e il criterio di gruppo ha un limite di dimensione di 5,120 byte.

### Impostazioni di controllo della coerenza per i criteri

Per impostazione predefinita, gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Una volta che un criterio di gruppo diventa coerente, le modifiche possono richiedere altri 15 minuti per essere effettive, a causa del caching delle policy. Per impostazione predefinita, anche gli aggiornamenti apportati alle policy del bucket sono coerenti.

Come richiesto, è possibile modificare le garanzie di coerenza per gli aggiornamenti delle policy bucket. Ad

esempio, è possibile che una modifica a una policy bucket diventi effettiva il prima possibile per motivi di sicurezza.

In questo caso, è possibile impostare `Consistency-Control` Nella richiesta di policy PUT bucket, oppure puoi utilizzare la richiesta DI coerenza PUT bucket. Quando si modifica il controllo di coerenza per questa richiesta, è necessario utilizzare il valore **all**, che fornisce la massima garanzia di coerenza di lettura dopo scrittura. Se si specifica qualsiasi altro valore di controllo di coerenza in un'intestazione per la richiesta di coerenza PUT bucket, la richiesta verrà rifiutata. Se si specifica qualsiasi altro valore per una richiesta di policy PUT bucket, il valore verrà ignorato. Una volta che una policy bucket diventa coerente, le modifiche possono richiedere altri 8 secondi per essere effettive, a causa del caching delle policy.



Se si imposta il livello di coerenza su **tutto** per forzare l'entrata in vigore di una nuova policy di bucket, assicurarsi di ripristinare il valore originale del controllo a livello di bucket al termine dell'operazione. In caso contrario, tutte le future richieste di bucket utilizzeranno l'impostazione **all**.

### Utilizzare ARN nelle dichiarazioni delle policy

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

- Utilizzare questa sintassi per specificare la risorsa S3 ARN:

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

- Utilizzare questa sintassi per specificare l'ARN della risorsa di 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 far corrispondere zero o più caratteri all'interno della chiave oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave oggetto, devono essere codificati utilizzando JSON UTF-8 o le sequenze di escape JSON. La codifica in percentuale non è supportata.

["Sintassi URN RFC 2141"](#)

Il corpo della richiesta HTTP per l'operazione del criterio PUT bucket deve essere codificato con `charset=UTF-8`.

### Specificare le risorse in un criterio

Nelle istruzioni policy, è possibile utilizzare l'elemento Resource per specificare il bucket o l'oggetto per cui le



autorizzazioni sono consentite o negate.

- Ogni dichiarazione di policy richiede un elemento Resource. In un criterio, le risorse sono indicate dall'elemento Resource, o in alternativa, NotResource per l'esclusione.
- Specificare le risorse con un ARN di risorsa S3. Ad esempio:

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

- È inoltre possibile utilizzare le variabili dei criteri all'interno della chiave a oggetti. Ad esempio:

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

- Il valore della risorsa può specificare un bucket che non esiste ancora quando viene creata una policy di gruppo.

### Specificare le entità in un criterio

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

- Ogni dichiarazione di policy in una policy bucket deve includere un elemento Principal. Le dichiarazioni di policy in una policy di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In un criterio, le entità sono indicate dall'elemento "Principal," o in alternativa "NotPrincipal" 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 dell'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 uno specifico gruppo federated ("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 utente invece del 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 cancellato. Se un nuovo Alex entra a far parte dell'organizzazione e viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe ereditare involontariamente le autorizzazioni concesse all'utente originale.

- Il valore principale può specificare un nome utente/gruppo che non esiste ancora quando viene creata una policy bucket.

## Specificare le autorizzazioni in un criterio

In un criterio, l'elemento Action viene utilizzato per consentire/negare le autorizzazioni a una risorsa. È possibile specificare una serie di autorizzazioni in un criterio, indicate dall'elemento "Action" o, in alternativa, "NotAction" per l'esclusione. Ciascuno di questi elementi viene associato a specifiche operazioni REST API S3.

Le tabelle elencano le autorizzazioni applicabili ai bucket e le autorizzazioni applicabili agli oggetti.



Amazon S3 ora utilizza l'autorizzazione `s3:PutReplicationConfiguration` per le azioni di replica PUT e DELETE bucket. StorageGRID utilizza autorizzazioni separate per ciascuna azione, che corrispondono alla specifica originale di Amazon S3.



L'ELIMINAZIONE viene eseguita quando si utilizza UN PUT per sovrascrivere un valore esistente.

## Autorizzazioni applicabili ai bucket

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:CreateBucket	METTI bucket	
s3:Deletebucket	ELIMINA bucket	
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione di notifica dei metadati del bucket	Sì
s3:DeleteBucketPolicy	ELIMINA policy bucket	
s3:DeleteReplicationConfiguration	ELIMINA replica bucket	Sì, separare i permessi per PUT ed DELETE*
s3:GetBucketAcl	OTTIENI ACL bucket	
s3:GetBucketCompliance	OTTIENI compliance bucket (obsoleta)	Sì
s3:GetBucketConsistency	COERENZA del bucket	Sì
s3:GetBucketCORS	OTTIENI bucket cors	
s3:GetEncryptionConfiguration	OTTIENI la crittografia bucket	
s3:GetBucketLastAccessTime	OTTIENI l'ultimo tempo di accesso a bucket	Sì
s3:GetBucketLocation	OTTIENI posizione bucket	
s3:GetBucketMetadataNotification	OTTIENI la configurazione della notifica dei metadati del bucket	Sì
s3:GetBucketNotification	OTTIENI notifica bucket	
s3:GetBucketObjectLockConfiguration	OTTIENI configurazione blocco oggetto	
s3:GetBucketPolicy	OTTIENI la policy bucket	
s3:GetBucketTagging	OTTIENI il contrassegno bucket	
s3:GetBucketVersioning	SCARICA la versione di bucket	
s3:GetLifecycleConfiguration	OTTIENI il ciclo di vita del bucket	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetReplicationConfiguration	OTTIENI la replica bucket	
s3:ListAllMyBucket	<ul style="list-style-type: none"> <li>• OTTIENI assistenza</li> <li>• OTTIENI l'utilizzo dello storage</li> </ul>	Sì, per OTTENERE l'utilizzo dello storage
s3:ListBucket	<ul style="list-style-type: none"> <li>• OTTIENI bucket (Elenca oggetti)</li> <li>• BENNA PER LA TESTA</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3:ListBucketMultipartUploads	<ul style="list-style-type: none"> <li>• Elenca caricamenti multiparte</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3:ListBucketVersions	SCARICA le versioni di bucket	
s3:PutBucketCompliance	METTERE la compliance del bucket (obsoleta)	Sì
s3:PutBucketConsistency	METTI la coerenza del bucket	Sì
s3:PutBucketCORS	<ul style="list-style-type: none"> <li>• DELETE Bucket cors† (ELIMINA cors bucket)</li> <li>• METTI cors bucket</li> </ul>	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> <li>• ELIMINA crittografia bucket</li> <li>• METTI la crittografia bucket</li> </ul>	
s3:PutBucketLastAccessTime	TEMPO ULTIMO accesso bucket	Sì
s3:PutBucketMetadataNotification	INSERIRE la configurazione della notifica dei metadati del bucket	Sì
s3:PutBucketNotification	NOTIFICA DEL bucket	
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> <li>• POSIZIONARE la benna con <code>x-amz-bucket-object-lock-enabled: true</code> Intestazione della richiesta (richiede anche l'autorizzazione <code>s3:CreateBucket</code>)</li> <li>• PUT Object Lock Configuration (CONFIGURAZIONE blocco oggetto)</li> </ul>	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutBucketPolicy	METTI la policy bucket	
s3:PutBucketTagging	<ul style="list-style-type: none"> <li>• ELIMINA contrassegno bucket†</li> <li>• INSERIRE il contrassegno bucket</li> </ul>	
s3:PutBucketVersioning	METTERE il bucket in versione	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> <li>• ELIMINA ciclo di vita bucket†</li> <li>• METTI IL ciclo di vita del bucket</li> </ul>	
s3:PutReplicationConfiguration	METTI la replica del bucket	Sì, separare i permessi per PUT ed DELETE*

#### Autorizzazioni applicabili agli oggetti

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> <li>• Interrompi caricamento multiparte</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3:BypassGovernanceRetention	<ul style="list-style-type: none"> <li>• ELIMINA oggetto</li> <li>• ELIMINARE più oggetti</li> <li>• METTI la conservazione degli oggetti</li> </ul>	
s3>DeleteObject	<ul style="list-style-type: none"> <li>• ELIMINA oggetto</li> <li>• ELIMINARE più oggetti</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3>DeleteObjectTagging	ELIMINA tag oggetti	
s3>DeleteObjectVersionTagging	DELETE Object Tagging (ELIMINA tag oggetti) (una versione specifica dell'oggetto)	
s3>DeleteObjectVersion	DELETE Object (UNA versione specifica dell'oggetto)	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetObject	<ul style="list-style-type: none"> <li>• OTTIENI oggetto</li> <li>• Oggetto TESTA</li> <li>• RIPRISTINO POST-oggetto</li> <li>• SELEZIONARE il contenuto dell'oggetto</li> </ul>	
s3:GetObjectAcl	GET Object ACL (OTTIENI ACL oggetto)	
s3:GetObjectLegalHold	OTTENERE un blocco legale degli oggetti	
s3:GetObjectRetention	OTTIENI la conservazione degli oggetti	
s3:GetObjectTagging	OTTIENI tag oggetti	
s3:GetObjectVersionTagging	GET Object Tagging (OTTIENI tag oggetti) (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GET Object (UNA versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	List Parts, POST-ripristino degli oggetti	
s3:PutObject	<ul style="list-style-type: none"> <li>• METTI oggetto</li> <li>• METTI oggetto - Copia</li> <li>• RIPRISTINO POST-oggetto</li> <li>• Avvia caricamento multiparte</li> <li>• Caricamento multiparte completo</li> <li>• Carica parte</li> <li>• Carica parte - Copia</li> </ul>	
s3:PutObjectLegalHold	METTERE in attesa legale l'oggetto	
s3:PutObjectRetention	METTI la conservazione degli oggetti	
s3:PutObjectTagging	INSERIRE tag oggetti	
s3:PutObjectVersionTagging	PUT Object Tagging (UNA versione specifica dell'oggetto)	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutOverwriteObject	<ul style="list-style-type: none"> <li>• METTI oggetto</li> <li>• METTI oggetto - Copia</li> <li>• INSERIRE tag degli oggetti</li> <li>• ELIMINA tag oggetti</li> <li>• Caricamento multiparte completo</li> </ul>	Sì
s3:RestoreObject (Riavvia oggetto)	RIPRISTINO POST-oggetto	

### Utilizza 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 impostazioni possibili per questa autorizzazione includono:

- **Allow:** Il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega:** Il client non può sovrascrivere un oggetto. Se impostata 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 il tag S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se la versione S3 è attivata, l'impostazione Nega impedisce alle operazioni DI TAGGING OGGETTI PUT o DELETE di modificare il TagSet per un oggetto e le relative 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 di se Allow è stato impostato.



Se il criterio S3 corrente 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 il tagging degli oggetti. Inoltre, se la casella di controllo **Impedisci modifica client** è selezionata (**CONFIGURAZIONE > Impostazioni di sicurezza > rete e oggetti**), tale impostazione sovrascrive l'impostazione dell'autorizzazione PutOverwriteObject.

### Specificare le condizioni in un criterio

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

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

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

Nell'esempio seguente, la condizione ipaddress utilizza la chiave SourceIp Condition.

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

### Operatori delle condizioni supportati

Gli operatori delle condizioni sono classificati come segue:

- Stringa
- Numerico
- Booleano
- Indirizzo IP
- Controllo nullo

Condizionare gli operatori	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole).
StringNotEquals	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora maiuscole/minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora maiuscole/minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole). Possono includere * e ? caratteri jolly.
StringNotLike	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). Possono includere * e ? caratteri jolly.



Condizionare gli operatori	Descrizione
Valori numerici Equals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericNotEquals	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericGreaterThan	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di".
NumericGreaterThanEquals	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a".
NumericLessThan	Confronta una chiave con un valore numerico in base alla corrispondenza "meno di".
NumericLessThanEquals	Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale a".
Bool	Confronta una chiave con un valore booleano in base alla corrispondenza "true o false".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NotIpAddress	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.
Null	Controlla se è presente una chiave di condizione nel contesto della richiesta corrente.

#### Chiavi di condizione supportate

Categoria	Chiavi di condizione applicabili	Descrizione
Operatori IP	aws: Sourcelp	<p>Viene confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti.</p> <p><b>Nota:</b> se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi Admin e Gateway, viene confrontato con l'indirizzo IP a monte del servizio Load Balancer.</p> <p><b>Nota:</b> Se si utilizza un bilanciamento del carico non trasparente di terze parti, questo viene confrontato con l'indirizzo IP del bilanciamento del carico. Qualsiasi X-Forwarded-For l'intestazione verrà ignorata perché la sua validità non può essere accertata.</p>
Risorsa/identità	aws:nome utente	Viene confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti.
s3:ListBucket e. s3:autorizzazioni ListBucketVersions	s3:delimitatore	Viene confrontato con il parametro delimitatore specificato in una richiesta GET bucket o GET Bucket Object Versions.
s3:ListBucket e. s3:autorizzazioni ListBucketVersions	s3: tasti max	Viene confrontato con il parametro max-keys specificato in una richiesta GET bucket o GET Bucket Object Versions.
s3:ListBucket e. s3:autorizzazioni ListBucketVersions	s3:prefisso	Viene confrontato con il parametro di prefisso specificato in una richiesta DI versioni DI oggetti GET Bucket o GET Bucket.
s3:PutObject	s3:giorni-rimanti- conservazione-blocco- oggetto	<p>Viene confrontato 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 rientrino nell'intervallo consentito per le seguenti richieste:</p> <ul style="list-style-type: none"> <li>• METTI oggetto</li> <li>• METTI oggetto - Copia</li> <li>• Avvia caricamento multiparte</li> </ul>

Categoria	Chiavi di condizione applicabili	Descrizione
s3:PutObjectRetention	s3:giorni-rimanenti-conservazione-blocco-oggetto	Viene confrontato con la data di conservazione fino alla data specificata nella richiesta DI conservazione degli oggetti PUT per garantire che rientri nell'intervallo consentito.

### Specificare le variabili in un criterio

È possibile utilizzare le variabili nei criteri per popolare le informazioni sui criteri quando sono disponibili. È possibile utilizzare le variabili dei criteri in `Resource` confronto tra elementi e stringhe in `Condition` elemento.

In questo esempio, la variabile `${aws:username}` Fa parte dell'elemento `Resource`:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore della condizione nel blocco `condition`:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variabile	Descrizione
<code>\${aws:SourceIp}</code>	Utilizza la chiave <code>SourceIp</code> come variabile fornita.
<code>\${aws:username}</code>	Utilizza la chiave <code>Username</code> come variabile fornita.
<code>\${s3:prefix}</code>	Utilizza la chiave di prefisso specifica del servizio come variabile fornita.
<code>\${s3:max-keys}</code>	Utilizza la chiave <code>max-keys</code> specifica del servizio come variabile fornita.
<code>\${*}</code>	Carattere speciale. Utilizza il carattere come carattere <code>*</code> letterale.
<code>\${?}</code>	Carattere speciale. Utilizza il carattere come letterale <code>?</code> carattere.
<code>\${\$}</code>	Carattere speciale. Utilizza il carattere come carattere letterale.

## Creare policy che richiedono una gestione speciale

A volte un criterio può concedere autorizzazioni pericolose per la sicurezza o pericolose per operazioni continue, come il blocco dell'utente root dell'account. L'implementazione dell'API REST di StorageGRID S3 è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Negare automaticamente le autorizzazioni all'account root	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Negare automaticamente le autorizzazioni all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consenti a un gruppo di account esterno qualsiasi autorizzazione	Bucket	Principal non valido	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio
Consentire a un account root esterno o a un utente qualsiasi autorizzazione	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio	Stesso
Consenti a tutti i permessi per tutte le azioni	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) per l'account root esterno e gli utenti	Stesso
Negare a Everyone le autorizzazioni per tutte le azioni	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Principal è un utente o un gruppo inesistente	Bucket	Principal non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Bucket	Principal non valido	Valido
La policy concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni PER INSERIRE gli oggetti	Bucket	Valido. Gli oggetti sono di proprietà dell'account creatore e la policy bucket non si applica. L'account creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL a oggetti.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la policy 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. I bucket WORM vengono configurati in modo da consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione del contenuto esistente. Utilizzare uno degli approcci descritti di seguito.

Per garantire che le sovrascritture vengano sempre negate, è possibile:

- Da Grid Manager, selezionare **CONFIGURATION > Security > Security settings > Network and Objects**, quindi selezionare la casella di controllo **Impedisci modifica client**.
- Applicare le seguenti regole e criteri S3:
  - Aggiungere un'operazione di NEGAZIONE PutOverwriteObject al criterio S3.
  - Aggiungere un'operazione di NEGAZIONE DeleteObject al criterio S3.
  - Aggiungere un'operazione PUT object ALLOW al criterio S3.



L'impostazione di DeleteObject per NEGARE in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".



Anche quando tutte queste regole e policy vengono applicate, non si proteggono dalle scritture simultanee (vedi situazione A). Si 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 (con protezione)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

### Informazioni correlate

- ["Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"](#)
- ["Esempio di policy bucket"](#)
- ["Criteri di gruppo di esempio"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Utilizzare un account tenant"](#)

## Esempio di policy bucket

Utilizza gli esempi di questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri del bucket specificano le autorizzazioni di accesso per il bucket a cui è associata la policy. I criteri del bucket vengono configurati utilizzando l'API S3 PutBucketPolicy. Vedere ["Operazioni sui bucket"](#).

È possibile configurare un criterio bucket utilizzando l'interfaccia CLI AWS seguendo il seguente comando:

```
> 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, Everyone, incluso l'anonimo, è autorizzato a elencare gli oggetti nel bucket ed eseguire operazioni Get Object su tutti gli oggetti nel bucket. Tutte le altre operazioni verranno negate. Si noti che questo criterio potrebbe non essere particolarmente utile perché nessuno, ad eccezione dell'account root, dispone delle autorizzazioni di scrittura 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 elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket che iniziano con `shared/` prefisso chiave oggetto.



In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. La policy bucket si applica a questi oggetti.

```

{
  "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 per gruppo specificato**

In questo esempio, chiunque, incluso anonimo, può elencare il bucket ed eseguire operazioni GET Object su tutti gli oggetti nel bucket, mentre solo gli utenti appartengono 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 si trova nell'intervallo IP**

In questo esempio, Everyone, incluso l'anonimato, è autorizzato a elencare il bucket ed eseguire qualsiasi operazione oggetto 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 rifiutate e tutte le richieste al di fuori dell'intervallo IP verranno rifiutate.

```

{
  "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 da un utente federato specificato**

In questo esempio, all'utente federato Alex è consentito l'accesso completo a `examplebucket` bucket e i suoi oggetti. A tutti gli altri utenti, tra cui 'root', vengono esplicitamente negate tutte le operazioni. Si noti tuttavia che a 'root' non vengono mai negate le autorizzazioni 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 Effect` per `PutOverwriteObject` e `DeleteObject` garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging degli oggetti 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 di 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 nel criterio perché è implicito. I criteri di gruppo vengono configurati utilizzando il tenant Manager o l'API.

## Esempio: Impostare i criteri di gruppo utilizzando Tenant Manager

Quando si aggiunge o si modifica un gruppo in Tenant Manager, è possibile selezionare una policy 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 sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
- **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 gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile 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 ad accesso completo. Impossibile modificare questa stringa.
- **Ransomware Mitigation:** 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 in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti.

Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.

- **Personalizzato:** Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

## Esempio: Consentire l'accesso completo del gruppo 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 sia esplicitamente negato dalla policy bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

## Esempio: Consentire l'accesso di gruppo 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 sia esplicitamente negato dalla policy del bucket. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag.

```

{
  "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 di accedere completamente solo alla “cartella” in un bucket**

In questo esempio, i membri del gruppo possono solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.

```
{
  "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}/*"
    }
  ]
}
```

## Configurare la sicurezza per l'API REST

È necessario esaminare le misure di sicurezza implementate per L'API REST e comprendere come proteggere il sistema.

### In che modo StorageGRID fornisce la sicurezza per l'API REST

È necessario comprendere in che modo il sistema StorageGRID implementa la sicurezza, l'autenticazione e l'autorizzazione per l'API REST.

StorageGRID utilizza le seguenti misure di sicurezza.

- Le comunicazioni del client con il servizio Load Balancer utilizzano HTTPS se HTTPS è configurato per l'endpoint del bilanciamento del carico.

Quando si configura un endpoint di bilanciamento del carico, è possibile attivare HTTP. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

- Per impostazione predefinita, StorageGRID utilizza HTTPS per le comunicazioni client con i nodi di storage.

È possibile abilitare HTTP per queste connessioni. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire le intestazioni di autenticazione HTTP a StorageGRID per eseguire operazioni REST API.

## Certificati di sicurezza e applicazioni client

I client possono connettersi al servizio Load Balancer sui nodi Gateway o sui nodi Admin, direttamente ai nodi Storage.

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint specifico del bilanciamento del carico utilizzato per stabilire la connessione. Ogni endpoint dispone di un proprio certificato, ovvero un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.
- Quando le applicazioni client si connettono direttamente a un nodo di storage, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia.

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

Consultare le istruzioni per l'amministrazione di StorageGRID per informazioni sulla configurazione degli endpoint del bilanciamento del carico e per istruzioni sull'aggiunta di un singolo certificato server personalizzato per le connessioni TLS direttamente ai nodi di storage.

## Riepilogo

La seguente tabella mostra come vengono implementati i problemi di sicurezza nelle API S3 e Swift REST:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore
Autenticazione del client	<ul style="list-style-type: none"> <li>• S3: Account S3 (ID chiave di accesso e chiave di accesso segreta)</li> <li>• Swift: Account Swift (nome utente e password)</li> </ul>
Autorizzazione del client	<ul style="list-style-type: none"> <li>• S3: Proprietà del bucket e tutte le policy di controllo degli accessi applicabili</li> <li>• Swift: Accesso al ruolo di amministratore</li> </ul>



## Informazioni correlate

["Amministrare StorageGRID"](#)

## Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un set limitato di suite di crittografia che le applicazioni client possono utilizzare quando si stabilisce una sessione TLS (Transport Layer Security). Per configurare la crittografia, andare a **CONFIGURATION > Security > Security settings** e selezionare **TLS and SSH policy**.

### Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.



SSLv3 e TLS 1.1 (o versioni precedenti) non sono più supportati.

## Informazioni correlate

["Configurare gli account e le connessioni del tenant"](#)

## Monitorare e controllare le operazioni

### Monitorare le velocità di acquisizione e recupero degli oggetti

È possibile monitorare i tassi di acquisizione e recupero degli oggetti, nonché le metriche per i conteggi degli oggetti, le query e la verifica. È possibile visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di lettura, scrittura e modifica degli oggetti nel sistema StorageGRID.

#### Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Nella dashboard, selezionare **Performance > S3 Operations** o **Performance > Swift Operations**.

In questa sezione viene riepilogato il numero di operazioni client eseguite dal sistema StorageGRID. Le velocità dei protocolli vengono calcolate in media negli ultimi due minuti.

3. Selezionare **NODI**.
4. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **Load Balancer**.

I grafici mostrano i trend di tutto il traffico client diretto agli endpoint del bilanciamento del carico all'interno della griglia. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

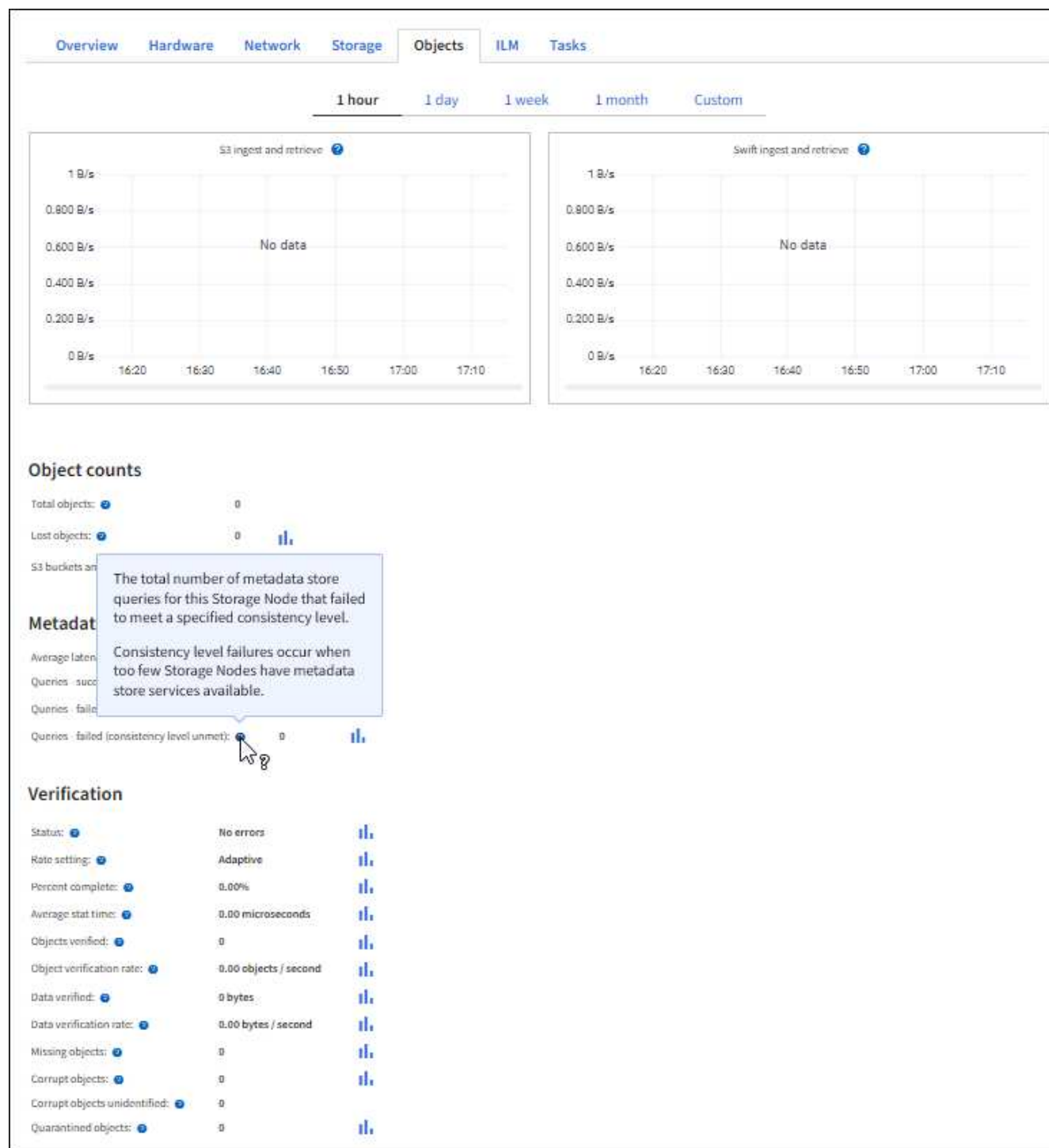
5. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero dell'intero sistema StorageGRID in byte al secondo e byte totali. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

6. Per visualizzare le informazioni relative a un nodo di storage specifico, selezionarlo dall'elenco a sinistra e fare clic sulla scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero degli oggetti per questo nodo di storage. La scheda

include anche metriche per il conteggio degli oggetti, le query e la verifica. È possibile fare clic sulle etichette per visualizzare le definizioni di queste metriche.



7. Se desideri ulteriori dettagli:

- Selezionare **SUPPORT > Tools > Grid topology**.
- Selezionare **Site > Overview > Main**.

La sezione API Operations (operazioni API) visualizza informazioni riepilogative per l'intera griglia.

- Selezionare **Storage Node > LDR > client application > Overview > Main**

La sezione Operations (operazioni) visualizza informazioni riepilogative per il nodo di storage selezionato.

## Accesso e revisione dei registri di audit

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. I messaggi di audit specifici delle API nei registri di audit forniscono dati critici di sicurezza, funzionamento e monitoraggio delle performance che possono aiutare a valutare lo stato di salute del sistema.

### Prima di iniziare

- Si dispone di autorizzazioni di accesso specifiche.
- Hai il `Passwords.txt` file.
- Si conosce l'indirizzo IP di un nodo amministratore.

### A proposito di questa attività

Il file di log di audit attivo viene denominato `audit.log` e viene memorizzato nei nodi di amministrazione.

Una volta al giorno, il file `audit.log` attivo viene salvato e viene visualizzato un nuovo file `audit.log` il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato `yyyy-mm-dd.txt.gz`, che conserva la data originale.

In questo esempio viene visualizzato il valore attivo `audit.log` file del giorno precedente (2018-04-15.txt) e il file compresso per il giorno precedente (2018-04-14.txt.gz).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

### Fasi

1. Accedere a un nodo amministratore:
  - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
  - b. Immettere la password elencata in `Passwords.txt` file.
  - c. Immettere il seguente comando per passare a root: `su -`
  - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Accedere alla directory contenente i file di log di controllo:

```
cd /var/local/audit/export
```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

## Operazioni S3 registrate nei registri di audit

Nei registri di audit di StorageGRID vengono registrate diverse operazioni bucket e operazioni a oggetti.

### Operazioni bucket registrate nei registri di audit

- ELIMINA bucket
- ELIMINA tag bucket
- ELIMINARE più oggetti
- OTTIENI bucket (Elenca oggetti)
- SCARICA le versioni degli oggetti bucket
- OTTIENI il contrassegno bucket
- BENNA PER LA TESTA
- METTI bucket
- METTI la compliance del bucket
- INSERIRE il contrassegno bucket
- METTERE il bucket in versione

### Operazioni a oggetti registrate nei registri di audit

- Caricamento multiparte completo
- Parte di caricamento (quando la regola ILM utilizza comportamenti di acquisizione bilanciati o rigorosi)
- Parte di caricamento - Copia (quando la regola ILM utilizza comportamenti di acquisizione rigorosi o bilanciati)
- ELIMINA oggetto
- OTTIENI oggetto
- Oggetto TESTA
- RIPRISTINO POST-oggetto
- METTI oggetto
- METTI oggetto - Copia

### Informazioni correlate

["Operazioni sui bucket"](#)

["Operazioni sugli oggetti"](#)

## Vantaggi delle connessioni HTTP attive, inattive e simultanee

La modalità di configurazione delle connessioni HTTP può influire sulle prestazioni del sistema StorageGRID. Le configurazioni variano a seconda che la connessione HTTP sia attiva o inattiva o che si dispongano di più connessioni simultanee.

È possibile identificare i vantaggi in termini di prestazioni per i seguenti tipi di connessioni HTTP:

- Connessioni HTTP inattive
- Connessioni HTTP attive
- Connessioni HTTP simultanee

## **I vantaggi di mantenere aperte le connessioni HTTP inattive**

È necessario mantenere aperte le connessioni HTTP anche quando le applicazioni client sono inattive per consentire alle applicazioni client di eseguire transazioni successive sulla connessione aperta. In base alle misurazioni del sistema e all'esperienza di integrazione, è necessario mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP che rimane aperta e inattiva per più di 10 minuti.

Le connessioni HTTP aperte e inattive offrono i seguenti vantaggi:

- Latenza ridotta dal momento in cui il sistema StorageGRID stabilisce di eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

La latenza ridotta è il vantaggio principale, in particolare per il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dei dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con i trasferimenti eseguiti in precedenza
- Notifica istantanea di diverse classi di condizioni di errore che interrompono la connettività tra l'applicazione client e il sistema StorageGRID

Determinare per quanto tempo mantenere aperta una connessione inattiva è un compromesso-tra i benefici dell'avvio lento associati alla connessione esistente e l'allocazione ideale della connessione alle risorse di sistema interne.

## **Vantaggi delle connessioni HTTP attive**

Per le connessioni dirette ai nodi di storage, è necessario limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

La determinazione della durata massima per-cui una connessione deve essere mantenuta aperta è un compromesso tra i benefici della persistenza della connessione e l'allocazione ideale della connessione alle risorse di sistema interne.

Per le connessioni client ai nodi di storage, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID.

Con il passare del tempo, una connessione HTTP potrebbe non essere più ottimale con il variare dei requisiti di bilanciamento del carico. Il sistema esegue il miglior bilanciamento del carico quando le applicazioni client stabiliscono una connessione HTTP separata per ciascuna transazione, ma questo nega i guadagni molto più preziosi associati alle connessioni persistenti.

- Consente alle applicazioni client di indirizzare le transazioni HTTP ai servizi LDR che dispongono di spazio disponibile.
- Consente l'avvio delle procedure di manutenzione.

Alcune procedure di manutenzione vengono avviate solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, la limitazione della durata delle connessioni aperte può essere utile per consentire l'avvio tempestivo di alcune procedure di manutenzione. Se la durata delle connessioni client non è limitata, potrebbero essere necessari alcuni minuti per terminare automaticamente le connessioni attive.

## **Vantaggi delle connessioni HTTP simultanee**

Tenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, aumentando così le performance. Il numero ottimale di connessioni parallele dipende da diversi fattori.

Le connessioni HTTP simultanee offrono i seguenti vantaggi:

- Latenza ridotta

Le transazioni possono iniziare immediatamente invece di attendere il completamento di altre transazioni.

- Maggiore throughput

Il sistema StorageGRID può eseguire transazioni parallele e aumentare il throughput delle transazioni aggregate.

Le applicazioni client devono stabilire più connessioni HTTP. Quando un'applicazione client deve eseguire una transazione, può selezionare e utilizzare immediatamente qualsiasi connessione stabilita che non sta elaborando una transazione.

La topologia di ciascun sistema StorageGRID presenta un throughput di picco diverso per le transazioni e le connessioni simultanee prima che le performance comincino a degradarsi. Il throughput massimo dipende da fattori quali risorse di calcolo, risorse di rete, risorse di storage e collegamenti WAN. Anche il numero di server e servizi e il numero di applicazioni supportate dal sistema StorageGRID sono fattori.

I sistemi StorageGRID spesso supportano più applicazioni client. Tenere presente questo aspetto quando si determina il numero massimo di connessioni simultanee utilizzate da un'applicazione client. Se l'applicazione client è costituita da più entità software che stabiliscono connessioni al sistema StorageGRID, è necessario sommare tutte le connessioni tra le entità. Potrebbe essere necessario regolare il numero massimo di connessioni simultanee nelle seguenti situazioni:

- La topologia del sistema StorageGRID influisce sul numero massimo di transazioni e connessioni simultanee supportate dal sistema.
- Le applicazioni client che interagiscono con il sistema StorageGRID su una rete con larghezza di banda limitata potrebbero dover ridurre il grado di concorrenza per garantire che le singole transazioni vengano completate in un tempo ragionevole.
- Quando molte applicazioni client condividono il sistema StorageGRID, potrebbe essere necessario ridurre il grado di concorrenza per evitare di superare i limiti del sistema.

## **Separazione dei pool di connessione HTTP per le operazioni di lettura e scrittura**

È possibile utilizzare pool separati di connessioni HTTP per le operazioni di lettura e scrittura e controllare la quantità di un pool da utilizzare per ciascuno di essi. I pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi dominanti dal recupero (lettura) o dominanti dal negozio (scrittura). Con pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile regolare la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.