



Operazioni personalizzate di StorageGRID

StorageGRID software

NetApp
July 23, 2026

Sommario

Operazioni personalizzate di StorageGRID	1
Operazioni personalizzate sui bucket supportate in StorageGRID	1
Recupera il livello di coerenza del bucket in StorageGRID con la richiesta GET Bucket consistency	2
Esempio di richiesta	2
Risposta	2
Esempio di risposta	2
Specificare i livelli di consistenza in StorageGRID con la richiesta PUT Bucket consistency	3
Richiesta	3
Esempio di richiesta	4
Recupera lo stato dell'ultimo accesso al bucket in StorageGRID con la richiesta GET Bucket last access time	4
Esempio di richiesta	4
Esempio di risposta	4
Abilita e disabilita gli aggiornamenti dell'ora dell'ultimo accesso in StorageGRID con la richiesta PUT Bucket last access time	5
Esempi di richieste	6
Disabilitare il servizio di integrazione della ricerca con la richiesta di configurazione della notifica dei metadati DELETE Bucket in StorageGRID	6
Esempio di richiesta	6
Configura l'integrazione della ricerca in StorageGRID con la richiesta di configurazione della notifica dei metadati del bucket GET	7
Esempio di richiesta	7
Risposta	7
Esempio di risposta	9
Abilita il servizio di integrazione della ricerca in StorageGRID con la richiesta di configurazione della notifica dei metadati del bucket PUT	10
Richiesta	10
Esempi di richieste	12
JSON generato dal servizio di integrazione della ricerca	14
Metadati degli oggetti inclusi nelle notifiche dei metadati	15
Recupera l'utilizzo dello storage dell'account e del bucket in StorageGRID con la richiesta GET Storage Usage	16
Esempio di richiesta	16
Esempio di risposta	16
Versioning	17
`\${post_edited_translations.segment}`	17
Richieste di bucket deprecated per la Compliance StorageGRID legacy	17
Elemento SGCompliance obsoleto in StorageGRID	18
Richiesta GET Bucket compliance obsoleta in StorageGRID	19
Richiesta PUT Bucket compliance obsoleta in StorageGRID	20

Operazioni personalizzate di StorageGRID

Operazioni personalizzate sui bucket supportate in StorageGRID

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

La tabella seguente elenca le operazioni personalizzate supportate da StorageGRID.

Operazione	Descrizione
"Coerenza GET Bucket"	Restituisce la coerenza applicata a un determinato bucket.
"Coerenza PUT Bucket"	Imposta la coerenza applicata a un determinato bucket.
"Ora dell'ultimo accesso GET Bucket"	Restituisce se gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati o disabilitati per un determinato bucket.
"Ora dell'ultimo accesso PUT Bucket"	Ti permette di abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso per un determinato bucket.
"ELIMINA la configurazione della notifica dei metadati del bucket"	Elimina il file XML di configurazione della notifica dei metadati associato a un bucket specifico.
"GET Configurazione della notifica dei metadati del bucket"	Restituisce il file XML di configurazione della notifica dei metadati associato a un determinato bucket.
"Configurazione della notifica dei metadati del bucket PUT"	Configura il servizio di notifica dei metadati per un bucket.
"Ottieni l'utilizzo dello storage"	Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ogni bucket associato all'account.
"Obsoleto: CreateBucket con impostazioni di conformità"	Obsoleto e non supportato: non puoi più creare nuovi bucket con la Compliance abilitata.
"Obsoleto: GET Bucket compliance"	Obsoleto ma supportato: restituisce le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente.
"Obsoleto: PUT Bucket compliance"	Obsoleto ma supportato: ti permette di modificare le impostazioni di conformità per un bucket Compliant legacy esistente.

Recupera il livello di coerenza del bucket in StorageGRID con la richiesta GET Bucket consistency

La richiesta GET Bucket consistency ti permette di determinare la coerenza applicata a uno specifico bucket.

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

Devi avere l'autorizzazione s3:GetBucketConsistency, oppure essere l'utente root, per completare questa operazione.

Esempio di richiesta

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

Risposta

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

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, oppure la richiesta non andrà a buon fine.
forte globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client su tutti i siti.
strong-site	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo una nuova scrittura	(Predefinito) Garantisce la coerenza di lettura dopo la scrittura per i nuovi oggetti e la coerenza finale per gli aggiornamenti degli oggetti. Offre elevata disponibilità e garanzie di protezione dei dati. Consigliato nella maggior parte dei casi.
disponibile	Garantisce la coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, usalo solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi 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

["Coerenza"](#)

Specificare i livelli di consistenza in StorageGRID con la richiesta PUT Bucket consistency

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

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

Prima di iniziare

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

Richiesta

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

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, oppure la richiesta non andrà a buon fine.
forte globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client su tutti i siti.
strong-site	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo una nuova scrittura	(Predefinito) Garantisce la coerenza di lettura dopo la scrittura per i nuovi oggetti e la coerenza finale per gli aggiornamenti degli oggetti. Offre elevata disponibilità e garanzie di protezione dei dati. Consigliato nella maggior parte dei casi.

Coerenza	Descrizione
disponibile	Garantisce la coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, usalo solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Nota: In generale, dovresti usare la coerenza "Read-after-new-write". Se le richieste non funzionano correttamente, cambia il comportamento del client dell'applicazione se possibile. Oppure, configura il client per specificare la coerenza per ogni richiesta API. Imposta la 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

["Coerenza"](#)

Recupera lo stato dell'ultimo accesso al bucket in StorageGRID con la richiesta GET Bucket last access time

La richiesta GET dell'ora dell'ultimo accesso al bucket ti permette di determinare se gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket.

Devi avere l'autorizzazione s3:GetBucketLastAccessTime, oppure essere l'utente root, per completare questa operazione.

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 aggiornamenti dell'ora dell'ultimo accesso sono abilitati per il bucket.

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

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

Abilita e disabilita gli aggiornamenti dell'ora dell'ultimo accesso in StorageGRID con la richiesta PUT Bucket last access time

La richiesta PUT Bucket last access time consente di abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso per i singoli bucket. La disabilitazione degli aggiornamenti dell'ora dell'ultimo accesso migliora le prestazioni ed è l'impostazione predefinita per tutti i bucket creati con la versione 10.3.0 o successive.

Devi avere l'autorizzazione `s3:PutBucketLastAccessTime` per un bucket, oppure essere account root, per completare questa operazione.



A partire dalla versione 10.3 di StorageGRID, gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per impostazione predefinita per tutti i nuovi bucket. Se hai bucket creati con una versione precedente di StorageGRID e vuoi che corrispondano al nuovo comportamento predefinito, devi disabilitare esplicitamente gli aggiornamenti all'ora dell'ultimo accesso per ciascuno di questi bucket precedenti. Puoi abilitare o disabilitare gli aggiornamenti all'ora dell'ultimo accesso utilizzando la richiesta PUT Bucket last access time o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedi ["Attiva o disattiva gli aggiornamenti dell'ora dell'ultimo accesso"](#).

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

- `GetObject`, `GetObjectAcl`, `GetObjectTagging` e `HeadObject` non aggiornano l'ora dell'ultimo accesso. L'oggetto non viene aggiunto alle code per la valutazione della gestione del ciclo di vita delle informazioni (ILM).
- `CopyObject` e `PutObjectTagging` richieste che aggiornano solo i metadati aggiornano anche l'ora dell'ultimo accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per il bucket di origine, le richieste `CopyObject` non aggiornano l'ora dell'ultimo accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM per il bucket di origine. Tuttavia, per la destinazione, le richieste `CopyObject` aggiornano sempre l'ora dell'ultimo accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.

- CompleteMultipartUpload aggiorna l'ora dell'ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

Esempi di richieste

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

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

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

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

Disabilitare il servizio di integrazione della ricerca con la richiesta di configurazione della notifica dei metadati DELETE Bucket in StorageGRID

La richiesta DELETE Bucket metadata notification configuration ti permette di disabilitare il servizio di integrazione della ricerca per singoli bucket eliminando il file XML di configurazione.

Devi avere l'autorizzazione s3:DeleteBucketMetadataNotification per un bucket, oppure essere account root, per completare questa operazione.

Esempio di richiesta

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

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

Configura l'integrazione della ricerca in StorageGRID con la richiesta di configurazione della notifica dei metadati del bucket GET

La richiesta GET Bucket metadata notification configuration consente di recuperare il file XML di configurazione utilizzato per configurare l'integrazione della ricerca per i singoli bucket.

Devi avere l'autorizzazione `s3:GetBucketMetadataNotification`, oppure essere l'utente `root`, per completare questa operazione.

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 ti permette di determinare come il bucket è configurato per l'integrazione con la ricerca. Cioè, ti permette di stabilire 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. Ciascuna regola specifica gli oggetti a cui

si applica e la destinazione a cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID.

Nome	Descrizione	Richiesto
MetadataNotificationConfiguration	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi Rule.	Sì
Regola	Etichetta contenitore 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	Identificativo univoco per la regola. Incluso nell'elemento Regola.	No
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Per le regole disabilitate non viene intrapresa alcuna azione. Incluso nell'elemento Regola.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per selezionare tutti gli oggetti, specifica un prefisso vuoto. Incluso nell'elemento Regola.	Sì
Destinazione	Etichetta contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	Sì

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

Esempio di risposta

Il codice XML incluso tra i

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tag mostra come è configurata l'integrazione con un endpoint di integrazione di ricerca per il bucket. In questo esempio, i metadati degli oggetti vengono inviati a un indice Elasticsearch denominato `current` e di tipo denominato `2017` che è ospitato in un dominio AWS denominato `records`.

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

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

Informazioni correlate

["Usa un tenant account"](#)

Abilita il servizio di integrazione della ricerca in StorageGRID con la richiesta di configurazione della notifica dei metadati del bucket PUT

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

Devi avere l'autorizzazione `s3:PutBucketMetadataNotification` per un bucket, oppure essere account root, per completare questa operazione.

Richiesta

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

Puoi filtrare gli oggetti in base al prefisso del nome dell'oggetto. Ad esempio, puoi inviare i metadati degli oggetti con il prefisso `/images` a una destinazione e quelli con il prefisso `/videos` a un'altra.

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

oggetti con il prefisso test2 non sarebbe consentita.

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

Nome	Descrizione	Richiesto
MetadataNotificationConfiguration	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi Rule.	Sì
Regola	Etichetta contenitore 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	Identificativo univoco per la regola. Incluso nell'elemento Regola.	No

Nome	Descrizione	Richiesto
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Per le regole disabilite non viene intrapresa alcuna azione. Incluso nell'elemento Regola.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per selezionare tutti gli oggetti, specifica un prefisso vuoto. Incluso nell'elemento Regola.	Sì
Destinazione	Etichetta contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	Sì
Urn	URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel formato <code>domain-name/myindex/mytype</code>. Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> L'endpoint deve essere configurato prima dell'invio del file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. Urn è incluso nell'elemento Destinazione.	Sì

Esempi di richieste

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

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

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

In questo esempio, i metadati degli oggetti che corrispondono al prefisso `/images` vengono inviati a una destinazione, mentre i metadati degli oggetti che corrispondono al prefisso `/videos` vengono inviati 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 abiliti il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato alla destinazione ogni volta che i metadati o i tag di un oggetto vengono aggiunti, aggiornati o eliminati.

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

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

Metadati degli oggetti inclusi nelle notifiche dei metadati

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando l'integrazione della ricerca è abilitata.

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

Tipo	Nome articolo	Descrizione
Informazioni su bucket e oggetto	bucket	Nome del bucket
Informazioni su bucket e oggetto	chiave	Nome chiave oggetto
Informazioni su bucket e oggetto	ID versione	Versione dell'oggetto, per gli oggetti in bucket con versioning
Informazioni su bucket e oggetto	regione	Regione del 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 dell'oggetto
Metadati utente	metadati <i>key:value</i>	Tutti i metadati utente per l'oggetto, come coppie chiave-valore
Etichette	tag <i>key:value</i>	Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore



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

Informazioni correlate

["Usa un tenant account"](#)

Recupera l'utilizzo dello storage dell'account e del bucket in StorageGRID con la richiesta GET Storage Usage

La richiesta GET Storage Usage ti dice la quantità totale di storage utilizzato da un account e per ogni bucket associato all'account.

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

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando la strong-global consistency. Se non è possibile raggiungere la strong-global consistency, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una strong-site consistency.

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

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 che contiene 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>
```

Versioning

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

Informazioni correlate

["Coerenza"](#)

`${post_edited_translations.segment}`

Richieste di bucket deprecate per la Compliance StorageGRID legacy

Potresti dover usare l'API REST S3 di StorageGRID per gestire i bucket creati con la funzionalità Compliance legacy.

Funzionalità di conformità deprecata

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

Se in precedenza avevi abilitato l'impostazione globale di Compliance, l'impostazione globale di S3 Object Lock è abilitata in StorageGRID 11.6. Non puoi più creare nuovi bucket con Compliance abilitato; tuttavia, se necessario, puoi usare la StorageGRID S3 REST API per gestire qualsiasi bucket Compliant legacy esistente.

- ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)
- ["Gestisci gli oggetti con ILM"](#)
- ["NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

Richieste di conformità obsolete:

- ["Obsoleto - Modifiche alla richiesta PUT Bucket per la conformità"](#)

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

- ["Obsoleto - GET Bucket compliance"](#)

La richiesta GET Bucket compliance è obsoleta. Tuttavia, puoi continuare a usare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente.

- ["Obsoleto - PUT Bucket compliance"](#)

La richiesta di conformità PUT Bucket è obsoleta. Tuttavia, puoi continuare a utilizzarla per modificare le impostazioni di conformità di un bucket Compliant legacy esistente. Ad esempio, puoi mettere un bucket esistente in legal hold o aumentarne il periodo di conservazione.

Elemento SGCompliance obsoleto in StorageGRID

L'elemento XML SGCompliance è obsoleto. In precedenza, potevi includere questo elemento personalizzato StorageGRID nel corpo facoltativo della richiesta XML di CreateBucket per creare un bucket conforme.



La funzionalità di conformità StorageGRID disponibile nelle versioni precedenti di StorageGRID è stata deprecata e sostituita da S3 Object Lock. Per maggiori dettagli, consulta quanto segue:

- ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)
- ["NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

Non puoi più creare nuovi bucket con la Compliance abilitata. Se provi a usare le modifiche alla richiesta CreateBucket per la compliance per creare un nuovo bucket Compliant, viene restituito il seguente messaggio di errore:

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

Richiesta GET Bucket compliance obsoleta in StorageGRID

La richiesta GET Bucket compliance è obsoleta. Tuttavia, puoi continuare a usare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente.



La funzionalità di conformità StorageGRID disponibile nelle versioni precedenti di StorageGRID è stata deprecata e sostituita da S3 Object Lock. Per maggiori dettagli, consulta quanto segue:

- ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)
- ["NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

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

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 conformità in vigore per il bucket. Questo esempio di risposta mostra le impostazioni di conformità per un bucket in cui ogni oggetto verrà conservato per un anno (525,600 minuti), a partire dal momento in cui l'oggetto viene inserito nella grid. Attualmente non è presente alcun blocco legale su questo bucket. Ogni oggetto verrà eliminato automaticamente 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 inserito nella grid.
LegalHold	• Vero: questo bucket è attualmente soggetto a un blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché il blocco legale non viene revocato, anche se il loro periodo di conservazione è scaduto. • Falso: questo bucket non è attualmente soggetto a un blocco legale. Gli oggetti in questo bucket possono essere eliminati quando il loro periodo di conservazione scade.
AutoDelete	• Vero: gli oggetti in questo bucket verranno eliminati automaticamente quando il loro periodo di conservazione scade, a meno che il bucket non sia soggetto a un blocco legale. • Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Devi eliminare manualmente questi oggetti se hai bisogno di eliminarli.

Risposte di errore

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

Richiesta PUT Bucket compliance obsoleta in StorageGRID

La richiesta di conformità PUT Bucket è obsoleta. Tuttavia, puoi continuare a utilizzarla per modificare le impostazioni di conformità di un bucket Compliant legacy esistente. Ad esempio, puoi mettere un bucket esistente in legal hold o aumentarne il periodo di conservazione.



La funzionalità di conformità StorageGRID disponibile nelle versioni precedenti di StorageGRID è stata deprecata e sostituita da S3 Object Lock. Per maggiori dettagli, consulta quanto segue:

- ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)
- ["NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5"](#)

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

Devi specificare un valore per ogni campo delle impostazioni di conformità quando invii una richiesta di conformità PUT Bucket.

Esempio di richiesta

Questa richiesta di esempio modifica le impostazioni di conformità per il bucket denominato `mybucket`. In questo esempio, gli oggetti in `mybucket` ora verranno conservati per due anni (1.051.200 minuti) invece di un

anno, a partire dal momento in cui l'oggetto viene inserito nella grid. Non c'è alcun blocco legale su questo bucket. Ogni oggetto verrà eliminato automaticamente 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	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella grid. Importante Quando specifichi un nuovo valore per RetentionPeriodMinutes, devi specificare un valore uguale o superiore all'attuale periodo di conservazione del bucket. Dopo che il periodo di conservazione del bucket è stato impostato, non puoi diminuire quel valore; puoi solo aumentarlo.
LegalHold	• Vero: questo bucket è attualmente soggetto a un blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché il blocco legale non viene revocato, anche se il loro periodo di conservazione è scaduto. • Falso: questo bucket non è attualmente soggetto a un blocco legale. Gli oggetti in questo bucket possono essere eliminati quando il loro periodo di conservazione scade.
AutoDelete	• Vero: gli oggetti in questo bucket verranno eliminati automaticamente quando il loro periodo di conservazione scade, a meno che il bucket non sia soggetto a un blocco legale. • Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Devi eliminare manualmente questi oggetti se hai bisogno di eliminarli.

Coerenza per le impostazioni di conformità

Quando aggiorni le impostazioni di conformità per un bucket S3 con una richiesta PUT Bucket compliance, StorageGRID tenta di aggiornare i metadati del bucket in tutta la griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **Strong-global** per garantire che tutti i data center site e tutti i Storage Node che contengono i metadati del bucket abbiano coerenza read-after-write per le impostazioni di conformità

modificate.

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

Se ricevi questa risposta, devi contattare l'amministratore della griglia per assicurarti che i servizi di archiviazione richiesti vengano resi disponibili il prima possibile. Se l'amministratore della griglia non è in grado di rendere disponibili un numero sufficiente di Storage Node in ciascun sito, il supporto tecnico potrebbe suggerirti di riprovare la richiesta non riuscita forzando la coerenza **Strong-site**.



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

Quando la coerenza viene ridotta a **Strong-site**, StorageGRID garantisce che le impostazioni di conformità aggiornate avranno coerenza read-after-write solo per le richieste dei client all'interno di un sito. Questo significa che il sistema StorageGRID potrebbe temporaneamente avere più impostazioni incoerenti per questo bucket finché tutti i siti e i nodi di Storage non saranno disponibili. Le impostazioni incoerenti possono causare comportamenti imprevisti e indesiderati. Ad esempio, se metti un bucket sotto blocco legale e forzi una coerenza inferiore, le precedenti impostazioni di conformità del bucket (cioè, blocco legale disattivato) potrebbero continuare a essere attive in alcuni siti del data center. Di conseguenza, gli oggetti che pensi siano soggetti a blocco legale potrebbero essere eliminati quando il loro periodo di conservazione scade, sia dall'utente che da AutoDelete, se abilitato.

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

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

Risposte di errore

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

Informazioni correlate

"Obsoleto: modifiche alla richiesta PUT Bucket per la conformità"

Informazioni sul copyright

Copyright © 2026 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.