



Operazioni personalizzate StorageGRID

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-119/s3/custom-operations-on-buckets.html> on December 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Operazioni personalizzate StorageGRID	1
Operazioni personalizzate StorageGRID	1
OTTIENI la coerenza del bucket	1
Richiedi esempio	2
Risposta	2
Esempio di risposta	2
PUT Consistenza del secchio	3
Richiesta	3
Richiedi esempio	4
GET Ora dell'ultimo accesso al bucket	4
Richiedi esempio	4
Esempio di risposta	4
Ora dell'ultimo accesso al bucket PUT	5
Esempi di richiesta	6
ELIMINA la configurazione della notifica dei metadati del bucket	6
Richiedi esempio	6
Configurazione della notifica dei metadati del bucket GET	6
Richiedi esempio	7
Risposta	7
Esempio di risposta	9
Configurazione della notifica dei metadati del bucket PUT	10
Richiesta	10
Esempi di richiesta	12
JSON generato dal servizio di integrazione della ricerca	14
Metadati degli oggetti inclusi nelle notifiche dei metadati	15
Richiesta di utilizzo dello spazio di archiviazione GET	16
Richiedi esempio	16
Esempio di risposta	16
Controllo delle versioni	17
Richieste di bucket deprecate per la conformità legacy	17
Richieste di bucket deprecate per la conformità legacy	17
Obsoleto: modifiche alla richiesta CreateBucket per conformità	18
Obsoleto: richiesta di conformità del bucket GET	19
Obsoleto: richiesta di conformità del bucket PUT	20

Operazioni personalizzate StorageGRID

Operazioni personalizzate StorageGRID

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

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

Operazione	Descrizione
"OTTIENI la coerenza del bucket"	Restituisce la coerenza applicata a un determinato bucket.
"PUT Consistenza del secchio"	Imposta la coerenza applicata a un determinato bucket.
"GET Ora dell'ultimo accesso al bucket"	Restituisce se gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati o disabilitati per un determinato bucket.
"Ora dell'ultimo accesso al bucket PUT"	Consente di abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso per un determinato bucket.
"ELIMINA la configurazione della notifica dei metadati del bucket"	Elimina l'XML di configurazione delle notifiche dei metadati associato a un determinato bucket.
"Configurazione della notifica dei metadati del bucket GET"	Restituisce il file XML di configurazione delle notifiche dei metadati associato a un determinato bucket.
"Configurazione della notifica dei metadati del bucket PUT"	Configura il servizio di notifica dei metadati per un bucket.
"Utilizzo dello spazio di archiviazione GET"	Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.
"Obsoleto: CreateBucket con impostazioni di conformità"	Obsoleto e non supportato: non è più possibile creare nuovi bucket con la conformità abilitata.
"Obsoleto: conformità al bucket GET"	Obsoleto ma supportato: restituisce le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente.
"Obsoleto: conformità al bucket PUT"	Obsoleto ma supportato: consente di modificare le impostazioni di conformità per un bucket Compliant legacy esistente.

OTTIENI la coerenza del bucket

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

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

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

Richiedi esempio

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

Risposta

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

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

Esempio di risposta

```

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

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

```

Informazioni correlate

["Valori di coerenza"](#)

PUT Consistenza del secchio

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

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

Prima di iniziare

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

Richiesta

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

Coerenza	Descrizione
Tutto	Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
forte-globale	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
sito forte	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo nuova scrittura	(Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.

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

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

Richiedi esempio

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

Informazioni correlate

["Valori di coerenza"](#)

GET Ora dell'ultimo accesso al bucket

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

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

Richiedi esempio

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

Esempio di risposta

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

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

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

Ora dell'ultimo accesso al bucket PUT

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

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

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

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

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

Esempi di richiesta

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

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

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

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

ELIMINA la configurazione della notifica dei metadati del bucket

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

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

Richiedi esempio

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

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

Configurazione della notifica dei metadati del bucket GET

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

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

Richiedi esempio

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

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

Risposta

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

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

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

Nome	Descrizione	Necessario
MetadatiNotificaConfigura zione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	Sì

Nome	Descrizione	Necessario
Regola	<p>Tag contenitore 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 per la regola.</p> <p>Incluso nell'elemento Regola.</p>	NO
Stato	<p>Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate.</p> <p>Incluso nell'elemento Regola.</p>	Sì
Prefisso	<p>Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata.</p> <p>Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Regola.</p>	Sì
Destinazione	<p>Tag contenitore per la destinazione di una regola.</p> <p>Incluso nell'elemento Regola.</p>	Sì

Nome	Descrizione	Necessario
Urna	<p>URN della destinazione a 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"> • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato domain-name/myindex/mytype . <p>Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma:</p> <ul style="list-style-type: none"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404.</p> <p>L'urna è inclusa nell'elemento Destinazione.</p>	Sì

Esempio di risposta

L'XML incluso tra

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

```

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

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

```

Informazioni correlate

["Utilizzare un account tenant"](#)

Configurazione della notifica dei metadati del bucket PUT

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

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

Richiesta

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

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

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

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID . L'endpoint deve

esistere quando viene inviata la configurazione della notifica dei metadati, altrimenti la richiesta fallisce come 400 Bad Request Il messaggio di errore afferma: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

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

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

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

Nome	Descrizione	Necessario
Stato	<p>Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate.</p> <p>Incluso nell'elemento Regola.</p>	Sì
Prefisso	<p>Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata.</p> <p>Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Regola.</p>	Sì
Destinazione	<p>Tag contenitore per la destinazione di una regola.</p> <p>Incluso nell'elemento Regola.</p>	Sì
Urna	<p>URN della destinazione a 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"> • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato domain-name/myindex/mytype . <p>Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma:</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404.</p> <p>L'urna è inclusa nell'elemento Destinazione.</p>	Sì

Esempi di richiesta

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

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

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

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

```

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

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

JSON generato dal servizio di integrazione della ricerca

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

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

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

Metadati degli oggetti inclusi nelle notifiche dei metadati

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

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

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



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

Informazioni correlate

["Utilizzare un account tenant"](#)

Richiesta di utilizzo dello spazio di archiviazione GET

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

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

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

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

Richiedi esempio

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

Esempio di risposta

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

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

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

Controllo delle versioni

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

Informazioni correlate

["Valori di coerenza"](#)

Richieste di bucket deprecate per la conformità legacy

Richieste di bucket deprecate per la conformità legacy

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

Funzionalità di conformità deprecata

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

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

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

Richieste di conformità deprecate:

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

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

- ["Obsoleto - Conformità al bucket GET"](#)

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

- ["Obsoleto - Conformità al bucket PUT"](#)

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

Obsoleto: modifiche alla richiesta CreateBucket per conformità

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

 La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:

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

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

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Obsoleto: richiesta di conformità del bucket GET

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

La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:



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

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

Richiedi esempio

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

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

Esempio di risposta

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

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

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

Nome	Descrizione
Periodo di conservazioneMinuti	Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia.
LegalHold	<ul style="list-style-type: none"> Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto. Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione.
Eliminazione automatica	<ul style="list-style-type: none"> Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale. Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente.

Risposte di errore

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

Obsoleto: richiesta di conformità del bucket PUT

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

 La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:

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

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

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

Richiedi esempio

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

a partire dal momento in cui l'oggetto viene inserito nella griglia. Non esiste alcun vincolo legale su questo secchio. Ogni oggetto verrà automaticamente eliminato dopo due anni.

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

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

Nome	Descrizione
Periodo di conservazioneMinuti	Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia. Importante Quando si specifica un nuovo valore per RetentionPeriodMinutes, è necessario specificare un valore uguale o maggiore del periodo di conservazione corrente del bucket. Dopo aver impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore; è possibile solo aumentarlo.
LegalHold	<ul style="list-style-type: none">Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto.Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione.
Eliminazione automatica	<ul style="list-style-type: none">Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale.Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente.

Coerenza per le impostazioni di conformità

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

impostazioni di conformità modificate.

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

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



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

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

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

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

Risposte di errore

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

Informazioni correlate

["Obsoleto: modifiche alla richiesta PUT Bucket per conformità"](#)

Informazioni sul copyright

Copyright © 2025 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 COMMERCIALITÀ 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.