Richieste StorageGRID S3

StorageGRID 11.7

NetApp
April 12, 2024

Sommario

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.
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.
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.

Controllo della coerenza	Descrizione
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	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
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì

Nome	Descrizione	Obbligatorio
Urna	URNA della destinazione in 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 form `domain-name/myindex/mytype`. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'urn è incluso nell'elemento Destination.	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
MetadataNotificationConfiguration	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	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì
Urna	URNA della destinazione in 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 form `domain-name/myindex/mytype`. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'urn è incluso nell'elemento Destination.	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-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON generato dal servizio di integrazione della ricerca

Quando si 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 `us-east-1`
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 *`key:value`*	Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore

Tipo	Nome dell'elemento	Descrizione
Tag	tag *key:value*	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	• 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. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	• 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. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

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	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. **Importante** quando si specifica un nuovo valore per RetentionPeriodMinutes, 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.

Nome	Descrizione
LegalHold	• 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. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	• 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. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

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"