



StorageGRID 사용자 지정 작업

StorageGRID software

NetApp
July 23, 2026

목차

StorageGRID 사용자 지정 작업	1
StorageGRID에서 지원되는 사용자 지정 버킷 작업	1
GET Bucket consistency 요청을 사용하여 StorageGRID에서 버킷 정합성 보장 수준을 검색합니다	1
요청 예시	2
응답	2
응답 예시	2
PUT Bucket 정합성 보장 요청을 사용하여 StorageGRID에서 정합성 보장 수준 지정	3
요청	3
요청 예시	4
GET Bucket last access time 요청을 사용하여 StorageGRID에서 버킷 마지막 액세스 시간 상태를 검색합니다 ..	4
요청 예시	4
응답 예시	4
PUT Bucket last access time 요청을 사용하여 StorageGRID에서 마지막 액세스 시간 업데이트를 활성화 및 ..	5
비활성화합니다	6
요청 예시	6
StorageGRID에서 DELETE 버킷 메타데이터 알림 구성 요청을 사용하여 검색 통합 서비스를 비활성화합니다 ..	6
요청 예시	6
GET 버킷 메타데이터 알림 구성 요청을 사용하여 StorageGRID에서 검색 통합을 구성합니다	6
요청 예시	7
응답	7
응답 예시	9
PUT Bucket 메타데이터 알림 구성 요청을 사용하여 StorageGRID에서 검색 통합 서비스를 활성화합니다	10
요청	10
요청 예시	12
검색 통합 서비스에서 생성된 JSON	14
메타데이터 알림에 포함된 객체 메타데이터	14
GET Storage Usage 요청을 사용하여 StorageGRID에서 계정 및 버킷 스토리지 사용량을 조회합니다	15
요청 예시	15
응답 예시	15
버전 관리	16
기존 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청	16
기존 StorageGRID 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청	16
StorageGRID의 더 이상 사용되지 않는 SGCompliance 요소	17
StorageGRID의 더 이상 사용되지 않는 GET 버킷 규정 준수 요청	18
StorageGRID의 더 이상 사용되지 않는 PUT 버킷 규정 준수 요청	19

StorageGRID 사용자 지정 작업

StorageGRID에서 지원되는 사용자 지정 버킷 작업

StorageGRID 시스템은 S3 REST API에 추가되는 사용자 지정 작업을 지원합니다.

다음 표에는 StorageGRID에서 지원하는 사용자 지정 작업이 나열되어 있습니다.

작업	설명
"GET Bucket 일관성"	특정 버킷에 적용되는 일관성 수준을 반환합니다.
"PUT 버킷 일관성"	특정 버킷에 적용되는 일관성 수준을 설정합니다.
"GET 버킷 마지막 액세스 시간"	특정 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되었는지 또는 비활성화되었는지 여부를 반환합니다.
"PUT Bucket 마지막 액세스 시간"	특정 버킷에 대한 마지막 액세스 시간 업데이트를 활성화 또는 비활성화할 수 있습니다.
"DELETE Bucket 메타데이터 알림 구성"	특정 버킷과 연결된 메타데이터 알림 구성 XML을 삭제합니다.
"GET 버킷 메타데이터 알림 구성"	특정 버킷과 연결된 메타데이터 알림 구성 XML을 반환합니다.
"PUT 버킷 메타데이터 알림 구성"	버킷에 대한 메타데이터 알림 서비스를 구성합니다.
"저장 공간 사용량 가져오기"	계정에서 사용 중인 총 저장 용량과 해당 계정과 연결된 각 버킷의 저장 용량을 보여줍니다.
"더 이상 사용되지 않음: CreateBucket 규정 준수 설정 포함"	더 이상 사용되지 않으며 지원되지 않습니다. 규정 준수 기능이 활성화된 새 버킷을 더 이상 생성할 수 없습니다.
"사용 중단됨: GET 버킷 규정 준수"	더 이상 사용되지 않지만 지원되는 기능: 기존 레거시 규정 준수 버킷에 현재 적용되는 규정 준수 설정을 반환합니다.
"사용 중단됨: PUT Bucket compliance"	더 이상 사용되지 않지만 지원되는 기능: 기존 레거시 규정 준수 버킷의 규정 준수 설정을 수정할 수 있습니다.

GET Bucket consistency 요청을 사용하여 StorageGRID에서 버킷 정합성 보장 수준을 검색합니다

GET 버킷 일관성 요청을 사용하면 특정 버킷에 적용되는 일관성 수준을 확인할 수 있습니다.

기본 일관성은 새로 생성된 객체에 대해 쓰기 후 읽기를 보장하도록 설정되어 있습니다.

이 작업을 완료하려면 s3:GetBucketConsistency 권한이 있거나 루트 계정이어야 합니다.

요청 예시

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

응답

응답 XML에서 ``은(는) 다음 값 중 하나를 반환합니다.

일관성	설명
모두	모든 노드가 데이터를 즉시 수신해야 하며, 그렇지 않으면 요청이 실패합니다.
strong-global	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
strong-site	사이트 내 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
새 쓰기 후 읽기	(기본값) 새 객체에 대해서는 쓰기 후 읽기 일관성을, 객체 업데이트에 대해서는 최종 일관성을 제공합니다. 높은 가용성과 데이터 보호를 보장합니다. 대부분의 경우에 권장됩니다.
사용 가능	새로운 객체 생성 및 객체 업데이트 모두에 대해 최종 일관성을 제공합니다. S3 버킷의 경우, 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷 또는 존재하지 않는 키에 대한 HEAD 또는 GET 작업). S3 FabricPool 버킷에서는 지원되지 않습니다.

응답 예시

```

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>

```

관련 정보

["일관성"](#)

PUT Bucket 정합성 보장 요청을 사용하여 StorageGRID에서 정합성 보장 수준 지정

PUT 버킷 일관성 요청을 사용하면 버킷에서 수행되는 작업에 적용할 일관성 수준을 지정할 수 있습니다.

기본 일관성은 새로 생성된 객체에 대해 쓰기 후 읽기를 보장하도록 설정되어 있습니다.

시작하기 전에

이 작업을 완료하려면 s3:PutBucketConsistency 권한이 있거나 루트 계정이어야 합니다.

요청

The x-ntap-sg-consistency 매개변수에는 다음 값 중 하나가 포함되어야 합니다.

일관성	설명
모두	모든 노드가 데이터를 즉시 수신해야 하며, 그렇지 않으면 요청이 실패합니다.
strong-global	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
strong-site	사이트 내 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
새 쓰기 후 읽기	(기본값) 새 객체에 대해서는 쓰기 후 읽기 일관성을, 객체 업데이트에 대해서는 최종 일관성을 제공합니다. 높은 가용성과 데이터 보호를 보장합니다. 대부분의 경우에 권장됩니다.

일관성	설명
사용 가능	새로운 객체 생성 및 객체 업데이트 모두에 대해 최종 일관성을 제공합니다. S3 버킷의 경우, 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷 또는 존재하지 않는 키에 대한 HEAD 또는 GET 작업). S3 FabricPool 버킷에서는 지원되지 않습니다.

참고: 일반적으로 "새로 쓰기 후 읽기" 일관성을 사용하는 것이 좋습니다. 요청이 제대로 작동하지 않으면 가능하면 애플리케이션 클라이언트 동작을 변경하십시오. 또는 각 API 요청에 대해 일관성을 지정하도록 클라이언트를 구성하십시오. 버킷 수준에서 일관성을 설정하는 것은 최후의 수단으로만 사용하십시오.

요청 예시

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

관련 정보

["일관성"](#)

GET Bucket last access time 요청을 사용하여 StorageGRID에서 버킷 마지막 액세스 시간 상태를 검색합니다

GET 버킷 마지막 액세스 시간 요청을 사용하면 개별 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되었는지 또는 비활성화되었는지 확인할 수 있습니다.

이 작업을 완료하려면 s3:GetBucketLastAccessTime 권한이 있거나 계정 루트여야 합니다.

요청 예시

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

응답 예시

이 예시는 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되어 있음을 보여줍니다.

```
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>
```

PUT Bucket last access time 요청을 사용하여 StorageGRID에서 마지막 액세스 시간 업데이트를 활성화 및 비활성화합니다

PUT 버킷 최종 액세스 시간 요청을 사용하면 개별 버킷에 대한 최종 액세스 시간 업데이트를 활성화 또는 비활성화할 수 있습니다. 최종 액세스 시간 업데이트를 비활성화하면 성능이 향상되며, 버전 10.3.0 이상으로 생성된 모든 버킷의 기본 설정입니다.

이 작업을 완료하려면 버킷에 대한 s3:PutBucketLastAccessTime 권한이 있거나 계정 루트여야 합니다.



StorageGRID 버전 10.3부터 모든 새 버킷에 대해 마지막 액세스 시간 업데이트가 기본적으로 비활성화됩니다. 이전 버전의 StorageGRID를 사용하여 생성된 버킷이 있고 새 기본 동작과 일치하도록 하려면 해당 이전 버킷 각각에 대해 마지막 액세스 시간 업데이트를 명시적으로 비활성화해야 합니다. 마지막 액세스 시간 업데이트는 PUT Bucket last access time 요청을 사용하거나 테넌트 관리자의 버킷 세부 정보 페이지에서 활성화하거나 비활성화할 수 있습니다. ["마지막 액세스 시간 업데이트 활성화 또는 비활성화"](#)를 참조하십시오.

버킷에 대한 마지막 액세스 시간 업데이트가 비활성화된 경우, 해당 버킷에 대한 작업에는 다음과 같은 동작이 적용됩니다.

- GetObject, GetObjectAcl, GetObjectTagging, 및 HeadObject 요청은 마지막 액세스 시간을 업데이트하지 않습니다. 해당 객체는 정보 라이프사이클 관리(ILM) 평가를 위한 대기열에 추가되지 않습니다.
- CopyObject 및 PutObjectTagging 요청이 메타데이터만 업데이트하는 경우에도 마지막 액세스 시간이 업데이트됩니다. 해당 객체는 ILM 평가를 위한 대기열에 추가됩니다.
- 소스 버킷에 대한 마지막 액세스 시간 업데이트가 비활성화된 경우, CopyObject 요청은 소스 버킷의 마지막 액세스 시간을 업데이트하지 않습니다. 복사된 객체는 소스 버킷의 ILM 평가 대기열에 추가되지 않습니다. 그러나 대상 버킷의 경우, CopyObject 요청은 항상 마지막 액세스 시간을 업데이트합니다. 복사된 객체는 ILM 평가 대기열에 추가됩니다.
- CompleteMultipartUpload 요청은 마지막 액세스 시간을 업데이트합니다. 완료된 객체는 ILM 평가를 위한 큐에 추가됩니다.

요청 예시

이 예제는 버킷의 마지막 액세스 시간을 활성화합니다.

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

이 예제는 버킷의 마지막 액세스 시간을 비활성화합니다.

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

StorageGRID에서 DELETE 버킷 메타데이터 알림 구성 요청을 사용하여 검색 통합 서비스를 비활성화합니다

DELETE 버킷 메타데이터 알림 구성 요청을 사용하면 구성 XML을 삭제하여 개별 버킷에 대한 검색 통합 서비스를 비활성화할 수 있습니다.

이 작업을 완료하려면 버킷에 대한 s3:DeleteBucketMetadataNotification 권한이 있거나 계정 루트여야 합니다.

요청 예시

이 예시는 버킷에 대한 검색 통합 서비스를 비활성화하는 방법을 보여줍니다.

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

GET 버킷 메타데이터 알림 구성 요청을 사용하여 StorageGRID에서 검색 통합을 구성합니다

GET 버킷 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대한 검색 통합을 구성하는 데 사용되는 구성 XML을 검색할 수 있습니다.

이 작업을 완료하려면 s3:GetBucketMetadataNotification 권한이 있거나 계정 루트여야 합니다.

요청 예시

이 요청은 'bucket'라는 이름의 버킷에 대한 메타데이터 알림 구성을 검색합니다.

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

응답

응답 본문에는 버킷에 대한 메타데이터 알림 구성이 포함됩니다. 메타데이터 알림 구성을 통해 검색 통합을 위해 버킷을 구성하는 방법을 결정할 수 있습니다. 즉, 어떤 객체를 인덱싱할지, 그리고 해당 객체의 메타데이터가 어떤 엔드포인트로 전송될지를 지정할 수 있습니다.

```
<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>
```

각 메타데이터 알림 구성에는 하나 이상의 규칙이 포함됩니다. 각 규칙은 적용 대상 객체와 StorageGRID가 객체 메타데이터를 전송해야 하는 대상을 지정합니다. 대상은 StorageGRID 엔드포인트의 URN을 사용하여 지정해야 합니다.

이름	설명	필수
MetadataNotificationConfiguration	메타데이터 알림의 객체와 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 Rule 요소를 포함합니다.	예

이름	설명	필수
규칙	지정된 인덱스에 메타데이터를 추가해야 하는 객체를 식별하는 규칙에 대한 컨테이너 태그입니다. 접두사가 겹치는 규칙은 허용되지 않습니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID	규칙에 대한 고유 식별자입니다. 규칙 요소에 포함됩니다.	아니요
상태	상태는 '활성화됨' 또는 '비활성화됨'일 수 있습니다. 비활성화된 규칙에 대해서는 아무런 조치도 취해지지 않습니다. 규칙 요소에 포함됩니다.	예
접두사	접두사와 일치하는 객체는 해당 규칙의 영향을 받으며, 해당 객체의 메타데이터가 지정된 대상으로 전송됩니다. 모든 객체와 일치시키려면 빈 접두사를 지정하십시오. 규칙 요소에 포함됩니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. 규칙 요소에 포함됩니다.	예

이름	설명	필수
Urn	객체 메타데이터가 전송되는 대상의 URN입니다. 다음 속성을 가진 StorageGRID 엔드포인트의 URN이어야 합니다. • `es` 세 번째 요소여야 합니다. • URN은 메타데이터가 저장된 인덱스와 유형으로 끝나야 하며, 형식은 `domain-name/myindex/mytype`입니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 사용합니다. • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> 엔드포인트는 구성 XML을 제출하기 전에 구성되어야 합니다. 그렇지 않으면 구성이 실패하고 404 오류가 발생합니다. URN은 대상 요소에 포함됩니다.	예

응답 예시

```
`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`
```

그 사이에 포함된 XML은 버킷에 대한 검색 통합 엔드포인트와의 통합 구성 방식을 보여줍니다. 이 예에서는 객체 메타데이터가 `current`라는 이름의 Elasticsearch 인덱스와 `2017`라는 유형으로 전송되며, 이 인덱스는 `records`라는 이름의 AWS 도메인에 호스팅됩니다.

```
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-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

관련 정보

["테넌트 계정 사용"](#)

PUT Bucket 메타데이터 알림 구성 요청을 사용하여 StorageGRID에서 검색 통합 서비스를 활성화합니다

PUT 버킷 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대해 검색 통합 서비스를 활성화할 수 있습니다. 요청 본문에 제공하는 메타데이터 알림 구성 XML은 메타데이터가 대상 검색 인덱스로 전송되는 객체를 지정합니다.

이 작업을 완료하려면 버킷에 대한 s3:PutBucketMetadataNotification 권한이 있거나 계정 루트여야 합니다.

요청

요청 본문에는 메타데이터 알림 구성이 포함되어야 합니다. 각 메타데이터 알림 구성에는 하나 이상의 규칙이 포함됩니다. 각 규칙은 적용되는 객체와 StorageGRID가 객체 메타데이터를 전송해야 하는 대상을 지정합니다.

객체는 객체 이름의 접두사를 기준으로 필터링할 수 있습니다. 예를 들어, 접두사가 `/images`인 객체의 메타데이터는 한 대상으로 보내고, 접두사가 `/videos`인 객체는 다른 대상으로 보낼 수 있습니다.

접두사가 겹치는 구성은 유효하지 않으며 제출 시 거부됩니다. 예를 들어, 접두사가 `test`인 객체에 대한 규칙 하나와 접두사가 `test2`인 객체에 대한 규칙 하나를 포함하는 구성은 허용되지 않습니다.

대상은 StorageGRID 엔드포인트의 URN을 사용하여 지정해야 합니다. 메타데이터 알림 구성이 제출될 때 엔드포인트가 존재해야 하며, 그렇지 않으면 요청이 실패합니다 400 Bad Request. 오류 메시지는 다음과 같습니다. 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>
```

이 표는 메타데이터 알림 구성 XML의 요소를 설명합니다.

이름	설명	필수
MetadataNotificationConfiguration	메타데이터 알림의 객체와 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 Rule 요소를 포함합니다.	예
규칙	지정된 인덱스에 메타데이터를 추가해야 하는 객체를 식별하는 규칙에 대한 컨테이너 태그입니다. 접두사가 겹치는 규칙은 허용되지 않습니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID	규칙에 대한 고유 식별자입니다. 규칙 요소에 포함됩니다.	아니요
상태	상태는 '활성화됨' 또는 '비활성화됨'일 수 있습니다. 비활성화된 규칙에 대해서는 아무런 조치도 취해지지 않습니다. 규칙 요소에 포함됩니다.	예

이름	설명	필수
접두사	접두사와 일치하는 객체는 해당 규칙의 영향을 받으며, 해당 객체의 메타데이터가 지정된 대상으로 전송됩니다. 모든 객체와 일치시키려면 빈 접두사를 지정하십시오. 규칙 요소에 포함됩니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. 규칙 요소에 포함됩니다.	예
Urn	객체 메타데이터가 전송되는 대상의 URN입니다. 다음 속성을 가진 StorageGRID 엔드포인트의 URN이어야 합니다. • `es` 세 번째 요소여야 합니다. • URN은 메타데이터가 저장된 인덱스와 유형으로 끝나야 하며, 형식은 `domain-name/myindex/mytype`입니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 사용합니다. • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> 엔드포인트는 구성 XML을 제출하기 전에 구성되어야 합니다. 그렇지 않으면 구성이 실패하고 404 오류가 발생합니다. URN은 대상 요소에 포함됩니다.	예

요청 예시

이 예시는 버킷에 대한 검색 통합을 활성화하는 방법을 보여줍니다. 이 예시에서는 모든 객체의 메타데이터가 동일한 대상으로 전송됩니다.

```

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>

```

이 예시에서는 접두사 `/images`와 일치하는 객체의 객체 메타데이터는 한 대상으로 전송되고, 접두사 `/videos`와 일치하는 객체의 객체 메타데이터는 두 번째 대상으로 전송됩니다.

```

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>

```

검색 통합 서비스에서 생성된 JSON

버킷에 대한 검색 통합 서비스를 활성화하면 객체 메타데이터 또는 태그가 추가, 업데이트 또는 삭제될 때마다 JSON 문서가 생성되어 대상 엔드포인트로 전송됩니다.

이 예시는 키가 SGWS/Tagging.txt 인 객체가 test 라는 이름의 버킷에 생성될 때 생성될 수 있는 JSON의 예시를 보여줍니다. 해당 test 버킷은 버전 관리가 되지 않으므로 versionId 태그는 비어 있습니다.

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

메타데이터 알림에 포함된 객체 메타데이터

이 표는 검색 통합이 활성화되었을 때 대상 엔드포인트로 전송되는 JSON 문서에 포함된 모든 필드를 나열합니다.

문서 이름에는 버킷 이름, 객체 이름, 그리고 있는 경우 버전 ID가 포함됩니다.

유형	품목명	설명
버킷 및 객체 정보	버킷	버킷 이름
버킷 및 객체 정보	키	객체 키 이름
버킷 및 객체 정보	versionID	버전 관리 버킷에 있는 객체의 객체 버전입니다.
버킷 및 객체 정보	지역	버킷 영역(예: us-east-1)
시스템 메타데이터	크기	HTTP 클라이언트에 표시되는 객체 크기(바이트)
시스템 메타데이터	md5	객체 해시

유형	품목명	설명
사용자 메타데이터	메타데이터 <i>key:value</i>	객체에 대한 모든 사용자 메타데이터 (키-값 쌍)
태그	태그 <i>key:value</i>	객체에 대해 정의된 모든 객체 태그(키-값 쌍)



태그 및 사용자 메타데이터의 경우, StorageGRID는 낱파와 숫자를 문자열 또는 S3 이벤트 알림으로 Elasticsearch에 전달합니다. Elasticsearch가 이러한 문자열을 낱파 또는 숫자로 해석하도록 구성하려면 동적 필드 매핑 및 낱파 형식 매핑에 대한 Elasticsearch 지침을 따르세요. 검색 통합 서비스를 구성하기 전에 인덱스에서 동적 필드 매핑을 활성화해야 합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 유형을 편집할 수 없습니다.

관련 정보

["테넌트 계정 사용"](#)

GET Storage Usage 요청을 사용하여 StorageGRID에서 계정 및 버킷 스토리지 사용량을 조회합니다

GET 스토리지 사용량 요청은 계정에서 사용 중인 총 스토리지 용량과 해당 계정과 연결된 각 버킷의 스토리지 용량을 알려줍니다.

계정 및 버킷별 저장 용량은 `x-ntap-sg-usage` 쿼리 매개변수를 사용하여 수정된 ListBuckets 요청을 통해 확인할 수 있습니다. 버킷 저장 용량 사용량은 시스템에서 처리하는 PUT 및 DELETE 요청과 별도로 추적됩니다. 특히 시스템 부하가 높은 경우, 요청 처리 속도에 따라 사용량 값이 예상 값과 일치하기까지 다소 시간이 걸릴 수 있습니다.

기본적으로 StorageGRID는 강력한 전역 일관성을 사용하여 사용량 정보를 검색하려고 시도합니다. 강력한 전역 일관성을 달성할 수 없는 경우 StorageGRID는 강력한 사이트 일관성을 사용하여 사용량 정보를 검색하려고 시도합니다.

이 작업을 완료하려면 `s3:ListAllMyBuckets` 권한이 있거나 루트 계정이어야 합니다.

요청 예시

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

응답 예시

이 예시는 두 개의 버킷에 네 개의 객체와 12바이트의 데이터가 있는 계정을 보여줍니다. 각 버킷에는 두 개의 객체와 6바이트의 데이터가 포함되어 있습니다.

```
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>
```

버전 관리

저장된 모든 객체 버전은 응답의 ObjectCount 및 DataBytes 값에 영향을 미칩니다. 삭제 마커는 ObjectCount 총합에 추가되지 않습니다.

관련 정보

["일관성"](#)

기존 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청

기존 **StorageGRID** 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청

StorageGRID 기존 규정 준수 기능을 사용하여 생성된 버킷을 관리하려면 StorageGRID S3 REST API를 사용해야 할 수도 있습니다.

규정 준수 기능이 더 이상 사용되지 않습니다.

이전 StorageGRID 버전에서 제공되었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 Object

Lock으로 대체되었습니다.

이전에 전역 규정 준수 설정을 활성화한 경우, StorageGRID 11.6에서는 전역 S3 객체 잠금 설정이 활성화됩니다. 규정 준수가 활성화된 새 버킷은 더 이상 생성할 수 없습니다. 하지만 필요한 경우 StorageGRID S3 REST API를 사용하여 기존의 레거시 규정 준수 버킷을 관리할 수 있습니다.

- ["S3 REST API를 사용하여 S3 Object Lock 구성"](#)
- ["ILM을 사용하여 객체 관리"](#)
- ["NetApp 기술 자료: StorageGRID 11.5에서 기존 규정 준수 버킷을 관리하는 방법"](#)

더 이상 사용되지 않는 규정 준수 요청:

- ["사용 중단됨 - 규정 준수를 위한 PUT 버킷 요청 수정"](#)

SGCompliance XML 요소는 더 이상 사용되지 않습니다. 이전에는 PUT Bucket 요청의 선택적 XML 요청 본문에 이 StorageGRID 사용자 지정 요소를 포함하여 규정 준수 버킷을 생성할 수 있었습니다.

- ["사용 중단됨 - GET 버킷 규정 준수"](#)

GET 버킷 규정 준수 요청은 더 이상 사용되지 않습니다. 하지만 기존 레거시 규정 준수 버킷에 현재 적용 중인 규정 준수 설정을 확인하려면 이 요청을 계속 사용할 수 있습니다.

- ["사용 중단됨 - PUT Bucket compliance"](#)

PUT 버킷 규정 준수 요청은 더 이상 사용되지 않습니다. 하지만 기존의 레거시 규정 준수 버킷에 대한 규정 준수 설정을 수정하는 데에는 이 요청을 계속 사용할 수 있습니다. 예를 들어 기존 버킷에 법적 보존 조치를 적용하거나 보존 기간을 늘릴 수 있습니다.

StorageGRID의 더 이상 사용되지 않는 SGCompliance 요소

SGCompliance XML 요소는 더 이상 사용되지 않습니다. 이전에는 CreateBucket 요청의 선택적 XML 요청 본문에 이 StorageGRID 사용자 지정 요소를 포함하여 규정 준수 버킷을 생성할 수 있었습니다.



이전 StorageGRID 버전에서 제공되었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 Object Lock으로 대체되었습니다. 자세한 내용은 다음을 참조하십시오.

- ["S3 REST API를 사용하여 S3 Object Lock 구성"](#)
- ["NetApp 기술 자료: StorageGRID 11.5에서 기존 규정 준수 버킷을 관리하는 방법"](#)

규정 준수 기능이 활성화된 새 버킷을 더 이상 생성할 수 없습니다. 규정 준수를 위한 CreateBucket 요청 수정을 사용하여 새 규정 준수 버킷을 생성하려고 하면 다음 오류 메시지가 반환됩니다.

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

StorageGRID의 더 이상 사용되지 않는 GET 버킷 규정 준수 요청

GET 버킷 규정 준수 요청은 더 이상 사용되지 않습니다. 하지만 기존 레거시 규정 준수 버킷에 현재 적용 중인 규정 준수 설정을 확인하려면 이 요청을 계속 사용할 수 있습니다.



이전 StorageGRID 버전에서 제공되었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 Object Lock으로 대체되었습니다. 자세한 내용은 다음을 참조하십시오.

- ["S3 REST API를 사용하여 S3 Object Lock 구성"](#)
- ["NetApp 기술 자료: StorageGRID 11.5에서 기존 규정 준수 버킷을 관리하는 방법"](#)

이 작업을 완료하려면 s3:GetBucketCompliance 권한이 있거나 루트 계정이어야 합니다.

요청 예시

이 예시 요청을 통해 이름이 `mybucket`인 버킷에 대한 규정 준수 설정을 확인할 수 있습니다.

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

응답 예시

응답 XML에는 `` 버킷에 적용되는 규정 준수 설정이 나열됩니다. 이 예시 응답은 각 객체가 그리드에 수집된 시점부터 1년(525,600분) 동안 보존되는 버킷의 규정 준수 설정을 보여줍니다. 현재 이 버킷에는 법적 보존 조치가 적용되지 않았습니다. 각 객체는 1년 후 자동으로 삭제됩니다.

```
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>
```

이름	설명
RetentionPeriodMinutes	이 버킷에 추가된 객체의 보존 기간(분)입니다. 보존 기간은 객체가 그리드에 수집된 시점부터 시작됩니다.
LegalHold	- 참: 이 버킷은 현재 법적 보존 조치가 적용되어 있습니다. 이 버킷의 객체는 보존 기간이 만료되었더라도 법적 보존 조치가 해제될 때까지 삭제할 수 없습니다. - 거짓: 이 버킷은 현재 법적 보존 상태가 아닙니다. 이 버킷의 객체는 보존 기간이 만료되면 삭제될 수 있습니다.
AutoDelete	- True: 이 버킷에 있는 객체는 보존 기간이 만료되면 자동으로 삭제됩니다. 단, 버킷이 법적 보존 상태에 있는 경우는 예외입니다. - 거짓: 이 버킷의 객체는 보존 기간이 만료되어도 자동으로 삭제되지 않습니다. 삭제해야 하는 경우 수동으로 삭제해야 합니다.

오류 응답

버킷이 규정을 준수하도록 생성되지 않은 경우 응답의 HTTP 상태 코드는 `404 Not Found`이며 S3 오류 코드는 `XNoSuchBucketCompliance`입니다.

StorageGRID의 더 이상 사용되지 않는 PUT 버킷 규정 준수 요청

PUT 버킷 규정 준수 요청은 더 이상 사용되지 않습니다. 하지만 기존의 레거시 규정 준수 버킷에 대한 규정 준수 설정을 수정하는 데에는 이 요청을 계속 사용할 수 있습니다. 예를 들어 기존 버킷에 법적 보존 조치를 적용하거나 보존 기간을 늘릴 수 있습니다.



이전 StorageGRID 버전에서 제공되었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 Object Lock으로 대체되었습니다. 자세한 내용은 다음을 참조하십시오.

- ["S3 REST API를 사용하여 S3 Object Lock 구성"](#)
- ["NetApp 기술 자료: StorageGRID 11.5에서 기존 규정 준수 버킷을 관리하는 방법"](#)

이 작업을 완료하려면 s3:PutBucketCompliance 권한이 있거나 루트 계정이어야 합니다.

PUT 버킷 규정 준수 요청을 발행할 때는 규정 준수 설정의 모든 필드에 값을 지정해야 합니다.

요청 예시

이 예시 요청은 mybucket 라는 이름의 버킷에 대한 규정 준수 설정을 수정합니다. 이 예시에서는 mybucket 버킷에 저장된 객체가 그리드에 수집된 시점부터 1년이 아닌 2년(1,051,200분) 동안 보존됩니다. 이 버킷에는 법적 보존이 설정되어 있지 않습니다. 각 객체는 2년 후 자동으로 삭제됩니다.

```

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>

```

이름	설명
RetentionPeriodMinutes	이 버킷에 추가된 객체의 보존 기간(분)입니다. 보존 기간은 객체가 그리드에 수집된 시점부터 시작됩니다. 중요 RetentionPeriodMinutes에 새 값을 지정할 때는 버킷의 현재 보존 기간보다 크거나 같은 값을 지정해야 합니다. 버킷의 보존 기간이 설정되면 해당 값을 줄일 수 없으며, 늘릴 수만 있습니다.
LegalHold	- 참: 이 버킷은 현재 법적 보존 조치가 적용되어 있습니다. 이 버킷의 객체는 보존 기간이 만료되었더라도 법적 보존 조치가 해제될 때까지 삭제할 수 없습니다. - 거짓: 이 버킷은 현재 법적 보존 상태가 아닙니다. 이 버킷의 객체는 보존 기간이 만료되면 삭제될 수 있습니다.
AutoDelete	- True: 이 버킷에 있는 객체는 보존 기간이 만료되면 자동으로 삭제됩니다. 단, 버킷이 법적 보존 상태에 있는 경우는 예외입니다. - 거짓: 이 버킷의 객체는 보존 기간이 만료되어도 자동으로 삭제되지 않습니다. 삭제해야 하는 경우 수동으로 삭제해야 합니다.

규정 준수 설정의 일관성

PUT 버킷 규정 준수 요청을 사용하여 S3 버킷의 규정 준수 설정을 업데이트하면 StorageGRID는 그리드 전체에서 버킷의 메타데이터를 업데이트하려고 시도합니다. 기본적으로 StorageGRID는 **Strong-global** 일관성을 사용하여 모든 데이터 센터 사이트와 버킷 메타데이터를 포함하는 모든 스토리지 노드가 변경된 규정 준수 설정에 대해 쓰기 후 읽기 일관성을 갖도록 보장합니다.

데이터 센터 사이트 또는 해당 사이트의 여러 스토리지 노드를 사용할 수 없어 StorageGRID가 **Strong-global** 일관성을 달성할 수 없는 경우, 응답에 대한 HTTP 상태 코드는 503 Service Unavailable.

이 응답을 받으면 그리드 관리자에게 문의하여 필요한 스토리지 서비스를 최대한 빨리 사용할 수 있도록 해야 합니다. 그리드 관리자가 각 사이트에서 충분한 스토리지 노드를 사용할 수 있도록 확보할 수 없는 경우, 기술 지원 팀에서 **Strong-site** 일관성을 강제로 적용하여 실패한 요청을 다시 시도하도록 안내할 수 있습니다.



기술 지원 팀의 지시가 있거나 해당 수준 사용의 잠재적 결과를 완전히 이해하지 않는 한, PUT 버킷 규정 준수를 위해 **Strong-site** 일관성을 강제로 적용하지 마십시오.

일관성 수준을 *강력한 사이트(Strong-site)*로 낮추면 StorageGRID는 업데이트된 규정 준수 설정이 해당 사이트 내의 클라이언트 요청에 대해서만 쓰기 후 읽기 일관성을 유지하도록 보장합니다. 즉, 모든 사이트와 스토리지 노드를 사용할 수 있을 때까지 StorageGRID 시스템은 해당 버킷에 대해 일시적으로 여러 개의 일관되지 않은 설정을 유지할 수 있습니다. 이러한 일관되지 않은 설정은 여기치 않고 바람직하지 않은 동작을 초래할 수 있습니다. 예를 들어, 버킷을 법적 보존 상태로 설정한 후 일관성 수준을 낮추면 버킷의 이전 규정 준수 설정(즉, 법적 보존 해제)이 일부 데이터 센터 사이트에서 계속 적용될 수 있습니다. 결과적으로, 법적 보존 상태라고 생각했던 객체가 보존 기간이 만료되면 사용자 또는 AutoDelete(활성화된 경우)에 의해 삭제될 수 있습니다.

Strong-site 일관성 사용을 강제하려면 PUT Bucket 규정 준수 요청을 다시 실행하고 다음과 같이 Consistency-Control HTTP 요청 헤더를 포함하십시오.

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

오류 응답

- 버킷이 규정을 준수하도록 생성되지 않은 경우 응답의 HTTP 상태 코드는 `404 Not Found`입니다.
- 요청의 `RetentionPeriodMinutes`이 버킷의 현재 보존 기간보다 짧은 경우 HTTP 상태 코드는 `400 Bad Request`입니다.

관련 정보

["사용 중단 예정: 규정 준수를 위한 PUT 버킷 요청 수정"](#)

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.