S3 플랫폼 서비스 관리

StorageGRID software

NetApp
July 23, 2026

목차

S3 플랫폼 서비스 관리

S3 플랫폼 서비스

StorageGRID용 플랫폼 서비스에 대해 알아보십시오

플랫폼 서비스를 구현하기 전에 해당 서비스 사용에 대한 개요 및 고려 사항을 검토하십시오.

S3에 대한 자세한 내용은 "S3 REST API 사용"을 참조하십시오.

플랫폼 서비스 개요

StorageGRID 플랫폼 서비스를 이용하면 이벤트 알림과 S3 객체 및 객체 메타데이터의 복사본을 외부 대상으로 전송할 수 있으므로 하이브리드 클라우드 전략을 구현하는 데 도움이 됩니다.

플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 환경 외부에 있기 때문에, 플랫폼 서비스를 통해 외부 스토리지 리소스, 알림 서비스, 데이터 검색 또는 분석 서비스를 활용하여 강력한 기능과 유연성을 확보할 수 있습니다.

하나의 S3 버킷에 대해 다양한 플랫폼 서비스를 조합하여 구성할 수 있습니다. 예를 들어, StorageGRID S3 버킷에서 "CloudMirror 서비스" 및 "알림"를 모두 구성하여 특정 객체를 Amazon Simple Storage Service(S3)에 미러링하는 동시에 각 객체에 대한 알림을 타사 모니터링 애플리케이션으로 전송하여 AWS 비용을 추적할 수 있습니다.

플랫폼 서비스 사용은 StorageGRID 관리자가 Grid Manager 또는 Grid Management API를 사용하여 각 테넌트 계정에 대해 활성화해야 합니다.

플랫폼 서비스 구성 방법

플랫폼 서비스는 "테넌트 관리자" 또는 "테넌트 관리 API"를 사용하여 구성한 외부 엔드포인트와 통신합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon SNS 토픽, 웹훅 엔드포인트 또는 로컬, AWS 또는 다른 곳에 호스팅된 Elasticsearch 클러스터와 같은 외부 대상을 나타냅니다.

외부 엔드포인트를 생성한 후 버킷에 XML 구성을 추가하여 버킷에 대한 플랫폼 서비스를 활성화할 수 있습니다. XML 구성은 버킷이 처리해야 할 객체, 버킷이 수행해야 할 작업, 그리고 서비스에 사용할 엔드포인트를 지정합니다.

구성하려는 각 플랫폼 서비스에 대해 별도의 XML 구성을 추가해야 합니다. 예를 들면 다음과 같습니다.

- 키가 `/images`로 시작하는 모든 객체를 Amazon S3 버킷으로 복제하려면 소스 버킷에 복제 구성을 추가해야 합니다.
- 이러한 객체가 버킷에 저장될 때 알림을 보내려면 알림 구성을 추가해야 합니다.
- 이러한 객체의 메타데이터를 색인화하려면 검색 통합을 구현하는 데 사용되는 메타데이터 알림 구성을 추가해야 합니다.

구성 XML의 형식은 StorageGRID 플랫폼 서비스를 구현하는 데 사용되는 S3 REST API에 의해 결정됩니다.

플랫폼 서비스	**S3 REST API**	참조하십시오
CloudMirror 복제	• GetBucketReplication • PutBucketReplication	• "CloudMirror 복제" • "버킷에 대한 작업"
알림	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "알림" • "버킷에 대한 작업"
검색 통합	• GET 버킷 메타데이터 알림 구성 • PUT 버킷 메타데이터 알림 구성	• "검색 통합" • "StorageGRID 사용자 지정 작업"

플랫폼 서비스 사용 시 고려 사항

고려 사항	세부 정보
대상 엔드포인트 모니터링	각 대상 엔드포인트의 가용성을 모니터링해야 합니다. 대상 엔드포인트에 대한 연결이 장시간 끊어지고 요청이 대량으로 누적된 경우, StorageGRID에 대한 추가 클라이언트 요청(예: PUT 요청)이 실패할 수 있습니다. 엔드포인트에 다시 연결할 수 있게 되면 이러한 실패한 요청을 재시도해야 합니다.
대상 엔드포인트 스로틀링	StorageGRID 소프트웨어는 버킷으로 들어오는 S3 요청 속도가 대상 엔드포인트가 요청을 수신할 수 있는 속도를 초과하는 경우 해당 요청 속도를 제한할 수 있습니다. 속도 제한은 대상 엔드포인트로 전송될 요청이 누적되어 대기 중인 경우에만 발생합니다. 눈에 띄는 유일한 영향은 수신 S3 요청 실행 시간이 더 오래 걸린다는 것입니다. 성능 저하가 현저하게 감지되기 시작하면 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하면 클라이언트의 S3 작업(예: PUT 요청)이 결국 실패하게 됩니다. CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 더 큰 영향을 받을 가능성이 높습니다.
순서 보장	StorageGRID는 사이트 내 객체에 대한 작업 순서를 보장합니다. 객체에 대한 모든 작업이 동일한 사이트 내에서 이루어지는 한, 최종 객체 상태(복제용)는 항상 StorageGRID의 상태와 동일합니다. StorageGRID는 StorageGRID 사이트 간 작업 시 요청 순서를 최대한 정확하게 유지하려고 노력합니다. 예를 들어, 처음에 A 사이트에 객체를 기록한 후 나중에 B 사이트에서 동일한 객체를 덮어쓰는 경우, CloudMirror가 대상 버킷에 복제하는 최종 객체가 최신 객체라는 보장은 없습니다.

고려 사항	세부 정보
ILM 기반 객체 삭제	AWS CRR 및 Amazon Simple Notification Service의 삭제 동작과 일치하도록, StorageGRID ILM 규칙으로 인해 소스 버킷의 객체가 삭제될 경우 CloudMirror 및 이벤트 알림 요청이 전송되지 않습니다. 예를 들어, ILM 규칙에 따라 객체가 14일 후에 삭제되는 경우 CloudMirror 또는 이벤트 알림 요청이 전송되지 않습니다. 이와 대조적으로, ILM으로 인해 객체가 삭제될 때 검색 통합 요청이 전송됩니다.
Kafka 엔드포인트 사용	Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 따라서 Kafka 브로커 구성에서 `ssl.client.auth`을(를) `required`로 설정한 경우 Kafka 엔드포인트 구성 문제가 발생할 수 있습니다. Kafka 엔드포인트 인증에는 다음과 같은 인증 유형이 사용됩니다. 이러한 유형은 Amazon SNS와 같은 다른 엔드포인트 인증에 사용되는 유형과 다르며, 사용자 이름과 암호 자격 증명이 필요합니다. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 참고**:** 구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에는 적용되지 않습니다.

CloudMirror 복제 서비스 사용 시 고려 사항

고려 사항	세부 정보
복제 상태	StorageGRID는 `x-amz-replication-status` 헤더를 지원하지 않습니다.
객체 크기	CloudMirror 복제 서비스를 통해 대상 버킷으로 복제할 수 있는 객체의 최대 크기는 5TiB이며, 이는 지원되는 최대 객체 크기와 동일합니다. 참고: 단일 PutObject 작업의 최대 권장 크기는 5GiB(5,368,709,120바이트)입니다. 객체 크기가 5GiB보다 큰 경우 멀티파트 업로드를 사용하십시오.
버킷 버전 관리 및 버전 ID	StorageGRID의 소스 S3 버킷에 버전 관리가 활성화되어 있는 경우 대상 버킷에도 버전 관리를 활성화해야 합니다. 버전 관리를 사용할 때, S3 프로토콜의 제한 사항으로 인해 대상 버킷에서 객체 버전의 순서는 CloudMirror 서비스에서 보장되지 않고 최선을 다해 유지된다는 점에 유의하십시오. 참고: StorageGRID의 소스 버킷에 대한 버전 ID는 대상 버킷의 버전 ID와 관련이 없습니다.

고려 사항	세부 정보
객체 버전에 대한 태깅	CloudMirror 서비스는 S3 프로토콜의 제한 사항으로 인해 버전 ID를 제공하는 PutObjectTagging 또는 DeleteObjectTagging 요청을 복제하지 않습니다. 소스와 대상의 버전 ID가 서로 관련이 없기 때문에 특정 버전 ID에 대한 태그 업데이트가 복제되도록 보장할 방법이 없습니다. 반면, CloudMirror 서비스는 버전 ID를 지정하지 않는 PutObjectTagging 요청이나 DeleteObjectTagging 요청은 복제합니다. 이러한 요청은 최신 키(또는 버킷에 버전이 지정된 경우 최신 버전)에 대한 태그를 업데이트합니다. 태그가 포함된 일반적인 데이터 수집(태그 업데이트 제외)도 복제됩니다.
멀티파트 업로드 및 `ETag` 값	멀티파트 업로드를 사용하여 업로드된 객체를 미러링할 때 CloudMirror 서비스는 파트를 보존하지 않습니다. 따라서 미러링된 객체의 `ETag` 값은 원본 객체의 `ETag` 값과 다릅니다.
SSE-C로 암호화된 객체(고객이 제공한 키를 사용한 서버 측 암호화)	CloudMirror 서비스는 SSE-C로 암호화된 객체를 지원하지 않습니다. CloudMirror 복제를 위해 소스 버킷에 객체를 수집하려고 할 때 요청에 SSE-C 요청 헤더가 포함되어 있으면 작업이 실패합니다.
S3 객체 잠금이 활성화된 버킷	S3 객체 잠금이 활성화된 소스 또는 대상 버킷의 경우 복제가 지원되지 않습니다.

StorageGRID CloudMirror 복제 서비스에 대해 알아보세요

StorageGRID 버킷에 추가된 특정 객체를 하나 이상의 외부 대상 버킷으로 복제하도록 하려면 S3 버킷에 대해 CloudMirror 복제를 활성화할 수 있습니다.

예를 들어, CloudMirror 복제를 사용하여 특정 고객 기록을 Amazon S3에 미러링한 다음 AWS 서비스를 활용하여 데이터에 대한 분석을 수행할 수 있습니다.

CloudMirror 소스 버킷에 S3 객체 잠금이 활성화된 경우 CloudMirror 복제가 지원되지 않습니다.

CloudMirror 및 ILM

CloudMirror 복제는 그리드의 활성 ILM 정책과 독립적으로 작동합니다. CloudMirror 서비스는 객체가 소스 버킷에 저장되는 즉시 복제하여 가능한 한 빨리 대상 버킷으로 전달합니다. 복제된 객체의 전달은 객체 수집이 성공했을 때 시작됩니다.

CloudMirror 및 크로스그리드 복제

CloudMirror 복제는 크로스 그리드 복제 기능과 중요한 유사점과 차이점을 가지고 있습니다. 자세한 내용은 "크로스 그리드 복제와 CloudMirror 복제 비교"을 참조하십시오.

CloudMirror 및 S3 버킷

CloudMirror 복제는 일반적으로 외부 S3 버킷을 대상으로 구성됩니다. 하지만 다른 StorageGRID 배포 또는 S3 호환 서비스를 대상으로 복제를 구성할 수도 있습니다.

기존 버킷

CloudMirror 복제를 기존 버킷에 대해 활성화하면 해당 버킷에 새로 추가된 객체만 복제됩니다. 버킷에 이미 있는 객체는 복제되지 않습니다. 기존 객체를 강제로 복제하려면 객체 복사를 수행하여 기존 객체의 메타데이터를 업데이트하면 됩니다.

> CloudMirror 복제를 사용하여 객체를 Amazon S3 대상으로 복사하는 경우, Amazon S3는 각 PUT 요청 헤더 내 사용자 정의 메타데이터의 크기를 2KB로 제한한다는 점에 유의하십시오. 객체의 사용자 정의 메타데이터가 2KB를 초과하는 경우 해당 객체는 복제되지 않습니다.

여러 대상 버킷

단일 버킷의 객체를 여러 대상 버킷으로 복제하려면 복제 구성 XML에서 각 규칙에 대한 대상을 지정해야 합니다. 객체를 동시에 두 개 이상의 버킷으로 복제할 수는 없습니다.

버전 관리 버킷 또는 버전 관리되지 않는 버킷

버전 관리되는 버킷 또는 버전 관리되지 않는 버킷에서 CloudMirror 복제를 구성할 수 있습니다. 대상 버킷은 버전 관리되는 버킷이거나 버전 관리되지 않는 버킷일 수 있습니다. 버전 관리되는 버킷과 버전 관리되지 않는 버킷의 어떠한 조합도 사용할 수 있습니다. 예를 들어, 버전 관리되지 않는 소스 버킷의 대상으로 버전 관리되는 버킷을 지정하거나 그 반대로 지정할 수 있습니다. 버전 관리되지 않는 버킷 간에 복제할 수도 있습니다.

삭제, 복제 루프 및 이벤트

삭제 동작

이는 Amazon S3 서비스의 교차 리전 복제(CRR)와 동일한 삭제 동작입니다. 소스 버킷에서 객체를 삭제해도 대상 버킷의 복제된 객체는 삭제되지 않습니다. 소스 및 대상 버킷 모두 버전 관리가 적용된 경우 삭제 마커가 복제됩니다. 대상 버킷에 버전 관리가 적용되지 않은 경우 소스 버킷에서 객체를 삭제해도 삭제 마커가 대상 버킷으로 복제되지 않으며 대상 객체도 삭제되지 않습니다.

복제 루프로부터의 보호

객체가 대상 버킷으로 복제될 때 StorageGRID는 해당 객체를 "복제본"으로 표시합니다. 대상 StorageGRID 버킷은 복제본으로 표시된 객체를 다시 복제하지 않으므로 의도치 않은 복제 루프를 방지할 수 있습니다. 이 복제본 표시는 StorageGRID 내부적으로 처리되며, Amazon S3 버킷을 대상으로 사용할 때 AWS CRR을 활용하는 데 영향을 미치지 않습니다.

> 복제본을 표시하는 데 사용되는 사용자 지정 헤더는 `x-ntap-sg-replica`입니다. 이 표시는 계단식 미러링을 방지합니다. StorageGRID는 두 그리드 간의 양방향 CloudMirror를 지원합니다.

대상 버킷의 이벤트

대상 버킷의 이벤트 고유성 및 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행되는 작업으로 인해 소스 객체의 동일한 복사본이 대상에 두 개 이상 전달될 수 있습니다. 드물지만, 동일한 객체가 두 개 이상의 StorageGRID 사이트에서 동시에 업데이트되는 경우 대상 버킷의 작업 순서가 소스 버킷의 이벤트 순서와 일치하지 않을 수 있습니다.

S3 버킷에 대한 StorageGRID 이벤트 알림에 대해 알아보십시오

StorageGRID가 지정된 이벤트에 대한 알림을 대상 Kafka 클러스터, 웹훅 엔드포인트 또는 Amazon Simple Notification Service로 전송하도록 하려면 S3 버킷에 대한 이벤트 알림을 활성화할 수 있습니다.

예를 들어, 버킷에 추가되는 각 객체에 대해 관리자에게 알림을 보내도록 구성할 수 있습니다. 여기서 객체는 중요한

시스템 이벤트와 관련된 로그 파일을 나타냅니다.

이벤트 알림은 알림 구성에 지정된 대로 소스 버킷에서 생성되어 대상으로 전달됩니다. 객체와 관련된 이벤트가 성공적으로 처리되면 해당 이벤트에 대한 알림이 생성되어 전달 대기열에 추가됩니다.

알림의 고유성과 순서는 보장되지 않습니다. 전달 성공을 보장하기 위해 수행되는 작업으로 인해 동일한 이벤트에 대한 알림이 대상에 두 개 이상 전달될 수 있습니다. 또한 전달이 비동기적으로 이루어지기 때문에, 특히 서로 다른 StorageGRID 사이트에서 시작된 작업의 경우, 대상에서의 알림 시간 순서가 소스 버킷의 이벤트 순서와 일치한다는 보장은 없습니다. Amazon S3 설명서에 설명된 대로 이벤트 메시지의 `sequencer` 키를 사용하여 특정 객체에 대한 이벤트 순서를 확인할 수 있습니다.

StorageGRID 이벤트 알림은 일부 제한 사항이 있지만 Amazon S3 API를 따릅니다.

- 지원되는 이벤트 유형은 다음과 같습니다.
  - s3:ObjectCreated:
  - s3:ObjectCreated:Put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:
  - s3:ObjectRemoved:Delete
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- StorageGRID에서 전송된 이벤트 알림은 표준 JSON 형식을 사용하지만, 아래 표와 같이 일부 키는 포함하지 않고 다른 키에는 특정 값을 사용합니다.

키 이름	**StorageGRID** 값
eventSource	`sgws:s3`
awsRegion	포함되지 않음
x-amz-id-2	포함되지 않음
arn	`urn:sgws:s3:::bucket_name`

StorageGRID 검색 통합 서비스에 대해 알아보십시오

외부 검색 및 데이터 분석 서비스를 객체 메타데이터에 사용하려는 경우 S3 버킷에 대한 검색 통합을 활성화할 수 있습니다.

검색 통합 서비스는 StorageGRID 의 사용자 지정 서비스로, 객체가 생성되거나 삭제될 때, 또는 메타데이터나 태그가 업데이트될 때마다 S3 객체 메타데이터를 대상 엔드포인트로 자동으로 비동기 전송합니다. 대상 서비스에서 제공하는 정교한 검색, 데이터 분석, 시각화 또는 머신러닝 도구를 사용하여 객체 데이터를 검색, 분석하고 유용한 정보를 얻을 수 있습니다.

예를 들어, S3 객체 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷 전체에서 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.

S3 객체 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만, 객체의 S3 객체 잠금 메타데이터(보존 기한 및 법적 보존 상태 포함)는 Elasticsearch로 전송되는 메타데이터에 포함되지 않습니다.

> ⓘ 검색 통합 서비스는 객체 메타데이터를 대상으로 전송하기 때문에 해당 구성 XML을 "메타데이터 알림 구성 XML"이라고 합니다. 이 구성 XML은 이벤트 알림을 활성화하는 데 사용되는 "알림 구성 XML"과는 다릅니다.

검색 통합 및 **S3** 버킷

버전 관리 여부와 관계없이 모든 버킷에 대해 검색 통합 서비스를 활성화할 수 있습니다. 검색 통합은 작업할 객체와 객체 메타데이터의 대상을 지정하는 메타데이터 알림 구성 XML을 버킷에 연결하여 구성합니다.

메타데이터 알림은 버킷 이름, 객체 이름, 그리고 버전 ID(있는 경우)로 구성된 JSON 문서 형식으로 생성됩니다. 각 메타데이터 알림에는 객체의 모든 태그 및 사용자 메타데이터 외에도 객체에 대한 표준 시스템 메타데이터 세트가 포함됩니다.

> ⓘ 태그 및 사용자 메타데이터의 경우, StorageGRID는 날짜와 숫자를 문자열 또는 S3 이벤트 알림으로 Elasticsearch에 전달합니다. Elasticsearch가 이러한 문자열을 날짜 또는 숫자로 해석하도록 구성하려면 동적 필드 매핑 및 날짜 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.

검색 알림

메타데이터 알림은 다음과 같은 경우에 생성되어 전송 대기열에 추가됩니다.

- 객체가 생성되었습니다.
- 객체가 삭제됩니다. 여기에는 그리드의 ILM 정책 작동으로 인해 객체가 삭제되는 경우도 포함됩니다.
- 객체 메타데이터 또는 태그가 추가, 업데이트 또는 삭제됩니다. 메타데이터 업데이트 시에는 변경된 값뿐만 아니라 전체 메타데이터 및 태그 세트가 항상 전송됩니다.

버킷에 메타데이터 알림 구성 XML을 추가하면 새로 생성하는 모든 객체와 데이터, 사용자 메타데이터 또는 태그를 업데이트하여 수정하는 모든 객체에 대해 알림이 전송됩니다. 그러나 버킷에 이미 있는 객체에 대해서는 알림이 전송되지 않습니다. 버킷에 있는 모든 객체의 객체 메타데이터가 대상으로 전송되도록 하려면 다음 중 하나를 수행해야 합니다.

- 버킷을 생성한 직후, 그리고 객체를 추가하기 전에 검색 통합 서비스를 구성하십시오.
- 버킷에 이미 있는 모든 객체에 대해 메타데이터 알림 메시지가 대상으로 전송되도록 하는 작업을 수행합니다.

검색 통합 서비스 및 **Elasticsearch**

StorageGRID 검색 통합 서비스는 Elasticsearch 클러스터를 대상으로 지원합니다. 다른 플랫폼 서비스와 마찬가지로, 대상은 서비스의 구성 XML에서 URN이 사용되는 엔드포인트에 지정됩니다. "NetApp 상호 운용성 매트릭스 도구"을 사용하여 지원되는 Elasticsearch 버전을 확인하십시오.

플랫폼 서비스 엔드포인트 관리

StorageGRID에서 플랫폼 서비스 엔드포인트 구성

버킷에 대한 플랫폼 서비스를 구성하기 전에 플랫폼 서비스의 대상으로 사용할 엔드포인트를 하나 이상 구성해야 합니다.

플랫폼 서비스에 대한 액세스는 StorageGRID 관리자가 테넌트별로 활성화합니다. 플랫폼 서비스 엔드포인트를 생성하거나 사용하려면, 스토리지 노드가 외부 엔드포인트 리소스에 액세스할 수 있도록 네트워킹이 구성된 그리드에서 엔드포인트 관리 또는 루트 액세스 권한이 있는 테넌트 사용자여야 합니다. 단일 테넌트에 대해 최대 500개의 플랫폼 서비스 엔드포인트를 구성할 수 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하십시오.

플랫폼 서비스 엔드포인트란 무엇인가요**?**

플랫폼 서비스 엔드포인트는 StorageGRID가 외부 대상에 액세스하는 데 필요한 정보를 지정합니다.

예를 들어 StorageGRID 버킷의 객체를 Amazon S3 버킷으로 복제하려면 StorageGRID가 Amazon의 대상 버킷에 액세스하는 데 필요한 정보와 자격 증명이 포함된 플랫폼 서비스 엔드포인트를 생성해야 합니다.

각 플랫폼 서비스 유형에는 고유한 엔드포인트가 필요하므로 사용하려는 각 플랫폼 서비스에 대해 최소 하나 이상의 엔드포인트를 구성해야 합니다. 플랫폼 서비스 엔드포인트를 정의한 후에는 해당 엔드포인트의 URN을 서비스 활성화에 사용되는 구성 XML의 대상으로 사용합니다.

여러 소스 버킷에 대해 동일한 엔드포인트를 대상으로 사용할 수 있습니다. 예를 들어, 여러 소스 버킷에서 객체 메타데이터를 동일한 검색 통합 엔드포인트로 전송하도록 구성하여 여러 버킷에서 검색을 수행할 수 있습니다. 또한 소스 버킷이 여러 엔드포인트를 대상으로 사용하도록 구성할 수 있으므로 객체 생성 알림은 하나의 Amazon Simple Notification Service(Amazon SNS) 주제로, 객체 삭제 알림은 다른 Amazon SNS 주제로 전송하는 등의 작업을 수행할 수 있습니다.

CloudMirror 복제용 엔드포인트

StorageGRID는 S3 버킷을 나타내는 복제 엔드포인트를 지원합니다. 이러한 버킷은 Amazon Web Services, 동일하거나 원격의 StorageGRID 배포 환경, 또는 다른 서비스에 호스팅될 수 있습니다.

알림 엔드포인트

StorageGRID는 Amazon SNS, Kafka 및 웹훅 엔드포인트를 지원합니다. Simple Queue Service(SQS) 및 AWS Lambda 엔드포인트는 지원하지 않습니다.

Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 따라서 Kafka 브로커 구성에서 `ssl.client.auth`을(를) `required`로 설정한 경우 Kafka 엔드포인트 구성 문제가 발생할 수 있습니다.

검색 통합 서비스의 엔드포인트

StorageGRID는 Elasticsearch 클러스터를 나타내는 검색 통합 엔드포인트를 지원합니다. 이러한 Elasticsearch 클러스터는 로컬 데이터 센터에 있거나 AWS 클라우드 또는 다른 곳에 호스팅될 수 있습니다.

검색 통합 엔드포인트는 특정 Elasticsearch 인덱스 및 유형을 참조합니다. StorageGRID에서 엔드포인트를 생성하기 전에 Elasticsearch에서 인덱스를 생성해야 합니다. 그렇지 않으면 엔드포인트 생성이 실패합니다. 유형은 엔드포인트를 생성하기 전에 생성할 필요가 없습니다. StorageGRID는 객체 메타데이터를 엔드포인트로 전송할 때 필요한 경우 유형을 생성합니다.

관련 정보

"StorageGRID 관리"

StorageGRID 플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오

플랫폼 서비스 엔드포인트를 생성할 때는 고유 리소스 이름(URN)을 지정해야 합니다. 이 URN은 플랫폼 서비스의 구성 XML을 생성할 때 엔드포인트를 참조하는 데 사용됩니다. 각 엔드포인트의 URN은 고유해야 합니다.

StorageGRID는 플랫폼 서비스 엔드포인트를 생성할 때 유효성을 검사합니다. 플랫폼 서비스 엔드포인트를 생성하기 전에 엔드포인트에 지정된 리소스가 존재하고 접근 가능한지 확인하십시오.

URN 요소

플랫폼 서비스 엔드포인트의 URN은 다음과 같이 `arn:aws` 또는 `urn:mysite`로 시작해야 합니다.

- 서비스가 Amazon Web Services(AWS)에서 호스팅되는 경우 다음을 사용하십시오 `arn:aws`
- 서비스가 Google Cloud Platform(GCP)에서 호스팅되는 경우 다음을 사용하세요. `arn:aws`
- 서비스가 로컬에서 호스팅되는 경우 다음을 사용하십시오 `urn:mysite`

예를 들어 StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 URN을 지정하는 경우 URN은 `urn:sgws`으로 시작할 수 있습니다.

URN의 다음 요소는 다음과 같이 플랫폼 서비스 유형을 지정합니다.

서비스	유형
CloudMirror 복제	`s3`
알림	`sns`, `kafka` 또는 `webhook`
검색 통합	`es`

예를 들어 StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 URN을 계속 지정하려면 `s3`을 추가하여 `urn:sgws:s3`을 얻습니다.

대부분의 엔드포인트에서 URN의 마지막 요소는 대상 URI의 특정 대상 리소스를 식별합니다(예: `sns-topic-name`).

웹훅 엔드포인트의 경우 대상 리소스는 대상 URI 자체입니다.

서비스	특정 리소스
CloudMirror 복제	`bucket-name`

서비스	특정 리소스
알림	`sns-topic-name` 또는 `kafka-topic-name` 참고: 웹훅 엔드포인트의 경우, URN의 마지막 요소는 엔드포인트의 URN이 고유하기만 하면 어떤 문자열이든 될 수 있습니다.
검색 통합	`domain-name/index-name/type-name` 참고: Elasticsearch 클러스터가 인덱스를 자동으로 생성하도록 구성되어 있지 않은 경우, 엔드포인트를 생성하기 전에 인덱스를 수동으로 생성해야 합니다.

AWS 및 **GCP**에서 호스팅되는 서비스에 대한 **URN**

AWS 및 GCP 엔티티의 경우 전체 URN은 유효한 AWS ARN입니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

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

- 알림:

```
arn:aws:sns:region:account-id:topic-name
```

- 검색 통합:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> AWS 검색 통합 엔드포인트의 경우, `domain-name`에는 여기에 표시된 것처럼 리터럴 문자열 `domain/`이 포함되어야 합니다.

로컬에서 호스팅되는 서비스에 대한 **URN**

클라우드 서비스 대신 로컬 호스팅 서비스를 사용하는 경우, 세 번째와 마지막 위치에 필수 요소가 포함되어 있는 한, 유효하고 고유한 URN을 생성하는 어떤 방식으로든 URN을 지정할 수 있습니다. 선택 사항으로 표시된 요소는 비워두거나, 리소스를 식별하고 URN을 고유하게 만드는 데 도움이 되는 방식으로 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

```
urn:mysite:s3:optional:optional:bucket-name
```

StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 경우, 다음으로 시작하는 유효한 URN을 지정할 수

있습니다 `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- 알림:

  Amazon Simple Notification Service 엔드포인트를 지정하십시오.

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Kafka 엔드포인트를 지정합니다:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

  웹훅 엔드포인트를 지정합니다.

  ```
  urn:mysite:webhook:optional:optional:webhook-name
  ```

- 검색 통합:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  로컬에서 호스팅되는 검색 통합 엔드포인트의 경우, 해당 `domain-name` 요소는 엔드포인트의 URN이 고유한 한 어떤 문자열이든 될 수 있습니다.

StorageGRID 플랫폼 서비스 엔드포인트를 생성합니다.

플랫폼 서비스를 활성화하려면 먼저 올바른 유형의 엔드포인트를 하나 이상 생성해야 합니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.
- ${post_edited_translations.segment}
  - CloudMirror 복제: S3 버킷
  - 이벤트 알림: Amazon Simple Notification Service(Amazon SNS) 토픽, Kafka 토픽 또는 웹훅 엔드포인트
  - 검색 알림: 타겟 클러스터가 인덱스를 자동으로 생성하도록 구성되어 있지 않은 경우 Elasticsearch 인덱스에 대한 알림이 표시됩니다.
- 대상 리소스에 대한 정보를 가지고 있습니다.

◦ URI(Uniform Resource Identifier)의 호스트 및 포트

> StorageGRID 시스템에서 호스팅되는 버킷을 CloudMirror 복제의 엔드포인트로 사용하려는 경우, 입력해야 할 값을 확인하려면 그리드 관리자에게 문의하십시오.

◦ 고유 리소스 이름(URN)

"플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오."

◦ 인증 자격 증명(필요한 경우):

검색 통합 엔드포인트

검색 통합 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키
- 기본 HTTP: 사용자 이름과 비밀번호

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키
- ${post_edited_translations.segment}

Amazon SNS 엔드포인트

Amazon SNS 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키

Kafka 엔드포인트

${post_edited_translations.segment}

- SASL/PLAIN: 사용자 이름 및 비밀번호
- SASL/SCRAM-SHA-256: 사용자 이름 및 비밀번호
- ${post_edited_translations.segment}

◦ 보안 인증서(인증서 확인이 필요한 경우)

- Elasticsearch 보안 기능이 활성화된 경우 연결 테스트를 위한 클러스터 모니터링 권한과 문서 업데이트를 위한 쓰기 인덱스 권한 또는 인덱스 및 인덱스 삭제 권한 모두가 필요합니다.

단계

1. **STORAGE (S3)** > *Platform services endpoints*를 선택합니다. Platform services endpoints 페이지가 나타납니다.
2. *엔드포인트 생성*을 선택합니다.
3. 엔드포인트와 그 용도를 간략하게 설명하는 표시 이름을 입력하십시오.

${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   ```
   https://host:port
   http://host:port
   ```

   포트를 지정하지 않으면 다음 기본 포트가 사용됩니다.

   - HTTPS URI의 경우 포트 443, HTTP URI의 경우 포트 80(대부분의 엔드포인트)
   - HTTPS 및 HTTP URI용 포트 9092 (Kafka 엔드포인트에만 해당)

   예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같을 수 있습니다.

   ```
   https://s3.example.com:10443
   ```

   이 예에서 `s3.example.com`은 StorageGRID 고가용성(HA) 그룹의 가상 IP(VIP)에 대한 DNS 엔트리를 나타내며, `10443`은 로드 밸런서 엔드포인트에 정의된 포트를 나타냅니다.

   가능한 경우 단일 장애 지점을 방지하기 위해 로드 밸런싱 노드의 HA 그룹에 연결해야 합니다.

   마찬가지로 AWS에서 호스팅되는 버킷의 URI는 다음과 같을 수 있습니다.

   ```
   https://s3-aws-region.amazonaws.com
   ```

   엔드포인트가 CloudMirror 복제 서비스에 사용되는 경우, URI에 버킷 이름을 포함하지 마십시오. 버킷 이름은 **URN** 필드에 포함합니다.

5. 엔드포인트의 고유 리소스 이름(URN)을 입력하십시오.

   엔드포인트가 생성된 후에는 해당 엔드포인트의 URN을 변경할 수 없습니다.

6. *Continue*를 선택합니다.
7. *인증 유형*에 대한 값을 선택하십시오.

   웹훅 엔드포인트에 대한 인증을 사용하려면 9단계에서 mTLS(상호 전송 계층 보안)를 구성하십시오.

검색 통합 엔드포인트

검색 통합 엔드포인트에 대한 자격 증명을 입력하거나 업로드하십시오.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.
액세스 키	대상과의 연결을 인증하기 위해 AWS 스타일 자격 증명을 사용합니다.	• 액세스 키 ID • ${post_edited_translations.segment}
기본 HTTP	${post_edited_translations.segment}	• 사용자 이름 • 비밀번호

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트에 대한 자격 증명을 입력하거나 업로드하세요.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.
액세스 키	대상과의 연결을 인증하기 위해 AWS 스타일 자격 증명을 사용합니다.	• 액세스 키 ID • ${post_edited_translations.segment}

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
${post_edited_translations.segment}	대상과의 연결을 인증하기 위해 인증서와 키를 사용합니다.	• 임시 자격 증명 URL • ${post_edited_translations.segment} • 클라이언트 인증서(PEM 파일 업로드) • 클라이언트 개인 키(PEM 파일 업로드, OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식) • 클라이언트 개인 키 암호(선택 사항)

Amazon SNS 엔드포인트

Amazon SNS 엔드포인트에 대한 자격 증명을 입력하거나 업로드하십시오.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.
액세스 키	대상과의 연결을 인증하기 위해 AWS 스타일 자격 증명을 사용합니다.	• 액세스 키 ID • ${post_edited_translations.segment}

Kafka 엔드포인트

Kafka 엔드포인트에 대한 자격 증명을 입력하거나 업로드합니다.

제공하는 자격 증명에는 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
익명의	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 엔드포인트에만 작동합니다.	인증이 필요하지 않습니다.

${post_edited_translations.segment}	설명	**${post_edited_translations.segment}**
SASL/PLAIN	${post_edited_translations.segment}	• 사용자 이름 • 비밀번호
SASL/SCRAM-SHA-256	${post_edited_translations.segment}	• 사용자 이름 • 비밀번호
SASL/SCRAM-SHA-512	챌린지-응답 프로토콜과 SHA-512 해싱을 사용하는 사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 비밀번호

사용자 이름과 비밀번호가 Kafka 클러스터에서 얻은 위임 토큰에서 파생된 경우 *위임된 토큰 인증 사용*을 선택하십시오.

8. *Continue*를 선택합니다.
9. 인증서 확인 라디오 버튼을 선택하여 엔드포인트에 대한 TLS 연결을 확인하는 방법을 선택하십시오.

대부분의 엔드포인트

검색 통합, CloudMirror 복제, Amazon SNS 또는 Kafka 엔드포인트에 대한 TLS 연결을 확인하십시오.

인증서 검증 유형	설명
TLS	엔드포인트 리소스에 대한 TLS 연결에 사용되는 서버 인증서를 검증합니다.
비활성화됨	인증서 확인 기능이 비활성화되었습니다. 이 옵션은 안전하지 않습니다.
사용자 지정 CA 인증서 사용	사용자 지정 CA 인증서는 엔드포인트에 연결할 때 서버의 신원을 확인하는 데 사용됩니다.
운영 체제 CA 인증서 사용	${post_edited_translations.segment}

웹훅 엔드포인트만 해당

웹훅 엔드포인트에 대한 TLS 연결을 확인하십시오.

인증서 검증 유형	설명
TLS	엔드포인트 리소스에 대한 TLS 연결에 사용되는 서버 인증서를 검증합니다.
mTLS	엔드포인트 리소스에 대한 상호 TLS 연결에 사용되는 클라이언트 및 서버 인증서를 검증합니다.
비활성화됨	인증서 확인 기능이 비활성화되었습니다. 이 옵션은 안전하지 않습니다.
사용자 지정 CA 인증서 사용	사용자 지정 CA 인증서는 엔드포인트에 연결할 때 서버의 신원을 확인하는 데 사용됩니다.

${post_edited_translations.segment}

인증서 검증 유형	설명
서버 인증서를 확인하지 않음	서버 인증서 검증을 비활성화합니다. 즉, 서버의 신원이 확인되지 않습니다. 이 옵션은 보안에 취약합니다.
클라이언트 인증서	클라이언트 인증서는 엔드포인트에 연결할 때 클라이언트의 신원을 확인하는 데 사용됩니다.
클라이언트 개인 키	클라이언트 인증서의 개인 키입니다. 암호화된 경우 기존 PKCS #1 형식을 사용해야 합니다(PKCS #8 형식은 지원되지 않습니다).

인증서 검증 유형	설명
클라이언트 개인 키 암호	클라이언트 개인 키를 복호화하는 데 사용할 암호입니다. 개인 키가 암호화되지 않은 경우 이 필드를 비워 두십시오.

10. *테스트 및 엔드포인트 생성*을 선택합니다.
    - 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
    - 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하기 위해 엔드포인트를 수정해야 하는 경우, *엔드포인트 세부 정보로 돌아가기*를 선택하고 정보를 업데이트합니다. 그런 다음 *엔드포인트 테스트 및 생성*을 선택합니다.

> ⓘ 테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다. StorageGRID 관리자에게 문의하십시오.

엔드포인트를 구성한 후에는 해당 URN을 사용하여 플랫폼 서비스를 구성할 수 있습니다.

관련 정보

- "플랫폼 서비스 엔드포인트에 대한 URN을 지정하십시오."
- "CloudMirror 복제 구성"
- "이벤트 알림 구성"
- "검색 통합 서비스 구성"

StorageGRID 플랫폼 서비스 엔드포인트의 연결을 테스트합니다

플랫폼 서비스에 대한 연결이 변경된 경우 엔드포인트에 대한 연결을 테스트하여 대상 리소스가 존재하고 지정한 자격 증명을 사용하여 접근할 수 있는지 확인할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.

이 작업 정보

StorageGRID는 자격 증명에 올바른 권한이 있는지 검증하지 않습니다.

단계

1. **STORAGE (S3)** > *플랫폼 서비스 엔드포인트*를 선택합니다.

   플랫폼 서비스 엔드포인트 페이지가 나타나고 이미 구성된 플랫폼 서비스 엔드포인트 목록이 표시됩니다.

2. 연결을 테스트할 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

3. *연결 테스트*를 선택합니다.
   - 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
   - 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하기 위해 엔드포인트를 수정해야 하는 경우, *구성*을 선택하고 정보를 업데이트합니다. 그런 다음 *테스트 및 변경 사항 저장*을 선택합니다.

StorageGRID에서 플랫폼 서비스 엔드포인트 편집

플랫폼 서비스 엔드포인트의 구성을 편집하여 이름, URI 또는 기타 세부 정보를 변경할 수 있습니다. 예를 들어 만료된 자격 증명을 업데이트하거나 장애 조치를 위해 백업 Elasticsearch 인덱스를 가리키도록 URI를 변경해야 할 수 있습니다. 플랫폼 서비스 엔드포인트의 URN은 변경할 수 없습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. **STORAGE (S3)** > *플랫폼 서비스 엔드포인트*를 선택합니다.

   플랫폼 서비스 엔드포인트 페이지가 나타나고 이미 구성된 플랫폼 서비스 엔드포인트 목록이 표시됩니다.

2. 편집할 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

3. *구성*을 선택합니다.
4. 필요에 따라 엔드포인트의 구성을 변경하십시오.

   엔드포인트가 생성된 후에는 해당 엔드포인트의 URN을 변경할 수 없습니다.

   a. 엔드포인트의 표시 이름을 변경하려면 편집 아이콘 을 선택합니다.
   b. 필요에 따라 URI를 변경하십시오.
   c. 필요에 따라 인증 유형을 변경하십시오.
      - 액세스 키 인증의 경우, *S3 키 편집*을 선택하고 새 액세스 키 ID와 비밀 액세스 키를 붙여넣어 필요에 따라 키를 변경하십시오. 변경 사항을 취소하려면 *S3 키 편집 되돌리기*를 선택하십시오.
      - CAP(C2S 액세스 포털) 인증의 경우, 필요에 따라 임시 자격 증명 URL 또는 선택적 클라이언트 개인 키 암호를 변경하고 새 인증서 및 키 파일을 업로드하십시오.

        클라이언트 개인 키는 OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식이어야 합니다.

   d. 필요에 따라 인증서 확인 방법을 변경하십시오.
5. *테스트 후 변경 사항 저장*을 선택합니다.

◦ 지정된 자격 증명을 사용하여 엔드포인트에 연결할 수 있으면 성공 메시지가 표시됩니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

◦ 엔드포인트 유효성 검사에 실패하면 오류 메시지가 표시됩니다. 오류를 수정하려면 엔드포인트를 수정하고 *테스트 및 변경 사항 저장*을 선택하십시오.

StorageGRID 플랫폼 서비스 엔드포인트를 삭제합니다

연결된 플랫폼 서비스를 더 이상 사용하지 않으려면 엔드포인트를 삭제할 수 있습니다.

시작하기 전에

- 현재 "지원되는 웹 브라우저"을(를) 사용하여 테넌트 관리자에 로그인했습니다.
- 귀하는 "엔드포인트 또는 루트 액세스 권한 관리"이(가) 있는 사용자 그룹에 속해 있습니다.

단계

1. **STORAGE (S3)** > *플랫폼 서비스 엔드포인트*를 선택합니다.

   플랫폼 서비스 엔드포인트 페이지가 나타나고 이미 구성된 플랫폼 서비스 엔드포인트 목록이 표시됩니다.

2. 삭제하려는 각 엔드포인트의 확인란을 선택합니다.

   사용 중인 플랫폼 서비스 엔드포인트를 삭제하면 해당 엔드포인트를 사용하는 모든 버킷에 대해 연결된 플랫폼 서비스가 비활성화됩니다. 아직 완료되지 않은 요청은 모두 삭제됩니다. 삭제된 URN을 더 이상 참조하지 않도록 버킷 구성을 변경하기 전까지는 새로운 요청이 계속 생성됩니다. StorageGRID는 이러한 요청을 복구할 수 없는 오류로 보고합니다.

3. 작업 > *엔드포인트 삭제*를 선택합니다.

   확인 메시지가 나타납니다.

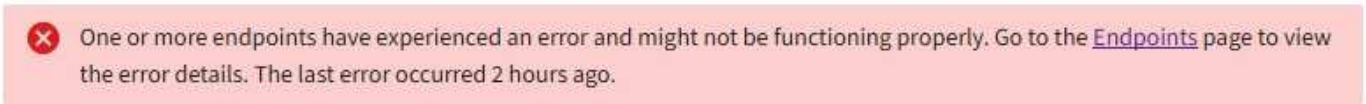
4. *엔드포인트 삭제*를 선택합니다.

StorageGRID 플랫폼 서비스 엔드포인트 오류 해결

StorageGRID가 플랫폼 서비스 엔드포인트와 통신하려고 할 때 오류가 발생하면 대시보드에 메시지가 표시됩니다. 플랫폼 서비스 엔드포인트 페이지의 마지막 오류 열에는 오류가 발생한 시간이 표시됩니다. 엔드포인트 자격 증명과 연결된 권한이 올바르지 않은 경우에는 오류가 표시되지 않습니다.

오류가 발생했는지 확인합니다.

지난 7일 동안 플랫폼 서비스 엔드포인트 오류가 발생한 경우 테넌트 관리자 대시보드에 알림 메시지가 표시됩니다. 플랫폼 서비스 엔드포인트 페이지에서 오류에 대한 자세한 내용을 확인할 수 있습니다.



대시보드에 표시되는 것과 동일한 오류가 플랫폼 서비스 엔드포인트 페이지 상단에도 나타납니다. 자세한 오류 메시지를

보려면 다음을 참조하십시오.

단계

1. 엔드포인트 목록에서 오류가 발생한 엔드포인트를 선택합니다.
2. 엔드포인트 세부 정보 페이지에서 *연결*을 선택합니다. 이 탭에는 엔드포인트에 대한 가장 최근 오류만 표시되며 오류 발생 시점이 표시됩니다. 빨간색 X 아이콘 이 포함된 오류는 지난 7일 이내에 발생한 오류입니다.

오류가 여전히 유효한지 확인하십시오.

일부 오류는 해결된 후에도 마지막 오류 열에 계속 표시될 수 있습니다. 오류가 현재 발생 중인지 확인하거나 해결된 오류를 표에서 강제로 제거하려면 다음 단계를 따르세요.

단계

1. 엔드포인트를 선택합니다.

   엔드포인트 세부 정보 페이지가 나타납니다.

2. * 연결* > *연결 테스트*를 선택합니다.

*연결 테스트*를 선택하면 StorageGRID가 플랫폼 서비스 엔드포인트가 존재하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

엔드포인트 오류 해결

엔드포인트 세부 정보 페이지에서 마지막 오류 메시지를 확인하여 오류 원인을 파악할 수 있습니다. 일부 오류는 엔드포인트를 수정해야 해결할 수 있습니다. 예를 들어, StorageGRID가 올바른 액세스 권한이 없거나 액세스 키가 만료되어 대상 S3 버킷에 액세스할 수 없는 경우 CloudMirroring 오류가 발생할 수 있습니다. 이 경우 메시지는 "엔드포인트 자격 증명 또는 대상 액세스를 업데이트해야 합니다."이며, 세부 정보는 "AccessDenied" 또는 "InvalidAccessKeyId"로 표시됩니다.

오류를 해결하기 위해 엔드포인트를 수정해야 하는 경우, *테스트 및 변경 사항 저장*을 선택하면 StorageGRID가 업데이트된 엔드포인트를 검증하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트 연결은 각 사이트의 한 노드에서 검증됩니다.

단계

1. 엔드포인트를 선택합니다.
2. 엔드포인트 세부 정보 페이지에서 *구성*을 선택합니다.
3. 필요에 따라 엔드포인트 구성을 편집하십시오.
4. * 연결* > *연결 테스트*를 선택합니다.

${post_edited_translations.segment}

StorageGRID 플랫폼 서비스 엔드포인트를 검증할 때, 해당 엔드포인트의 자격 증명을 사용하여 대상 리소스에 연결할 수 있는지 확인하고 기본적인 권한 검사를 수행합니다. 그러나 StorageGRID는 특정 플랫폼 서비스 작업에 필요한 모든 권한을 검증하지는 않습니다. 따라서 플랫폼 서비스를 사용하려고 할 때 오류(예: "403 Forbidden")가 발생하는 경우, 엔드포인트 자격 증명과 연결된 권한을 확인하십시오.

관련 정보

- **StorageGRID** 관리 › 플랫폼 서비스 문제 해결

- "플랫폼 서비스 엔드포인트 생성"
- "플랫폼 서비스 엔드포인트에 대한 연결 테스트"
- "플랫폼 서비스 엔드포인트 편집"

StorageGRID에서 CloudMirror 복제 구성

버킷에 대한 CloudMirror 복제를 활성화하려면 유효한 버킷 복제 구성 XML을 생성하여 적용해야 합니다.

시작하기 전에

- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 이미 복제 소스 역할을 할 버킷을 생성했습니다.
- CloudMirror 복제 대상으로 사용하려는 엔드포인트가 이미 존재하며 해당 URN을 알고 있습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

CloudMirror 복제는 소스 버킷의 객체를 엔드포인트에 지정된 대상 버킷으로 복사합니다.

버킷 복제 및 구성 방법에 대한 일반 정보는 "Amazon Simple Storage Service (S3) 문서: 객체 복제"을 참조하십시오. StorageGRID가 GetBucketReplication, DeleteBucketReplication 및 PutBucketReplication을 구현하는 방법에 대한 자세한 내용은 "버킷에 대한 작업"을 참조하십시오.

> CloudMirror 복제는 크로스 그리드 복제 기능과 중요한 유사점과 차이점을 가지고 있습니다. 자세한 내용은 "크로스 그리드 복제와 CloudMirror 복제 비교"을 참조하십시오.

CloudMirror 복제를 구성할 때 다음 요구 사항 및 특징에 유의하십시오.

- 유효한 버킷 복제 구성 XML을 생성하고 적용할 때는 각 대상에 대해 S3 버킷 엔드포인트의 URN을 사용해야 합니다.
- S3 객체 잠금이 활성화된 소스 또는 대상 버킷의 경우 복제가 지원되지 않습니다.
- CloudMirror 복제를 객체가 포함된 버킷에서 활성화하면 버킷에 새로 추가된 객체는 복제되지만, 버킷에 이미 있는 객체는 복제되지 않습니다. 복제를 시작하려면 기존 객체를 업데이트해야 합니다.
- 복제 구성 XML에서 스토리지 클래스를 지정하면 StorageGRID는 대상 S3 엔드포인트에 대한 작업을 수행할 때 해당 클래스를 사용합니다. 대상 엔드포인트 또한 지정된 스토리지 클래스를 지원해야 합니다. 대상 시스템 공급업체에서 제공하는 권장 사항을 반드시 따르십시오.

단계

1. 원본 버킷에 대한 복제를 활성화합니다.
   - S3 복제 API에 명시된 대로 복제를 활성화하는 데 필요한 복제 구성 XML을 텍스트 편집기를 사용하여 생성합니다.
   - XML을 구성할 때:
     - StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 대한 `Filter`요소 사용을 지원하지 않으며, 객체 버전 삭제 시 V1 규칙을 따릅니다. 자세한 내용은 Amazon의 복제 구성 관련 문서를

참조하십시오.

- 대상으로 S3 버킷 엔드포인트의 URN을 사용합니다.
- 선택적으로 `<StorageClass>` 요소를 추가하고 다음 중 하나를 지정하십시오.
  - `STANDARD`: 기본 스토리지 클래스입니다. 객체를 업로드할 때 스토리지 클래스를 지정하지 않으면 `STANDARD` 스토리지 클래스가 사용됩니다.
  - `STANDARD_IA`: (Standard - infrequent access.) 액세스 빈도는 낮지만 필요할 때 신속한 액세스가 필요한 데이터에 이 스토리지 클래스를 사용하십시오.
  - `REDUCED_REDUNDANCY`: 이 스토리지 클래스는 중요하지 않고 재현 가능한 데이터, 즉 `STANDARD` 스토리지 클래스보다 중복성을 줄여도 되는 데이터에 사용하십시오.
- 구성 XML에 `Role`을 지정하더라도 해당 값은 무시됩니다. 이 값은 StorageGRID에서 사용되지 않습니다.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 대시보드에서 버킷 보기*를 선택하거나 *스토리지**(S3)** > *버킷*을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

4. 플랫폼 서비스 > *복제*를 선택합니다.
5. 복제 활성화 확인란을 선택하십시오.
6. 복제 구성 XML을 텍스트 상자에 붙여넣고 *변경 내용 저장*을 선택합니다.

   > 각 테넌트 계정에 대해 플랫폼 서비스를 활성화하려면 Grid Manager 또는 Grid Management API를 사용하는 StorageGRID 관리자가 필요합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 복제 구성이 올바르게 되어 있는지 확인하십시오.
   a. 복제 구성에 지정된 복제 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞서 보여드린 예시에서처럼 접두사 "2020"과 일치하는 객체가 복제됩니다.

   b. 객체가 대상 버킷에 복제되었는지 확인하십시오.

      작은 오브젝트의 경우 복제가 빠르게 이루어집니다.

관련 정보

"플랫폼 서비스 엔드포인트 생성"

StorageGRID에서 이벤트 알림을 구성합니다

버킷에 대한 알림을 활성화하려면 알림 구성 XML을 생성하고 Tenant Manager를 사용하여 해당 XML을 버킷에 적용하면 됩니다.

시작하기 전에

- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 이미 알림 소스로 사용할 버킷을 생성했습니다.
- 이벤트 알림 대상으로 사용하려는 엔드포인트가 이미 존재하며, 해당 URN을 알고 있습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

이벤트 알림은 알림 구성 XML을 소스 버킷과 연결하여 구성합니다. 알림 구성 XML은 버킷 알림 구성을 위한 S3 규칙을 따르며, 대상 Amazon SNS 토픽, Kafka 토픽 또는 웹훅 엔드포인트는 엔드포인트의 URN으로 지정됩니다.

이벤트 알림 및 구성 방법에 대한 일반 정보는 "Amazon 문서"을 참조하십시오. StorageGRID가 S3 버킷 알림 구성 API를 구현하는 방법에 대한 자세한 내용은 "S3 클라이언트 애플리케이션 구현 지침"을 참조하십시오.

버킷에 대한 이벤트 알림을 구성할 때 다음 요구 사항 및 특징을 참고하십시오.

- 유효한 알림 구성 XML을 생성하고 적용할 때는 각 대상에 대해 이벤트 알림 엔드포인트의 URN을 사용해야 합니다.
- S3 Object Lock이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만, 알림 메시지에는 객체의 S3 Object Lock 메타데이터(보존 기한 및 법적 보존 상태 포함)가 포함되지 않습니다.
- 이벤트 알림을 구성하면 소스 버킷의 객체에 대해 지정된 이벤트가 발생할 때마다 알림이 생성되어 대상으로 사용된 Amazon SNS 토픽, Kafka 토픽 또는 웹훅 엔드포인트로 전송됩니다.
- 객체가 포함된 버킷에 대해 이벤트 알림을 활성화하면 알림 구성이 저장된 후에 수행된 작업에 대해서만 알림이 전송됩니다.

단계

1. 소스 버킷에 대한 알림을 활성화합니다.
    - 텍스트 편집기를 사용하여 S3 알림 API에 명시된 대로 이벤트 알림을 활성화하는 데 필요한 알림 구성 XML을 생성합니다.
    - XML을 구성할 때 대상 토픽으로 이벤트 알림 엔드포인트의 URN을 사용하십시오.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 테넌트 관리자에서 **STORAGE (S3)** > *Buckets*를 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

4. 플랫폼 서비스 > *이벤트 알림*을 선택합니다.
5. 이벤트 알림 활성화 확인란을 선택합니다.
6. 알림 구성 XML을 텍스트 상자에 붙여넣고 *변경 사항 저장*을 선택합니다.

   각 테넌트 계정에 대해 플랫폼 서비스를 활성화하려면 Grid Manager 또는 Grid Management API를 사용하는 StorageGRID 관리자가 필요합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 이벤트 알림이 올바르게 구성되었는지 확인하십시오.

   a. 구성 XML에 설정된 대로 알림을 트리거하기 위한 요구 사항을 충족하는 소스 버킷의 객체에 대해 작업을 수행합니다.

      예시에서는 `images/` 접두사가 붙은 객체가 생성될 때마다 이벤트 알림이 전송됩니다.

   b. 알림이 대상 Amazon SNS 토픽, Kafka 토픽 또는 웹훅 엔드포인트로 전달되었는지 확인하십시오.

      예를 들어, 대상 주제가 Amazon SNS에 호스팅되어 있는 경우, 알림이 전달될 때 이메일을 보내도록 서비스를 구성할 수 있습니다.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+ 대상 토픽에서 알림을 수신하면 StorageGRID 알림에 대한 소스 버킷 구성이 성공적으로 완료된 것입니다.

관련 정보

- "버킷에 대한 알림 이해"
- "S3 REST API 사용"
- "플랫폼 서비스 엔드포인트 생성"

StorageGRID에서 검색 통합 서비스 구성

버킷에 대한 검색 통합을 활성화하려면 검색 통합 XML을 생성하고 Tenant Manager를 사용하여 해당 XML을 버킷에 적용하면 됩니다.

시작하기 전에

- 플랫폼 서비스는 StorageGRID 관리자가 테넌트 계정에 대해 활성화했습니다.
- 이미 S3 버킷을 생성했으며, 해당 버킷의 콘텐츠를 인덱싱하려고 합니다.
- 검색 통합 서비스의 대상으로 사용하려는 엔드포인트가 이미 존재하며, 해당 URN을 가지고 있습니다.
- 귀하는 "모든 버킷 또는 루트 액세스 권한 관리"을(를) 가진 사용자 그룹에 속해 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업 정보

소스 버킷에 대한 검색 통합 서비스를 구성한 후 객체를 생성하거나 객체의 메타데이터 또는 태그를 업데이트하면 객체 메타데이터가 대상 엔드포인트로 전송됩니다.

이미 객체가 포함된 버킷에 대해 검색 통합 서비스를 활성화하면 기존 객체에 대한 메타데이터 알림이 자동으로 전송되지 않습니다. 대상 검색 인덱스에 메타데이터가 추가되도록 하려면 기존 객체를 업데이트해야 합니다.

단계

1. 버킷에 대한 검색 통합을 활성화합니다.

   - 메타데이터 검색 통합을 활성화하는 데 필요한 메타데이터 알림 XML을 생성하려면 텍스트 편집기를 사용하십시오.
   - XML을 구성할 때 대상으로는 검색 통합 엔드포인트의 URN을 사용하십시오.

     객체는 객체 이름의 접두사를 기준으로 필터링할 수 있습니다. 예를 들어, 접두사가 `images`인 객체의 메타데이터는 한 대상으로 보내고, 접두사가 `videos`인 객체의 메타데이터는 다른 대상으로 보낼 수 있습니다. 접두사가 중복되는 구성은 유효하지 않으며 제출 시 거부됩니다. 예를 들어, 접두사가 `test`인 객체에 대한 규칙 하나와 접두사가 `test2`인 객체에 대한 두 번째 규칙이 포함된 구성은 허용되지 않습니다.

     필요에 따라 메타데이터 구성 XML의 예시를 참조하십시오.

     ```
     <MetadataNotificationConfiguration>
      <Rule>
         <Status>Enabled</Status>
         <Prefix></Prefix>
         <Destination>
            <Urn>/Urn>
            </Destination>
      </Rule>
     </MetadataNotificationConfiguration>
     ```

     메타데이터 알림 구성 XML의 요소:

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
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. • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 엔드포인트는 구성 XML을 제출하기 전에 구성되어야 합니다. 그렇지 않으면 구성이 실패하고 404 오류가 발생합니다. URN은 Destination 요소에 포함되어 있습니다.	예

2. 테넌트 관리자에서 **STORAGE (S3)** > *Buckets*를 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 상세 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 검색 통합 * 을 선택합니다.
5. 검색 통합 활성화 확인란을 선택합니다.
6. 메타데이터 알림 구성을 텍스트 상자에 붙여넣고 *변경 사항 저장*을 선택합니다.

   각 테넌트 계정에 대한 플랫폼 서비스는 StorageGRID 관리자가 Grid Manager 또는 관리 API를 사용하여 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 검색 통합 서비스가 올바르게 구성되었는지 확인하십시오.
   a. 구성 XML에 지정된 대로 메타데이터 알림을 트리거하기 위한 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞서 보여드린 예시에서처럼 버킷에 추가되는 모든 객체는 메타데이터 알림을 트리거합니다.

   b. 해당 객체의 메타데이터와 태그가 포함된 JSON 문서가 엔드포인트에 지정된 검색 인덱스에 추가되었는지 확인하십시오.

완료한 후

필요에 따라 다음 방법 중 하나를 사용하여 버킷에 대한 검색 통합을 비활성화할 수 있습니다.

- **STORAGE (S3)** > **Buckets***를 선택하고 ***Enable search integration** 확인란을 선택 해제합니다.

- S3 API를 직접 사용하는 경우, DELETE Bucket 메타데이터 알림 요청을 사용하십시오. S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

예시: 모든 객체에 적용되는 메타데이터 알림 구성

이 예시에서는 모든 객체의 객체 메타데이터가 동일한 대상으로 전송됩니다.

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

예시: 두 개의 규칙이 포함된 메타데이터 알림 구성

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

```
<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>
```

메타데이터 알림 형식

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"
  }
}
```

JSON 문서에 포함된 필드

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

버킷 및 객체 정보

`bucket`: 버킷 이름

`key`: 객체 키 이름

`versionID`: 버전 관리 버킷에 있는 객체의 객체 버전입니다.

`region`: 버킷 영역, 예를 들어 `us-east-1`

시스템 메타데이터

`size`: HTTP 클라이언트에 표시되는 객체 크기(바이트)

`md5`: 객체 해시

사용자 메타데이터

`metadata`: 객체에 대한 모든 사용자 메타데이터(키-값 쌍 형식)

`key:value`

태그

`tags`: 키-값 쌍으로 나타낸 객체에 대해 정의된 모든 객체 태그

```
key:value
```

Elasticsearch에서 결과를 보는 방법

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