S3 플랫폼 서비스 관리

StorageGRID 11.8

NetApp
March 19, 2024

목차

S3 플랫폼 서비스 관리

플랫폼 서비스 관리: 개요

StorageGRID 플랫폼 서비스를 사용하면 S3 오브젝트 및 오브젝트 메타데이터의 이벤트 알림과 복사본을 외부 대상에 보낼 수 있으므로 하이브리드 클라우드 전략을 구현할 수 있습니다.

테넌트 계정에 플랫폼 서비스를 사용할 수 있는 경우 모든 S3 버킷에 대해 다음 서비스를 구성할 수 있습니다.

CloudMirror 복제

사용 "StorageGRID CloudMirror 복제 서비스입니다" StorageGRID 버킷에서 지정된 외부 대상으로 특정 오브젝트를 미러링합니다.

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

> 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.

알림

사용 "버킷당 이벤트 알림" 객체에 대해 수행된 특정 작업에 대한 알림을 지정된 외부 Amazon SNS(Simple Notification Service)로 보냅니다.

예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.

> S3 오브젝트 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(마지막 보존 날짜 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

검색 통합 서비스

를 사용합니다 "검색 통합 서비스" 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있는 지정된 Elasticsearch 인덱스에 S3 개체 메타데이터를 보냅니다.

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

> S3 오브젝트 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 구축과 외부적이기 때문에 플랫폼 서비스는 데이터에 대한 외부 스토리지 리소스, 알림 서비스 및 검색 또는 분석 서비스를 사용하여 얻을 수 있는 성능과 유연성을 제공합니다.

단일 S3 버킷에 대해 모든 플랫폼 서비스 조합을 구성할 수 있습니다. 예를 들어, StorageGRID S3 버킷에서 CloudMirror 서비스 및 알림을 모두 구성하여 특정 오브젝트를 Amazon Simple Storage Service에 미러링하고 이러한 각 오브젝트에 대한 알림을 타사 모니터링 애플리케이션에 전송하여 AWS 비용을 추적할 수 있도록 할 수 있습니다.

> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스 사용을 활성화해야 합니다.

플랫폼 서비스 구성 방법

플랫폼 서비스는 을 사용하여 구성한 외부 끝점과 통신합니다 "테넌트 관리자" 또는 을 누릅니다 "테넌트 관리 API". 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon SNS 주제 또는 로컬이나 AWS 등에 호스팅된 Elasticsearch 클러스터와 같은 외부 대상을 나타냅니다.

외부 끝점을 만든 후 버킷에 XML 구성을 추가하여 버킷에 대한 플랫폼 서비스를 활성화할 수 있습니다. XML 구성은 버킷이 작업해야 하는 오브젝트, 버킷이 취해야 하는 조치 및 버킷이 서비스에 사용해야 하는 엔드포인트를 식별합니다.

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

- 로 시작하는 키를 가진 모든 개체를 원하는 경우 `/images` Amazon S3 버킷에 복제하려면 소스 버킷에 복제 구성을 추가해야 합니다.
- 이러한 객체가 버킷에 저장될 때 알림을 보내려면 알림 구성을 추가해야 합니다.
- 마지막으로 이러한 개체의 메타데이터를 인덱싱하려면 검색 통합을 구현하는 데 사용되는 메타데이터 알림 구성을 추가해야 합니다.

구성 XML의 형식은 StorageGRID 플랫폼 서비스를 구현하는 데 사용되는 S3 REST API를 통해 제어됩니다.

플랫폼 서비스	**S3 REST API**	을 참조하십시오
CloudMirror 복제	• GetBucketReplication 을 참조하십시오 • PutBucketReplication을 참조하십시오	• "CloudMirror 복제" • "버킷 작업"
알림	• GetBuckNotificationConfiguration 을 참조하십시오 • PutBucketNotificationConfiguration을 참조하십시오	• "알림" • "버킷 작업"
검색 통합	• Bucket 메타데이터 알림 구성 가져오기 • Put Bucket 메타데이터 알림 구성	• "검색 통합" • "StorageGRID 사용자 정의 작업"

관련 정보

"플랫폼 서비스에 대한 고려 사항"

CloudMirror 복제 서비스

StorageGRID가 버킷에 추가된 지정된 오브젝트를 하나 이상의 대상 버킷에 복제하도록 하려면 S3 버킷에 대해 CloudMirror 복제를 활성화할 수 있습니다.

CloudMirror 복제는 그리드의 활성 ILM 정책과 독립적으로 작동합니다. CloudMirror 서비스는 소스 버킷에 저장된 객체를 복제하여 가능한 한 빨리 대상 버킷에 제공합니다. 오브젝트 수집의 성공 시 복제된 오브젝트 제공이 트리거됩니다.

CloudMirror 복제는 교차 그리드 복제 기능과의 중요한 유사점과 차이점이 있습니다. 자세한 내용은 을 참조하십시오 "교차 그리드 복제와 CloudMirror 복제를 비교합니다".

기존 버킷에 대해 CloudMirror 복제를 설정하면 해당 버킷에 추가된 새 객체만 복제됩니다. 버킷의 기존 객체는

복제되지 않습니다. 기존 오브젝트의 복제를 강제로 수행하려면 오브젝트 복사를 수행하여 기존 오브젝트의 메타데이터를 업데이트할 수 있습니다.

> CloudMirror 복제를 사용하여 Amazon S3 대상으로 오브젝트를 복사하는 경우 Amazon S3는 각 PUT 요청 헤더 내의 사용자 정의 메타데이터 크기를 2KB로 제한합니다. 객체에 2KB보다 큰 사용자 정의 메타데이터가 있는 경우 해당 객체가 복제되지 않습니다.

StorageGRID에서는 단일 버킷의 오브젝트를 여러 개의 대상 버킷으로 복제할 수 있습니다. 이렇게 하려면 복제 구성 XML에서 각 규칙의 대상을 지정합니다. 객체를 둘 이상의 버킷에 동시에 복제할 수 없습니다.

또한 버전 관리되거나 버전이 지정되지 않은 버킷에서 CloudMirror 복제를 구성하고 버전 관리되거나 버전이 지정되지 않은 버킷을 대상으로 지정할 수 있습니다. 버전 및 비버전 버킷의 모든 조합을 사용할 수 있습니다. 예를 들어 버전이 지정되지 않은 소스 버킷의 대상으로 버전 관리가 지정된 버킷을 지정하거나 그 반대로 지정할 수 있습니다. 버전이 지정되지 않은 버킷 간에 복제할 수도 있습니다.

CloudMirror 복제 서비스의 삭제 동작은 Amazon S3에서 제공하는 CRR(Cross Region Replication) 서비스의 삭제 동작과 같습니다. 소스 버킷에서 객체를 삭제해도 대상에서 복제된 객체는 삭제되지 않습니다. 소스 및 대상 버킷의 버전이 모두 지정된 경우 삭제 마커가 복제됩니다. 대상 버킷의 버전이 지정되지 않은 경우 소스 버킷에서 오브젝트를 삭제해도 삭제 마커가 대상 버킷에 복제되거나 대상 오브젝트가 삭제되지 않습니다.

오브젝트가 대상 버킷에 복제되면 StorageGRID는 객체를 "복제본"으로 표시합니다. 대상 StorageGRID 버킷은 복제본으로 표시된 객체를 다시 복제하지 않으므로 실수로 인한 복제 루프로부터 사용자를 보호합니다. 이 복제 마크는 StorageGRID 내부에 있으며 Amazon S3 버킷을 대상으로 사용할 때 AWS CRR을 활용하는 것을 방지하지 않습니다.

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

목적지 버킷에서 이벤트의 고유성과 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행된 작업의 결과로 소스 객체의 동일한 복제본이 두 개 이상 대상에 제공될 수 있습니다. 드물지만 둘 이상의 서로 다른 StorageGRID 사이트에서 동일한 객체가 동시에 업데이트되는 경우 대상 버킷의 작업 순서가 소스 버킷의 이벤트 순서와 일치하지 않을 수 있습니다.

CloudMirror 복제는 일반적으로 외부 S3 버킷을 대상으로 사용하도록 구성됩니다. 그러나 다른 StorageGRID 배포나 S3 호환 서비스를 사용하도록 복제를 구성할 수도 있습니다.

버킷에 대한 알림을 이해합니다

StorageGRID에서 지정된 이벤트에 대한 알림을 대상 Kafka 클러스터 또는 Amazon Simple Notification Service로 보내려면 S3 버킷에 대한 이벤트 알림을 활성화할 수 있습니다.

가능합니다 "이벤트 알림을 구성합니다" 알림 구성 XML을 소스 버킷과 연결합니다. 알림 구성 XML은 끝점 URN으로 지정된 대상 Kafka 또는 Amazon SNS 항목과 함께 버킷 알림을 구성하는 S3 규칙을 따릅니다.

이벤트 알림은 알림 구성에 지정된 대로 소스 버킷에서 생성되며 대상으로 전달됩니다. 개체와 관련된 이벤트가 성공하면 해당 이벤트에 대한 알림이 생성되고 배달 대기 상태가 됩니다.

알림의 고유성과 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행된 작업의 결과로 하나 이상의 이벤트 알림이 대상에 전달될 수 있습니다. 그리고 납품이 비동기식이기 때문에, 특히 서로 다른 StorageGRID 사이트에서 발생하는 작업의 경우, 대상에서 알림의 시간 순서가 소스 버킷의 이벤트 순서와 일치한다고 보장할 수 없습니다. 를 사용할 수 있습니다 `sequencer` Amazon S3 설명서에 설명된 대로 이벤트 메시지를 키를 눌러 특정 개체의 이벤트 순서를 결정합니다.

지원되는 알림 및 메시지

StorageGRID 이벤트 알림은 Amazon S3 API를 따릅니다. 여기에는 몇 가지 제한 사항이 있습니다.

- 지원되는 이벤트 유형은 다음과 같습니다.
  - S3:오브젝트 생성: *
  - S3:오브젝트 생성:PUT
  - S3:오브젝트 작성:우편
  - S3:오브젝트 생성:복사
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved: *
  - S3:ObjectRemoved:Delete
  - S3:ObjectRemoved:DeleteMarkerCreated
  - S3:ObjectRestore:게시
- StorageGRID에서 보낸 이벤트 알림은 표준 JSON 형식을 사용하지만 일부 키는 포함하지 않으며 표에 나와 있는 대로 다른 키의 특정 값을 사용합니다.

키 이름	**StorageGRID** 값
이벤트 소스	`sgws:s3`
awsRegion	포함되지 않음
X-amz-id-2	포함되지 않음
ARN	`urn:sgws:s3:::bucket_name`

검색 통합 서비스를 이해합니다

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

검색 통합 서비스는 오브젝트 또는 해당 메타데이터가 업데이트될 때마다 자동으로 그리고 비동기적으로 S3 오브젝트 메타데이터를 대상 끝점에 보내는 사용자 지정 StorageGRID 서비스입니다. 그런 다음 대상 서비스에서 제공하는 정교한 검색, 데이터 분석, 시각화 또는 머신 러닝 도구를 사용하여 오브젝트 데이터를 검색, 분석 및 분석할 수 있습니다.

버전 관리되거나 버전이 지정되지 않은 모든 버킷에 대해 검색 통합 서비스를 활성화할 수 있습니다. 검색 통합은 메타데이터 알림 구성 XML을 작업할 개체 및 개체 메타데이터에 대한 대상을 지정하는 버킷과 연결하여 구성됩니다.

알림은 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)로 명명된 JSON 문서의 형식으로 생성됩니다. 각 메타데이터 알림에는 개체의 모든 태그 및 사용자 메타데이터 외에도 개체에 대한 표준 시스템 메타데이터 세트가 포함되어 있습니다.

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

알림은 다음과 같은 경우에 생성되고 전송 대기 상태가 됩니다.

- 객체가 생성됩니다.
- 그리드의 ILM 정책 작업으로 인해 오브젝트가 삭제된 경우를 포함하여 오브젝트가 삭제됩니다.
- 오브젝트 메타데이터 또는 태그가 추가, 업데이트 또는 삭제됩니다. 메타데이터 및 태그의 전체 집합은 항상 변경된 값뿐만 아니라 업데이트 시 전송됩니다.

메타데이터 알림 구성 XML을 버킷에 추가하면 생성한 새 개체 및 데이터, 사용자 메타데이터 또는 태그를 업데이트하여 수정하는 모든 개체에 대한 알림이 전송됩니다. 하지만 이미 버킷에 있는 객체에 대해서는 알림이 전송되지 않습니다. 버킷의 모든 오브젝트에 대한 오브젝트 메타데이터가 대상으로 전송되도록 하려면 다음 중 하나를 수행해야 합니다.

- 버킷을 생성한 후 개체를 추가하기 전에 즉시 검색 통합 서비스를 구성합니다.
- 메타데이터 알림 메시지가 대상으로 전송되도록 버킷에 이미 있는 모든 객체에 대해 작업을 수행합니다.

StorageGRID 검색 통합 서비스는 Elasticsearch 클러스터를 대상으로 지원합니다. 다른 플랫폼 서비스와 마찬가지로 대상은 서비스의 구성 XML에서 URN이 사용되는 끝점에서 지정됩니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 지원되는 Elasticsearch 버전을 확인합니다.

관련 정보

"검색 통합을 위한 구성 XML"

"메타데이터 알림에 포함된 개체 메타데이터입니다"

"JSON이 검색 통합 서비스에 의해 생성되었습니다"

"검색 통합 서비스를 구성합니다"

플랫폼 서비스에 대한 고려 사항

플랫폼 서비스를 구현하기 전에 이러한 서비스를 사용하기 위한 권장 사항 및 고려 사항을 검토하십시오.

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

플랫폼 서비스 사용에 대한 고려 사항

고려 사항	세부 정보
대상 엔드포인트 모니터링	각 대상 끝점의 가용성을 모니터링해야 합니다. 대상 끝점에 대한 연결이 오랜 시간 동안 손실되고 요청의 백로그가 많은 경우 StorageGRID에 대한 추가 클라이언트 요청(예: PUT 요청)이 실패합니다. 엔드포인트에 연결할 수 있게 되면 실패한 요청을 다시 시도해야 합니다.

고려 사항	세부 정보
대상 끝점 임계치 조절	요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다. 단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다. CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 영향을 받을 가능성이 더 높습니다.
주문 보증	StorageGRID은 사이트 내의 개체에 대한 작업을 주문할 수 있도록 보장합니다. 객체에 대한 모든 작업이 동일한 사이트 내에 있는 한 최종 객체 상태(복제의 경우)는 항상 StorageGRID의 상태와 동일합니다. StorageGRID는 StorageGRID 사이트 전체에서 작업이 수행되는 경우 요청을 주문하기 위해 최선의 노력을 다하고 있습니다. 예를 들어 처음에 사이트 A에 오브젝트를 작성한 다음 나중에 사이트 B에서 동일한 오브젝트를 덮어쓰는 경우 CloudMirror에서 대상 버킷에 복제한 최종 오브젝트는 새로운 오브젝트일 수 없습니다.
ILM 기반 오브젝트 삭제	AWS CRR 및 Amazon Simple Notification Service의 삭제 동작과 일치시키기 위해 StorageGRID ILM 규칙으로 인해 소스 버킷의 오브젝트가 삭제될 때 CloudMirror 및 이벤트 알림 요청이 전송되지 않습니다. 예를 들어 ILM 규칙이 14일 후에 개체를 삭제하는 경우 CloudMirror 또는 이벤트 알림 요청이 전송되지 않습니다. 반면, 검색 통합 요청은 ILM로 인해 객체가 삭제될 때 전송됩니다.
Kafka 엔드포인트 사용	Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 그 결과 `ssl.client.auth` 를 로 설정합니다 `required` Kafka 브로커 구성에서 Kafka 엔드포인트 구성 문제를 유발할 수 있습니다. Kafka 엔드포인트 인증은 다음과 같은 인증 유형을 사용합니다. 이러한 유형은 Amazon SNS와 같은 다른 엔드포인트의 인증에 사용되는 유형과는 다르며 사용자 이름 및 암호 자격 증명이 필요합니다. • SASL/일반 • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 • 참고: * 구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

CloudMirror 복제 서비스 사용에 대한 고려 사항

고려 사항	세부 정보
복제 상태입니다	StorageGRID는 을 지원하지 않습니다 `x-amz-replication-status` 머리글.
개체 크기	CloudMirror 복제 서비스를 통해 대상 버킷에 복제할 수 있는 개체의 최대 크기는 5TiB이며, 이는 maximum_supported_object 크기와 같습니다. • 참고 *: 단일 PutObject 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다.
버킷 버전 관리 및 버전 ID	StorageGRID의 소스 S3 버킷에서 버전 관리가 활성화된 경우 대상 버킷의 버전 관리도 활성화해야 합니다. 버전 관리를 사용할 때는 S3 프로토콜의 제한으로 인해 대상 버킷에서 오브젝트 버전 순서가 CloudMirror 서비스에 의해 보장되지 않는 것이 가장 좋습니다. • 참고 *: StorageGRID의 소스 버킷에 대한 버전 ID는 대상 버킷의 버전 ID와 관련이 없습니다.
개체 버전에 태그 달기	CloudMirror 서비스는 S3 프로토콜의 제한으로 인해 버전 ID를 제공하는 PutObjectTagging 또는 DeleteObjectTagging 요청을 복제하지 않습니다. 소스 및 대상의 버전 ID는 관련이 없으므로 특정 버전 ID에 대한 태그 업데이트를 복제할 수 없습니다. 반면, CloudMirror 서비스는 버전 ID를 지정하지 않는 PutObjectTagging 요청이나 DeleteObjectTagging 요청을 복제합니다. 이러한 요청은 최신 키의 태그(또는 버킷의 버전이 지정된 경우 최신 버전)를 업데이트합니다. 태그가 있는 일반 베스트(업데이트 태그 지정 안 함)도 복제됩니다.
멀티파트 업로드 및 `ETag` 값	여러 부분 업로드를 사용하여 업로드한 개체를 미러링할 때 CloudMirror 서비스는 해당 파트를 보존하지 않습니다. 그 결과, 가 표시됩니다 `ETag` 대칭 복사된 개체의 값은 과 다릅니다 `ETag` 원래 오브젝트의 값입니다.
SSE-C로 암호화된 오브젝트(고객이 제공한 키를 사용한 서버측 암호화)	CloudMirror 서비스는 SSE-C로 암호화된 객체를 지원하지 않습니다 CloudMirror 복제를 위해 소스 버킷으로 객체를 수집하려고 하고 요청에 SSE-C 요청 헤더가 포함된 경우 작업이 실패합니다.
S3 오브젝트 잠금이 활성화된 버킷	CloudMirror 복제용 대상 S3 버킷에 S3 오브젝트 잠금이 설정되어 있는 경우 버킷 복제(PutBucketReplication) 구성 시도가 실패하고 AccessDenied 오류가 발생합니다.

플랫폼 서비스 끝점을 구성합니다

버킷에 대한 플랫폼 서비스를 구성하려면 먼저 플랫폼 서비스의 대상으로 하나 이상의 엔드포인트를 구성해야 합니다.

플랫폼 서비스에 대한 액세스는 StorageGRID 관리자가 테넌트 단위로 사용하도록 설정합니다. 플랫폼 서비스 끝점을 만들거나 사용하려면 스토리지 노드가 외부 끝점 리소스에 액세스할 수 있도록 네트워킹이 구성된 그리드에서 끝점 관리

또는 루트 액세스 권한이 있는 테넌트 사용자여야 합니다. 단일 테넌트의 경우 최대 500개의 플랫폼 서비스 엔드포인트를 구성할 수 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하십시오.

플랫폼 서비스 엔드포인트란 무엇입니까?

플랫폼 서비스 끝점을 만들 때 StorageGRID가 외부 대상에 액세스하는 데 필요한 정보를 지정합니다.

예를 들어, StorageGRID 버킷에서 Amazon S3 버킷으로 오브젝트를 복제하려는 경우 StorageGRID에서 Amazon의 대상 버킷에 액세스하는 데 필요한 정보 및 자격 증명이 포함된 플랫폼 서비스 엔드포인트를 생성합니다.

각 플랫폼 서비스 유형에는 고유한 엔드포인트가 필요하므로 사용하려는 각 플랫폼 서비스에 대해 하나 이상의 엔드포인트를 구성해야 합니다. 플랫폼 서비스 끝점을 정의한 후 서비스를 활성화하는 데 사용되는 구성 XML에서 끝점의 URN을 대상으로 사용합니다.

둘 이상의 소스 버킷에 대해 목적지와 동일한 끝점을 사용할 수 있습니다. 예를 들어, 여러 버킷에서 검색을 수행할 수 있도록 여러 소스 버킷을 구성하여 동일한 검색 통합 엔드포인트로 오브젝트 메타데이터를 보낼 수 있습니다. 하나 이상의 엔드포인트를 대상으로 사용하도록 소스 버킷을 구성할 수도 있습니다. 이를 통해 하나의 Amazon SNS(Simple Notification Service) 주제에 객체 생성에 대한 알림을 보내고 두 번째 Amazon SNS 주제에 대한 객체 삭제에 대한 알림을 보낼 수 있습니다.

CloudMirror 복제용 엔드포인트

StorageGRID는 S3 버킷을 나타내는 복제 엔드포인트를 지원합니다. 이러한 버킷은 Amazon Web Services, 동일한 또는 원격 StorageGRID 구축 또는 다른 서비스에서 호스팅될 수 있습니다.

알림의 끝점입니다

StorageGRID는 Amazon SNS 및 Kafka 엔드포인트를 지원합니다. SQS(Simple Queue Service) 또는 AWS Lambda 엔드포인트는 지원되지 않습니다.

Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 그 결과 `ssl.client.auth` 를 로 설정합니다 `required` Kafka 브로커 구성에서 Kafka 엔드포인트 구성 문제를 유발할 수 있습니다.

검색 통합 서비스의 끝점입니다

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

검색 통합 끝점은 특정 Elasticsearch 인덱스 및 유형을 참조합니다. StorageGRID에서 끝점을 만들기 전에 Elasticsearch에서 인덱스를 만들어야 합니다. 그렇지 않으면 끝점 생성이 실패합니다. 끝점을 만들기 전에 형식을 만들 필요가 없습니다. StorageGRID는 개체 메타데이터를 끝점으로 보낼 때 필요한 경우 형식을 만듭니다.

관련 정보

"StorageGRID 관리"

플랫폼 서비스 끝점에 **URN**을 지정합니다

플랫폼 서비스 끝점을 만들 때는 고유한 URN(리소스 이름)을 지정해야 합니다. 플랫폼 서비스에 대한 구성 XML을 만들 때 URN을 사용하여 끝점을 참조합니다. 각 끝점의 URN은 고유해야 합니다.

StorageGRID에서는 플랫폼 서비스 엔드포인트를 만들 때 이를 검증합니다. 플랫폼 서비스 끝점을 만들기 전에 끝점에 지정된 리소스가 있고 해당 리소스에 도달할 수 있는지 확인합니다.

urn 요소

플랫폼 서비스 끝점의 URN은 둘 중 하나로 시작해야 합니다 `arn:aws` 또는 `urn:mysite`다음과 같이 하십시오.

- AWS(Amazon Web Services)에서 서비스가 호스팅되는 경우 를 사용합니다 `arn:aws`
- 서비스가 GCP(Google Cloud Platform)에서 호스팅되는 경우 를 사용합니다 `arn:aws`
- 서비스가 로컬로 호스팅되는 경우 를 사용합니다 `urn:mysite`

예를 들어 StorageGRID에서 호스팅되는 CloudMirror 끝점에 URN을 지정하는 경우 URN이 로 시작될 수 있습니다 `urn:sgws`.

URN의 다음 요소는 다음과 같이 플랫폼 서비스의 유형을 지정합니다.

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

예를 들어 StorageGRID에서 호스팅되는 CloudMirror 끝점에 대해 URN을 계속 지정하려면 을 추가합니다 `s3` 얻을 수 있습니다 `urn:sgws:s3`.

URN의 마지막 요소는 대상 URI에서 특정 대상 리소스를 식별합니다.

서비스	특정 리소스
CloudMirror 복제	`bucket-name`
알림	`sns-topic-name` 또는 `kafka-topic-name`
검색 통합	`domain-name/index-name/type-name` • 참고: * Elasticsearch 클러스터가 자동으로 인덱스를 만들도록 * 구성되지 * 인 경우 끝점을 만들기 전에 수동으로 인덱스를 만들어야 합니다.

AWS 및 **GCP**에서 호스팅되는 서비스의 여관

AWS 및 GCP 엔터티의 경우 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, 를 참조하십시오 `domain-name` 리터럴 문자열을 포함해야 합니다 `domain/`를 클릭합니다.

현지 호스팅 서비스를 위한 여관

클라우드 서비스 대신 로컬로 호스팅된 서비스를 사용하는 경우 URN에 필요한 요소가 세 번째 및 최종 위치에 포함되어 있는 한 유효하고 고유한 URN을 만드는 방식으로 URN을 지정할 수 있습니다. 선택 사항으로 표시된 요소를 비워 두거나 자원을 식별하고 URN을 고유하게 만드는 데 도움이 되도록 원하는 방식으로 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

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

StorageGRID에서 호스팅되는 CloudMirror 끝점의 경우 로 시작하는 유효한 URN을 지정할 수 있습니다 `urn:sgws`:

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

- 알림:

Amazon Simple Notification Service 끝점 지정:

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

Kafka 끝점 지정:

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

- 검색 통합:

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

로컬로 호스팅되는 검색 통합 끝점의 경우 를 참조하십시오 `domain-name` 요소의 URN이 고유하면 모든 문자열이 될 수 있습니다.

플랫폼 서비스 끝점을 만듭니다

플랫폼 서비스를 사용하려면 먼저 올바른 유형의 끝점을 하나 이상 만들어야 합니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 이 있는 사용자 그룹에 속해 있습니다 "끝점 또는 루트 액세스 권한을 관리합니다".
- 플랫폼 서비스 끝점에서 참조하는 리소스가 생성되었습니다.
  - CloudMirror 복제: S3 버킷
  - 이벤트 알림: Amazon SNS(Simple Notification Service) 또는 Kafka 토픽입니다
  - 검색 알림: 대상 클러스터가 인덱스를 자동으로 생성하도록 구성되지 않은 경우 Elasticsearch index입니다.
- 대상 리소스에 대한 정보가 있습니다.
  - URI(Uniform Resource Identifier)의 호스트 및 포트

    StorageGRID 시스템에서 호스팅되는 버킷을 CloudMirror 복제의 엔드포인트로 사용하려면 그리드 관리자에게 문의하여 입력해야 하는 값을 확인하십시오.

  - 고유 리소스 이름(URN)

    "플랫폼 서비스 끝점에 URN을 지정합니다"

  - 인증 자격 증명(필요한 경우):

AWS 검색 통합 엔드포인트

AWS 검색 통합 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키
- 기본 HTTP: 사용자 이름 및 암호
- CAP(C2S Access Portal): 임시 자격 증명 URL, 서버 및 클라이언트 인증서, 클라이언트 키 및 선택적 클라이언트 개인 키 암호.

CloudMirror 복제 및 **Amazon SNS** 엔드포인트를 지원합니다

CloudMirror 복제 및 Amazon SNS 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키
- CAP(C2S Access Portal): 임시 자격 증명 URL, 서버 및 클라이언트 인증서, 클라이언트 키 및 선택적 클라이언트 개인 키 암호.

Kafka 엔드포인트

Kafka 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- SASL /plain: 사용자 이름 및 암호
- SASL/SCRAM-SHA-256: 사용자 이름 및 암호
- SASL/SCRAM-SHA-512: 사용자 이름 및 암호

  - 보안 인증서(사용자 지정 CA 인증서를 사용하는 경우)

- Elasticsearch 보안 기능이 활성화된 경우 연결 테스트에 대한 모니터 클러스터 권한, 쓰기 인덱스 권한 또는 문서 업데이트에 대한 인덱스 및 삭제 권한 모두가 있습니다.

단계

1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다. 플랫폼 서비스 끝점 페이지가 나타납니다.
2. 끝점 만들기 * 를 선택합니다.
3. 표시 이름을 입력하여 끝점과 그 용도를 간략하게 설명합니다.

   끝점이 지원하는 플랫폼 서비스 유형은 끝점 페이지에 나열될 때 끝점 이름 옆에 표시되므로 이름에 해당 정보를 포함할 필요가 없습니다.

4. URI * 필드에서 끝점의 고유 URI(Resource Identifier)를 지정합니다.

   다음 형식 중 하나를 사용합니다.

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

   포트를 지정하지 않으면 다음과 같은 기본 포트가 사용됩니다.

◦ HTTPS URI의 경우 포트 443, HTTP URI의 경우 포트 80(대부분의 끝점)

◦ HTTPS 및 HTTP URI용 포트 9092(Kafka 엔드포인트만 해당)

예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같습니다.

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

이 예에서는 `s3.example.com` StorageGRID HA(고가용성) 그룹의 VIP(가상 IP)에 대한 DNS 항목을 나타냅니다 `10443` 로드 밸런서 끝점에 정의된 포트를 나타냅니다.

가능하면 단일 장애 지점을 피하기 위해 로드 밸런싱 노드의 HA 그룹에 연결해야 합니다.

마찬가지로 AWS에서 호스팅되는 버킷의 URI는 다음과 같습니다.

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

엔드포인트가 CloudMirror 복제 서비스에 사용되는 경우 버킷 이름을 URI에 포함하지 마십시오. 버킷 이름을 * URN * 필드에 포함시킵니다.

5. 끝점에 대한 고유 URN(리소스 이름)을 입력합니다.

끝점이 생성된 후에는 끝점의 URN을 변경할 수 없습니다.

6. Continue * 를 선택합니다.
7. 인증 유형 * 의 값을 선택합니다.

AWS 검색 통합 엔드포인트

AWS 검색 통합 끝점에 대한 자격 증명을 입력하거나 업로드합니다.

제공하는 자격 증명에 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

인증 유형입니다	설명	자격 증명
익명	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 끝점에서만 작동합니다.	인증이 없습니다.
액세스 키	AWS 스타일 자격 증명을 사용하여 대상과의 연결을 인증합니다.	• 액세스 키 ID입니다 • 비밀 액세스 키
기본 HTTP	사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
CAP(C2S 액세스 포털)	인증서 및 키를 사용하여 대상에 대한 연결을 인증합니다.	• 임시 자격 증명 URL입니다 • 서버 CA 인증서(PEM 파일 업로드) • 클라이언트 인증서(PEM 파일 업로드) • 클라이언트 개인 키(PEM 파일 업로드, OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식) • 클라이언트 개인 키 암호 구문(선택 사항)

CloudMirror 복제 또는 **Amazon SNS** 엔드포인트를 지원합니다

CloudMirror 복제 또는 Amazon SNS 엔드포인트에 대한 자격 증명을 입력하거나 업로드합니다.

제공하는 자격 증명에 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

인증 유형입니다	설명	자격 증명
익명	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 끝점에서만 작동합니다.	인증이 없습니다.
액세스 키	AWS 스타일 자격 증명을 사용하여 대상과의 연결을 인증합니다.	• 액세스 키 ID입니다 • 비밀 액세스 키

인증 유형입니다	설명	자격 증명
CAP(C2S 액세스 포털)	인증서 및 키를 사용하여 대상에 대한 연결을 인증합니다.	• 임시 자격 증명 URL입니다 • 서버 CA 인증서(PEM 파일 업로드) • 클라이언트 인증서(PEM 파일 업로드) • 클라이언트 개인 키(PEM 파일 업로드, OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식) • 클라이언트 개인 키 암호 구문(선택 사항)

Kafka 엔드포인트

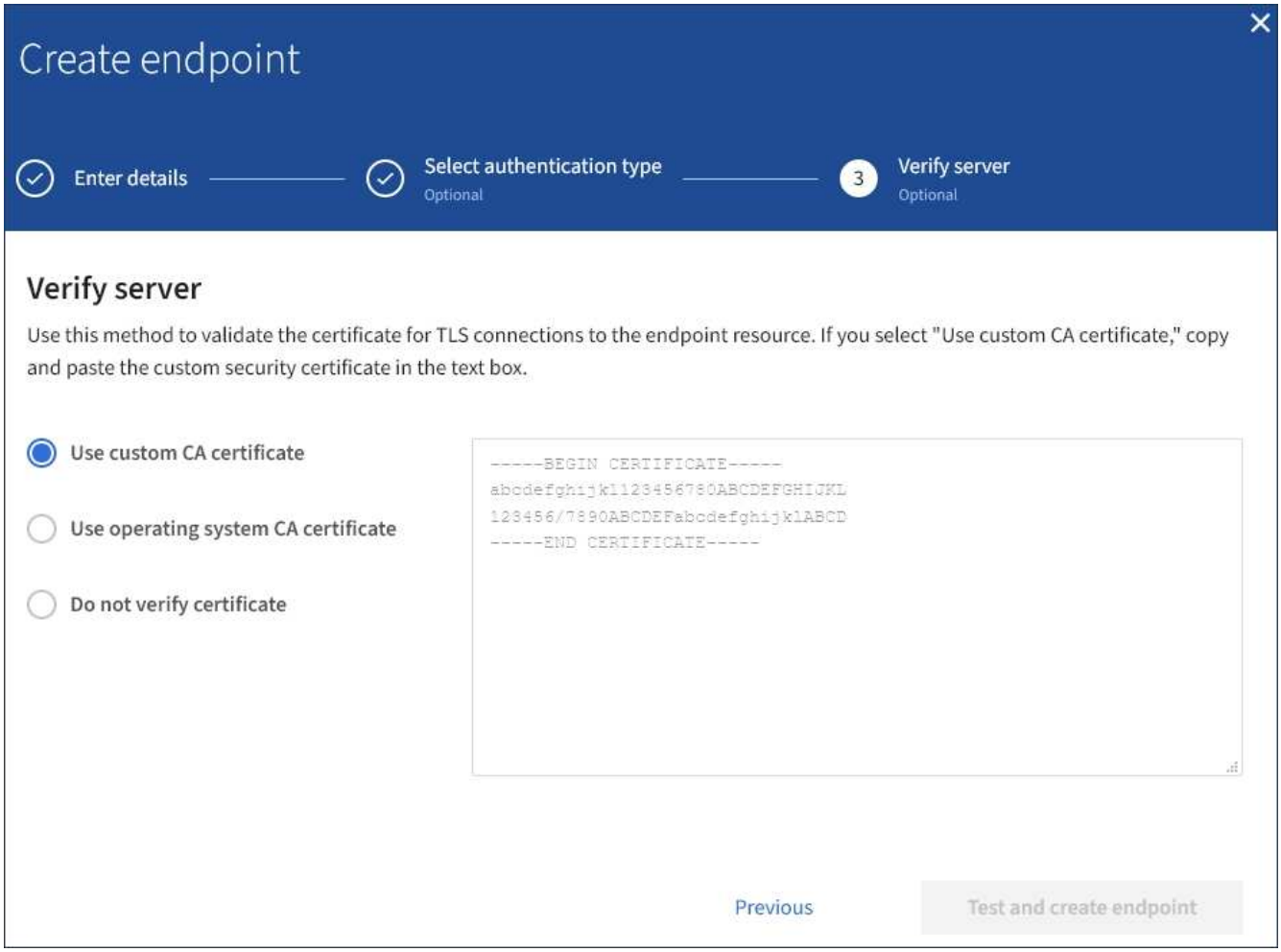
Kafka 엔드포인트에 대한 자격 증명을 입력하거나 업로드합니다.

제공하는 자격 증명에 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

인증 유형입니다	설명	자격 증명
익명	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 끝점에서만 작동합니다.	인증이 없습니다.
SASL/일반	사용자 이름과 암호를 일반 텍스트로 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
SASL/SCRAM-SHA-256	Challenge-Response 프로토콜 및 SHA-256 해싱을 사용하여 사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
SASL/SCRAM-SHA-512	Challenge-Response 프로토콜 및 SHA-512 해싱을 사용하여 사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호

사용자 이름과 암호가 Kafka 클러스터에서 가져온 위임 토큰에서 파생되는 경우 * Use 위임 인증 사용 * 을 선택합니다.

8. Continue * 를 선택합니다.
9. 끝점에 대한 TLS 연결을 확인하는 방법을 선택하려면 * 서버 확인 * 에 대한 라디오 버튼을 선택합니다.



인증서 확인 유형입니다	설명
사용자 지정 CA 인증서를 사용합니다	사용자 지정 보안 인증서를 사용합니다. 이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다. 이 옵션은 안전하지 않습니다.

10. 테스트를 선택하고 끝점 * 을 작성합니다.
    - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
    - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 오류를 수정하기 위해 끝점을 수정해야 하는 경우 * 끝점 세부 정보로 돌아가기 * 를 선택하고 정보를 업데이트합니다. 그런 다음 * 테스트 를 선택하고 끝점 * 을 만듭니다.

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

끝점을 구성한 후 URN을 사용하여 플랫폼 서비스를 구성할 수 있습니다.

관련 정보

"플랫폼 서비스 끝점에 URN을 지정합니다"

"CloudMirror 복제를 구성합니다"

"이벤트 알림을 구성합니다"

"검색 통합 서비스를 구성합니다"

플랫폼 서비스 끝점에 대한 연결을 테스트합니다

플랫폼 서비스에 대한 연결이 변경된 경우 끝점에 대한 연결을 테스트하여 대상 리소스가 있는지 그리고 지정한 자격 증명을 사용하여 해당 리소스에 연결할 수 있는지 확인할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 이 있는 사용자 그룹에 속해 있습니다 "끝점 또는 루트 액세스 권한을 관리합니다".

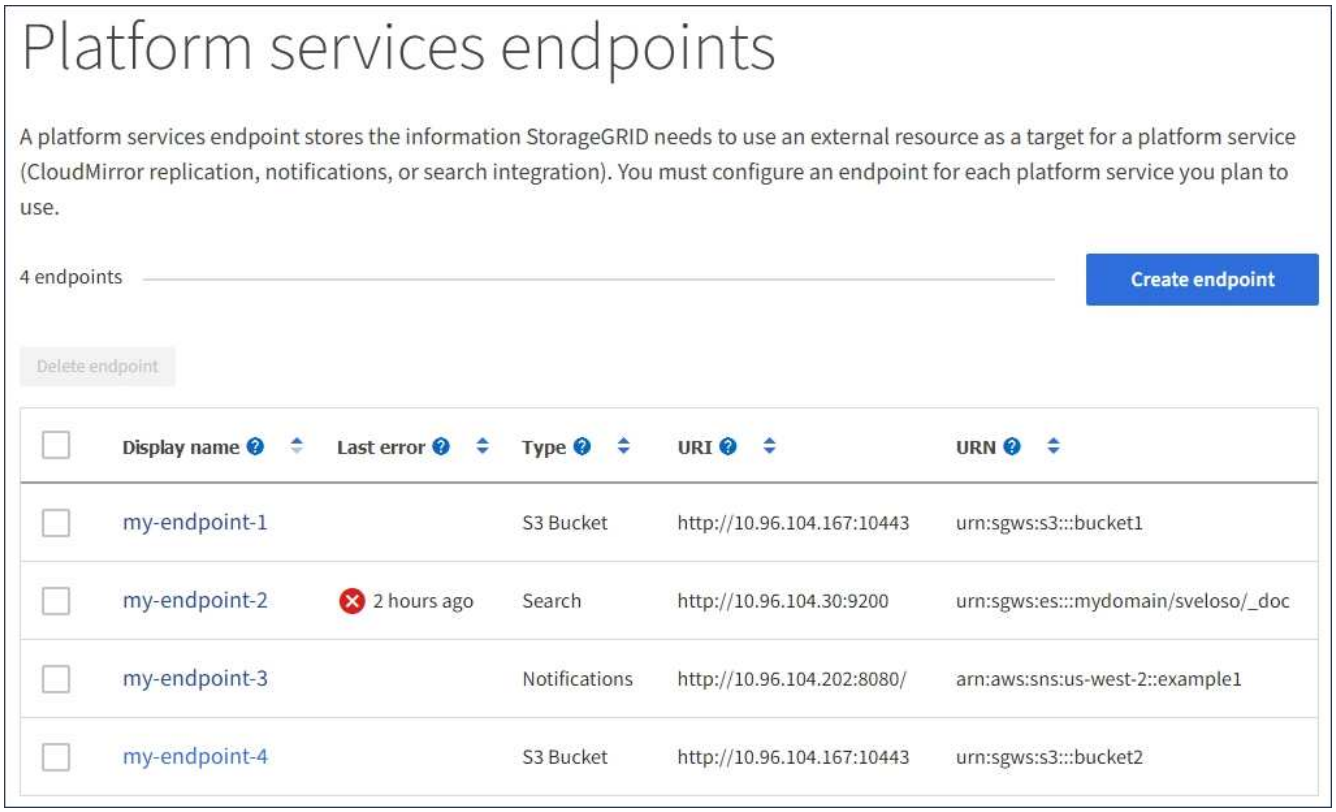
이 작업에 대해

StorageGRID는 자격 증명에 올바른 권한이 있는지 확인하지 않습니다.

단계

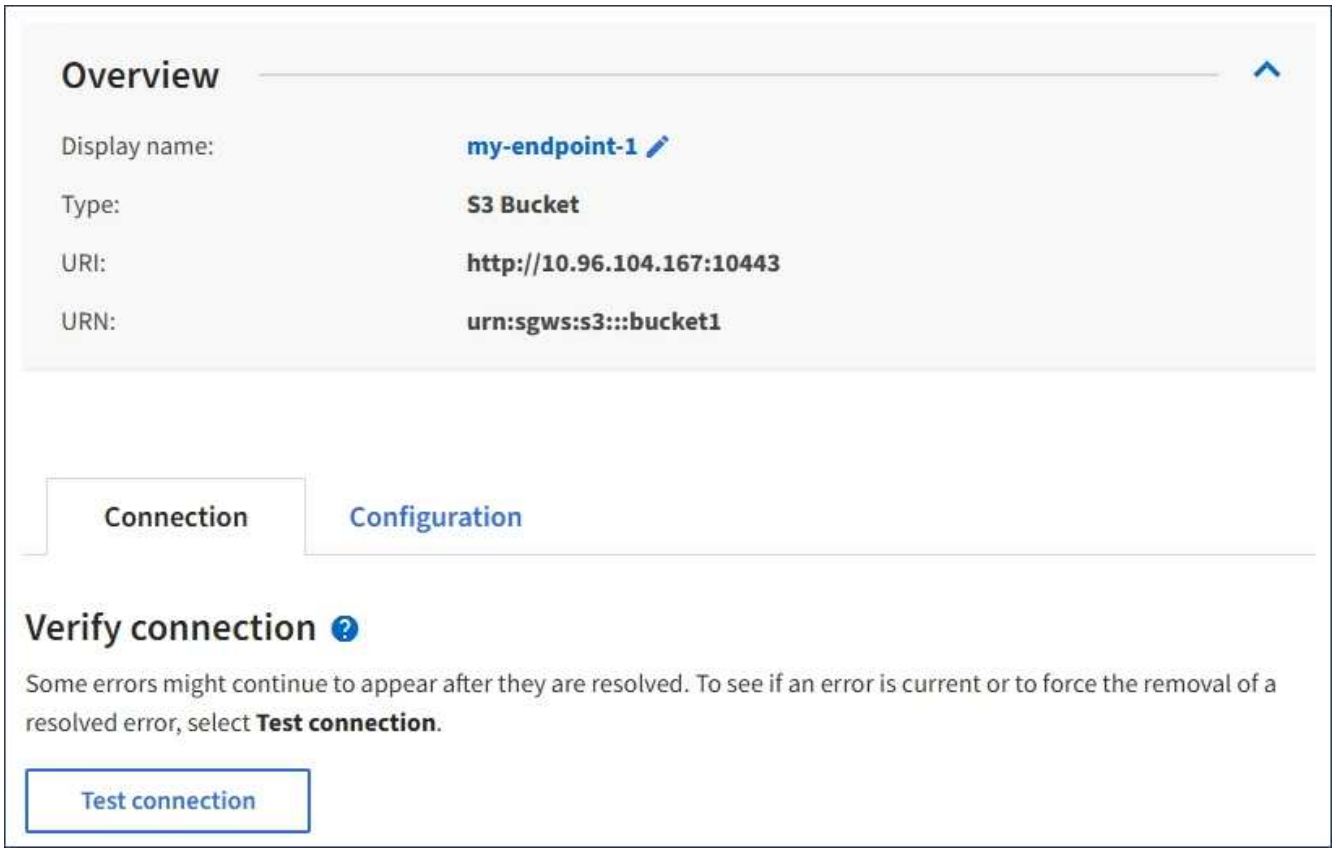
1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다.

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



2. 연결을 테스트할 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.



3. Test connection * 을 선택합니다.
   - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
   - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 오류를 정정하기 위해 끝점을 수정해야 하는 경우 * 구성 * 을 선택하고 정보를 업데이트합니다. 그런 다음 * 테스트 및 변경 내용 저장 * 을 선택합니다.

플랫폼 서비스 끝점을 편집합니다

플랫폼 서비스 끝점의 구성을 편집하여 이름, URI 또는 기타 세부 정보를 변경할 수 있습니다. 예를 들어 만료된 자격 증명을 업데이트하거나 대체 작동을 위한 백업 Elasticsearch 인덱스를 가리키도록 URI를 변경해야 할 수 있습니다. 플랫폼 서비스 끝점의 URN은 변경할 수 없습니다.

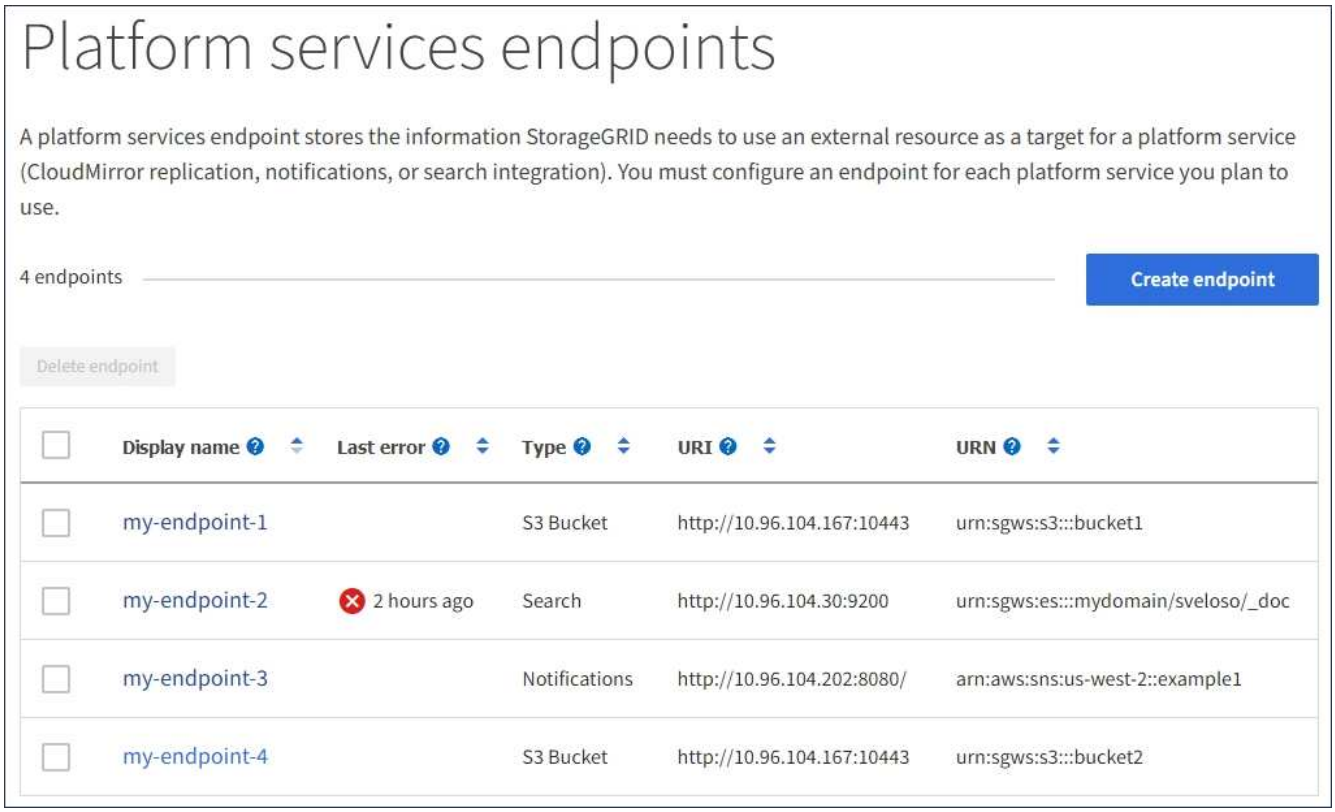
시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 이 있는 사용자 그룹에 속해 있습니다 "끝점 또는 루트 액세스 권한을 관리합니다".

단계

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

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



2. 편집할 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.

3. Configuration * 을 선택합니다.
4. 필요에 따라 끝점의 구성을 변경합니다.

   끝점이 생성된 후에는 끝점의 URN을 변경할 수 없습니다.

   a. 끝점의 표시 이름을 변경하려면 편집 아이콘을 선택합니다 .
   b. 필요에 따라 URI를 변경합니다.
   c. 필요에 따라 인증 유형을 변경합니다.
      - 액세스 키 인증의 경우 * S3 키 편집 * 을 선택하고 새 액세스 키 ID 및 비밀 액세스 키를 붙여 넣어 필요에 따라 키를 변경합니다. 변경 사항을 취소하려면 * S3 키 편집 되돌리기 * 를 선택합니다.
      - CAP(C2S Access Portal) 인증의 경우 임시 자격 증명 URL 또는 선택적 클라이언트 개인 키 암호를 변경하고 필요에 따라 새 인증서 및 키 파일을 업로드합니다.

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

   d. 필요에 따라 서버 확인 방법을 변경합니다.
5. Test(테스트)를 선택하고 변경 내용을 저장합니다 *.
   - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 확인합니다.

◦ 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 끝점을 수정하여 오류를 수정한 다음 * 테스트 및 변경 내용 저장 * 을 선택합니다.

플랫폼 서비스 끝점을 삭제합니다

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

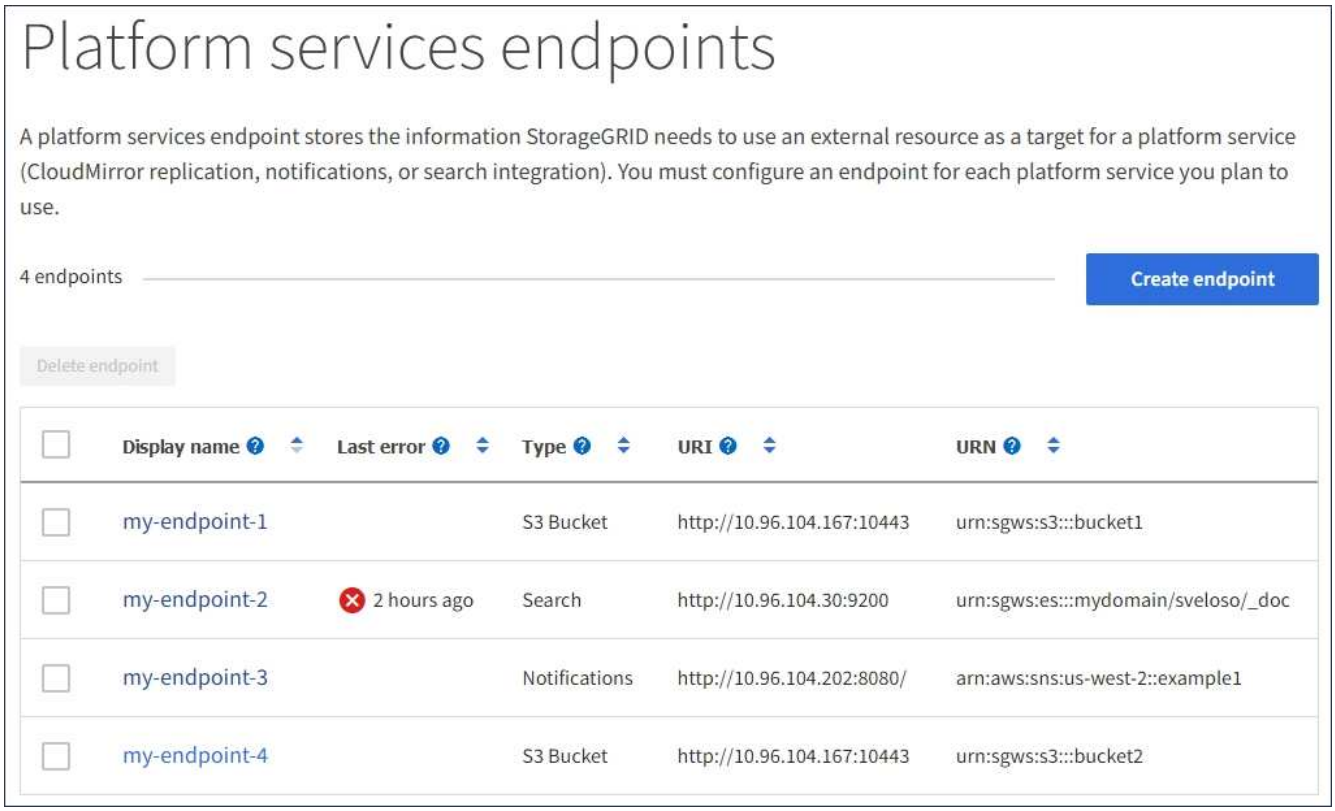
시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 이 있는 사용자 그룹에 속해 있습니다 "끝점 또는 루트 액세스 권한을 관리합니다".

단계

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

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

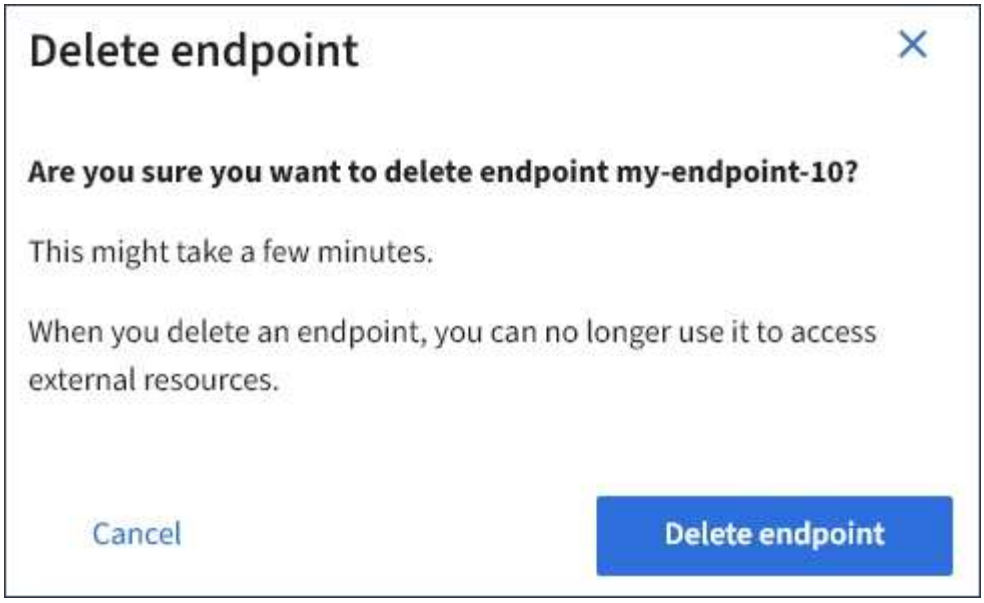


2. 삭제할 각 끝점의 확인란을 선택합니다.

   사용 중인 플랫폼 서비스 끝점을 삭제하면 해당 끝점을 사용하는 모든 버킷에 대해 연결된 플랫폼 서비스가 비활성화됩니다. 아직 완료되지 않은 요청은 삭제됩니다. 삭제된 URN을 더 이상 참조하지 않도록 버킷 구성을 변경할 때까지 새 요청은 계속 생성됩니다. StorageGRID는 이러한 요청을 복구할 수 없는 오류로 보고합니다.

3. 작업 * > * 끝점 삭제 * 를 선택합니다.

   확인 메시지가 나타납니다.



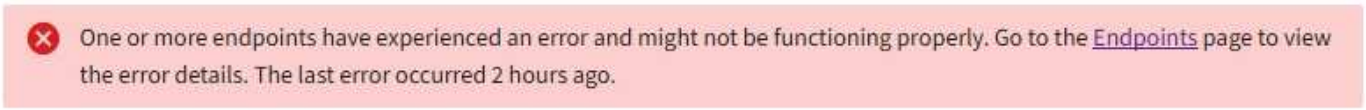
4. 끝점 삭제 * 를 선택합니다.

플랫폼 서비스 끝점 오류 문제 해결

StorageGRID가 플랫폼 서비스 끝점과 통신하려고 할 때 오류가 발생하면 대시보드에 메시지가 표시됩니다. 플랫폼 서비스 끝점 페이지에서 마지막 오류 열은 오류가 발생한 시간을 나타냅니다. 끝점의 자격 증명과 연결된 권한이 올바르지 않으면 오류가 표시되지 않습니다.

오류가 발생했는지 확인합니다

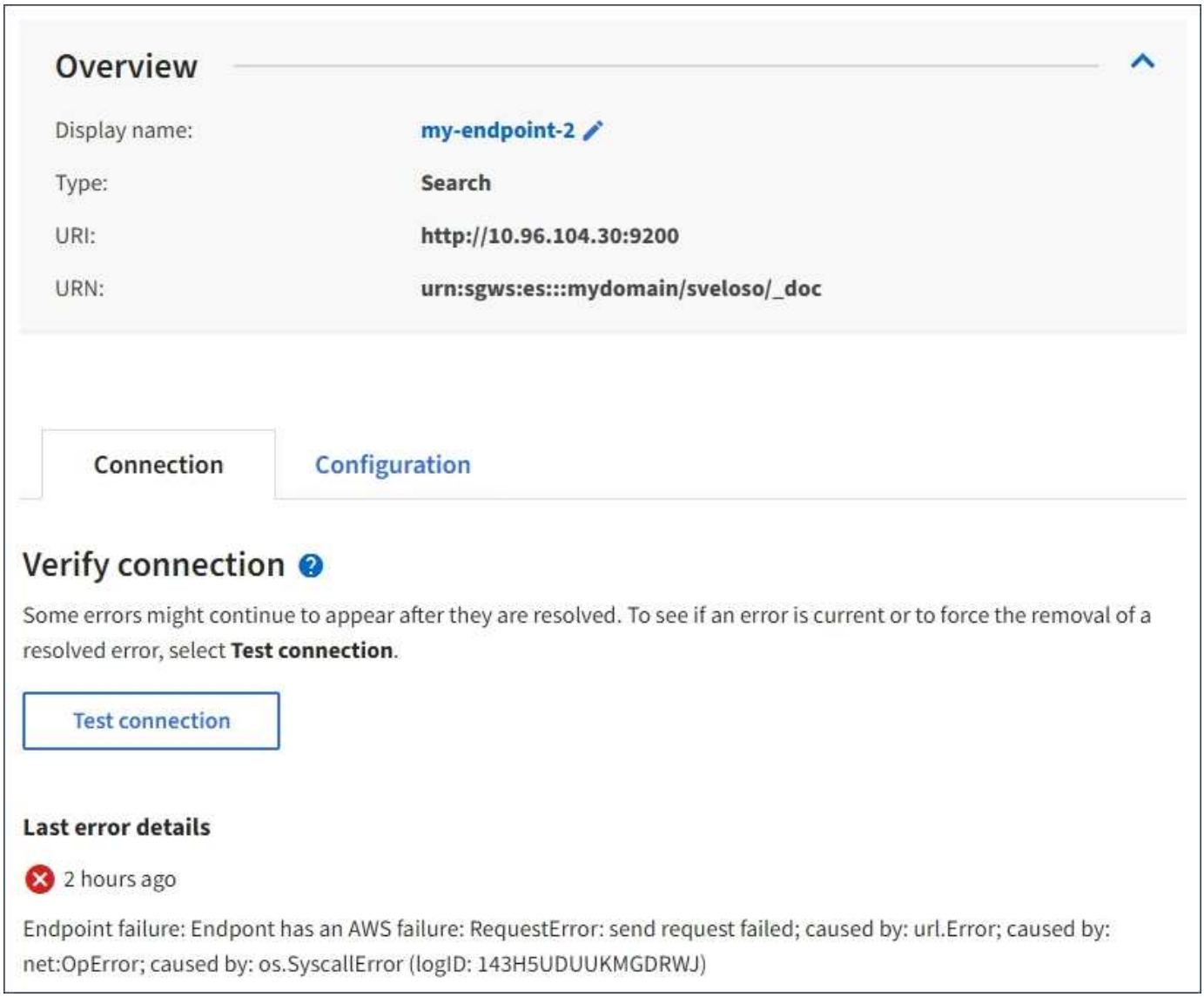
지난 7일 이내에 플랫폼 서비스 끝점 오류가 발생한 경우 테넌트 관리자 대시보드에 경고 메시지가 표시됩니다. 플랫폼 서비스 끝점 페이지로 이동하여 오류에 대한 자세한 정보를 볼 수 있습니다.



대시보드에 나타나는 동일한 오류가 플랫폼 서비스 끝점 페이지 맨 위에도 나타납니다. 자세한 오류 메시지를 보려면:

단계

1. 끝점 목록에서 오류가 있는 끝점을 선택합니다.
2. 끝점 세부 정보 페이지에서 * 연결 * 을 선택합니다. 이 탭은 끝점에 대한 가장 최근 오류만 표시하고 오류가 발생한 시간을 표시합니다. 빨간색 X 아이콘이 포함된 오류 지난 7일 이내에 발생했습니다.



오류가 여전히 최신 상태인지 확인합니다

일부 오류는 해결된 후에도 * 마지막 오류 * 열에 계속 표시될 수 있습니다. 오류가 현재 오류인지 확인하거나 테이블에서 해결된 오류를 강제로 제거하려면 다음과 같이 하십시오.

단계

1. 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.

2. 연결 * > * 연결 테스트 * 를 선택합니다.

연결 테스트 * 를 선택하면 StorageGRID가 플랫폼 서비스 끝점이 있는지, 그리고 현재 자격 증명으로 연결할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 오류를 해결합니다

끝점 세부 정보 페이지의 * 마지막 오류 * 메시지를 사용하여 오류의 원인을 확인할 수 있습니다. 일부 오류에서는 문제를 해결하기 위해 끝점을 편집해야 할 수 있습니다. 예를 들어, 올바른 액세스 권한이 없거나 액세스 키가 만료되어

StorageGRID가 대상 S3 버킷을 액세스할 수 없는 경우 클라우드미러링 오류가 발생할 수 있습니다. 메시지는 "끝점 자격 증명 또는 대상 액세스를 업데이트해야 합니다."이고 세부 정보는 "AccessDenied" 또는 "InvalidAccessKeyId"입니다.

오류를 해결하기 위해 끝점을 편집해야 하는 경우 * 테스트 및 변경 내용 저장 * 을 선택하면 StorageGRID가 업데이트된 끝점을 검증하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

단계

1. 끝점을 선택합니다.
2. 끝점 세부 정보 페이지에서 * 구성 * 을 선택합니다.
3. 필요에 따라 끝점 설정을 편집합니다.
4. 연결 * > * 연결 테스트 * 를 선택합니다.

권한이 부족한 끝점 자격 증명

StorageGRID에서 플랫폼 서비스 끝점의 유효성을 검사할 때 끝점의 자격 증명을 사용하여 대상 리소스에 연결할 수 있는지 확인하고 기본적인 사용 권한 검사를 수행합니다. 그러나 StorageGRID는 특정 플랫폼 서비스 작업에 필요한 모든 사용 권한의 유효성을 검사하지 않습니다. 이러한 이유로 플랫폼 서비스를 사용하려고 할 때 오류(예: "403 금지됨")가 발생하면 끝점의 자격 증명과 연결된 사용 권한을 확인하십시오.

관련 정보

- "StorageGRID 및 GT 관리, 플랫폼 서비스 문제 해결"
- "플랫폼 서비스 끝점을 만듭니다"
- "플랫폼 서비스 끝점에 대한 연결을 테스트합니다"
- "플랫폼 서비스 끝점을 편집합니다"

CloudMirror 복제를 구성합니다

를 클릭합니다 "CloudMirror 복제 서비스" 는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. CloudMirror 복제를 사용하여 오브젝트를 외부 S3 버킷에 자동으로 복제할 수 있습니다.

시작하기 전에

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 복제 소스로 사용할 버킷을 이미 생성했습니다.
- CloudMirror 복제의 대상으로 사용하려는 엔드포인트가 이미 있으며 URN이 있습니다.
- 이 있는 사용자 그룹에 속해 있습니다 "모든 버킷 또는 루트 액세스 권한을 관리합니다". 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

CloudMirror 복제는 소스 버킷에서 엔드포인트에 지정된 대상 버킷으로 객체를 복제합니다.

CloudMirror 복제는 교차 그리드 복제 기능과의 중요한 유사점과 차이점이 있습니다. 자세한 내용은 을 참조하십시오 "교차 그리드 복제와 CloudMirror 복제를 비교합니다".

버킷에 대해 CloudMirror 복제를 활성화하려면 유효한 버킷 복제 구성 XML을 생성하고 적용해야 합니다. 복제 구성 XML은 각 대상에 대해 S3 버킷 엔드포인트의 URN을 사용해야 합니다.

S3 오브젝트 잠금이 활성화된 소스 또는 대상 버킷에는 복제가 지원되지 않습니다.

버킷 복제 및 구성 방법에 대한 일반 정보는 을 참조하십시오 "Amazon S3(Simple Storage Service) 문서: 오브젝트 복제". StorageGRID가 GetBuckketReplication, DeleteBuckReplication 및 PutBuckReplication을 구현하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷 작업".

객체가 포함된 버킷에서 CloudMirror 복제를 활성화하면 버킷에 추가된 새 객체가 복제되지만 버킷의 기존 객체는 복제되지 않습니다. 복제를 트리거하려면 기존 객체를 업데이트해야 합니다.

복제 구성 XML에서 스토리지 클래스를 지정하는 경우 StorageGRID는 대상 S3 끝점에 대해 작업을 수행할 때 해당 클래스를 사용합니다. 대상 끝점은 지정된 저장소 클래스도 지원해야 합니다. 대상 시스템 공급업체에서 제공하는 권장 사항을 따르십시오.

단계

1. 소스 버킷에 대한 복제 지원:

   텍스트 편집기를 사용하여 S3 복제 API에 지정된 대로 복제를 활성화하는 데 필요한 복제 구성 XML을 생성합니다. XML을 구성할 때:

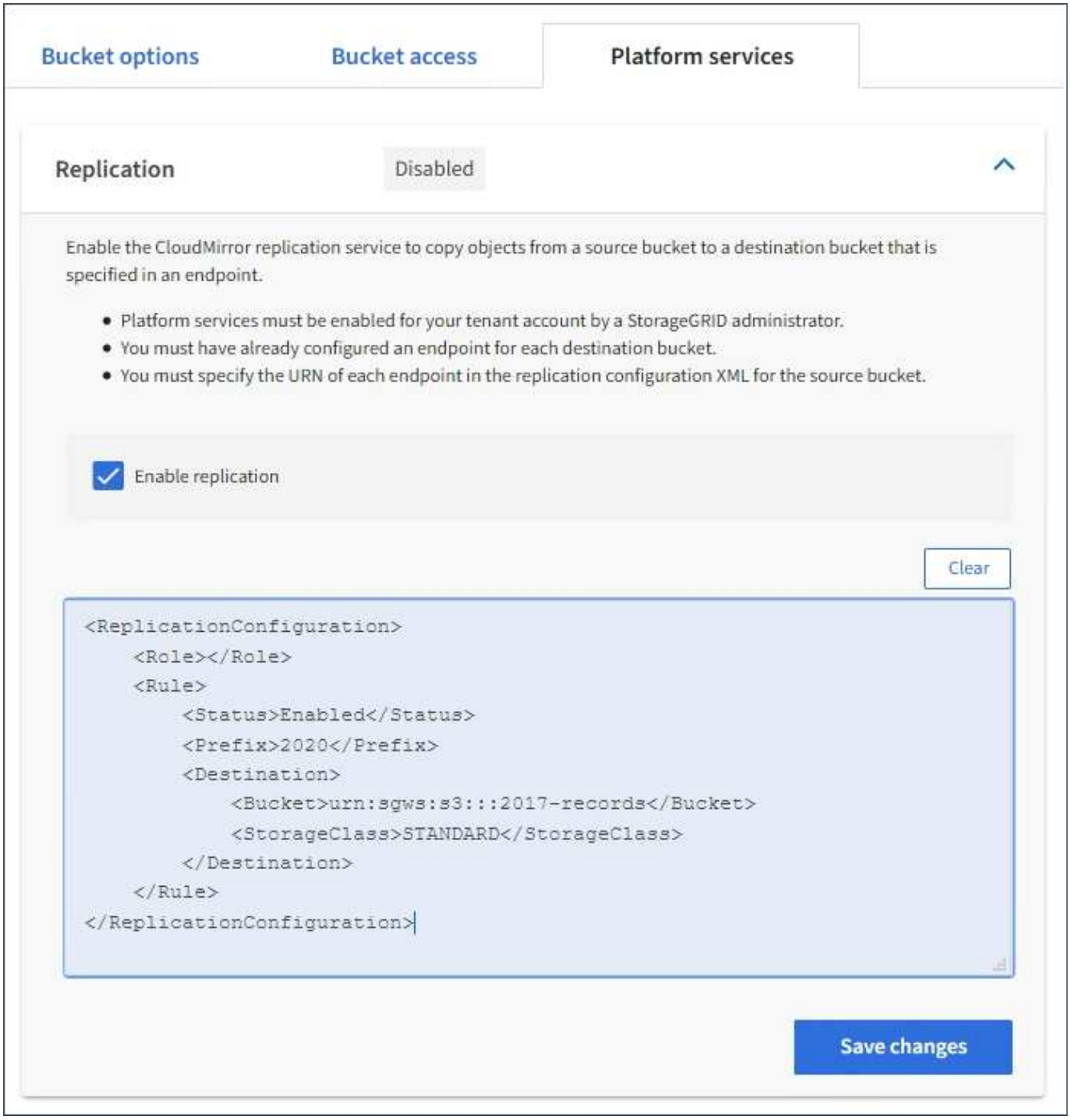
   - StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 의 사용을 지원하지 않습니다 `Filter` 규칙에 대한 요소로, 개체 버전 삭제에 대한 V1 규칙을 따릅니다. 자세한 내용은 복제 구성에 대한 Amazon 설명서를 참조하십시오.
   - S3 버킷 엔드포인트의 URN을 대상으로 사용합니다.
   - 필요에 따라 를 추가합니다 `<StorageClass>` 요소 로 다음 중 하나를 지정합니다.
     - `STANDARD`기본 스토리지 클래스입니다. 객체를 업로드할 때 스토리지 클래스를 지정하지 않으면 가 표시됩니다 `STANDARD` 스토리지 클래스가 사용됩니다.
     - `STANDARD_IA`(표준 - 낮은 액세스 빈도) 액세스 빈도가 낮지만 필요한 경우 빠른 액세스가 필요한 데이터에 이 스토리지 클래스를 사용합니다.
     - `REDUCED_REDUNDANCY`: 보다 낮은 중복성으로 저장할 수 있는 비위험, 재현성 있는 데이터에 이 스토리지 클래스를 사용합니다 `STANDARD` 스토리지 클래스.
   - 를 지정할 경우 `Role` 구성 XML에서는 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 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 복제 * 를 선택합니다.
5. 복제 사용 * 확인란을 선택합니다.
6. 복제 구성 XML을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 복제가 올바르게 구성되었는지 확인합니다.
   a. 복제 구성에 지정된 대로 복제 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞에 나와 있는 예에서 접두사 "2020"과 일치하는 객체가 복제됩니다.

   b. 객체가 대상 버킷에 복제되었는지 확인합니다.

      오브젝트 크기가 작은 경우 복제가 빠르게 수행됩니다.

관련 정보

"플랫폼 서비스 끝점을 만듭니다"

이벤트 알림을 구성합니다

알림 서비스는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. 버킷에 대한 알림을 활성화하여 지정된 이벤트에 대한 정보를 AWS SNS(Simple Notification Service)를 지원하는 대상 Kafka 클러스터 또는 서비스로 전송할 수 있습니다.

시작하기 전에

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 알림 소스로 사용할 버킷을 이미 생성했습니다.
- 이벤트 알림 대상으로 사용하려는 엔드포인트가 이미 있으며 URN이 있습니다.
- 이 있는 사용자 그룹에 속해 있습니다 "모든 버킷 또는 루트 액세스 권한을 관리합니다". 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

이벤트 알림을 구성한 후 소스 버킷의 오브젝트에 대해 지정된 이벤트가 발생할 때마다 알림이 생성되어 대상 끝점으로 사용되는 Amazon SNS 또는 Kafka 토픽으로 전송됩니다. 버킷에 대한 알림을 활성화하려면 유효한 알림 구성 XML을 생성하고 적용해야 합니다. 알림 구성 XML은 각 대상에 대해 이벤트 알림 끝점의 URN을 사용해야 합니다.

이벤트 알림 및 구성 방법에 대한 일반 정보는 아마존 문서를 참조하십시오. StorageGRID에서 S3 버킷 알림 구성 API를 구현하는 방법에 대한 자세한 내용은 를 참조하십시오 "S3 클라이언트 애플리케이션 구현 지침".

객체가 포함된 버킷에 대해 이벤트 알림을 활성화하면 알림 구성이 저장된 후 수행되는 작업에 대해서만 알림이 전송됩니다.

단계

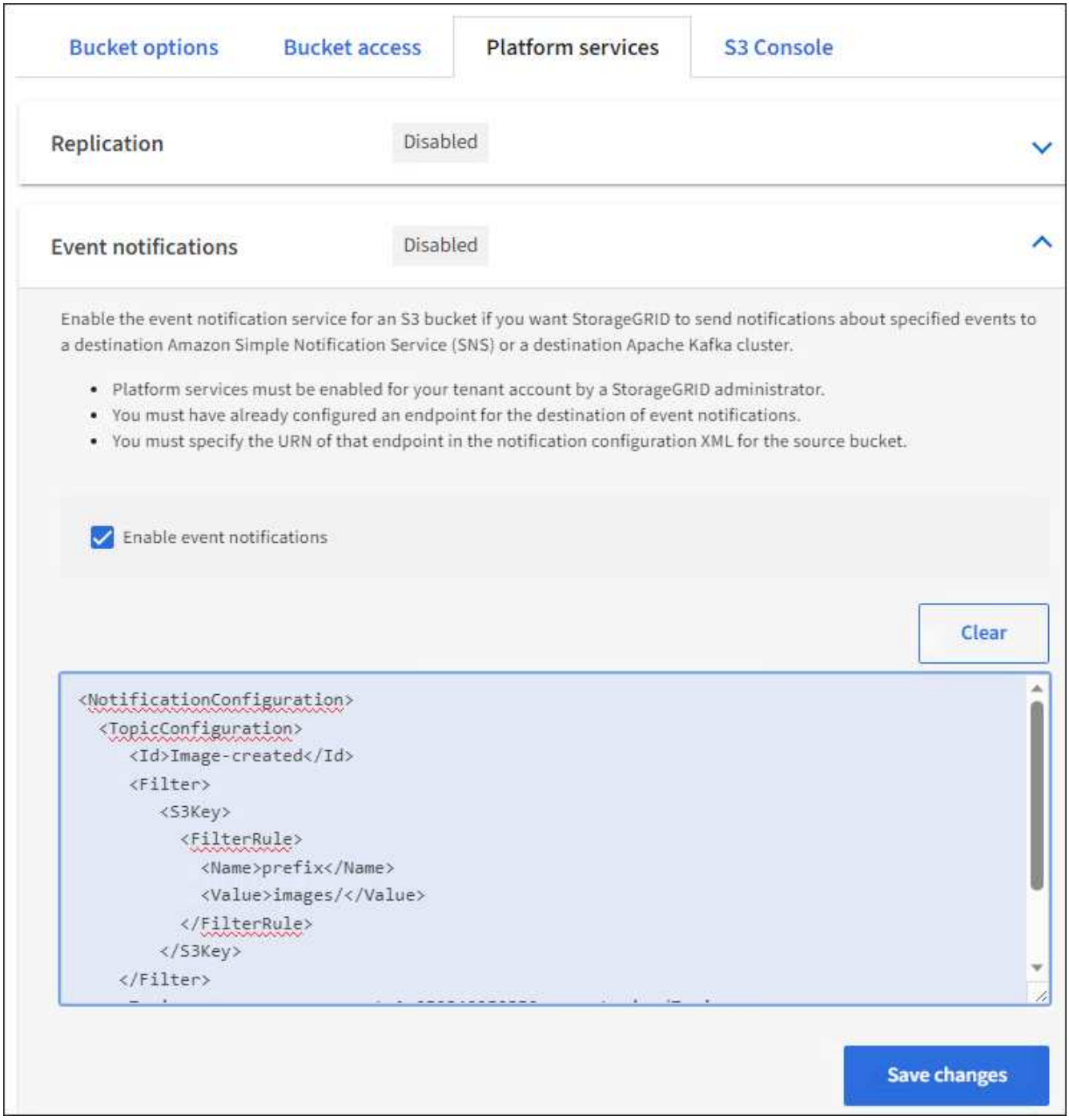
1. 소스 버킷에 대한 알림 활성화:
    - 텍스트 편집기를 사용하여 S3 알림 API에 지정된 대로 이벤트 알림을 활성화하는 데 필요한 알림 구성 XML을 생성합니다.
    - XML을 구성할 때는 이벤트 알림 끝점의 URN을 대상 항목으로 사용합니다.

```
<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 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 이벤트 알림 * 을 선택합니다.
5. 이벤트 알림 사용 * 확인란을 선택합니다.
6. 알림 구성 XML을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 이벤트 알림이 올바르게 구성되었는지 확인합니다.

   a. 구성 XML에 구성된 알림을 트리거하기 위한 요구 사항을 충족하는 소스 버킷의 객체에 대한 작업을 수행합니다.

      이 예제에서는 로 개체를 만들 때마다 이벤트 알림이 전송됩니다 `images/` 접두어.

   b. 알림이 대상 Amazon SNS 또는 Kafka 토픽에 전달되었는지 확인합니다.

예를 들어 대상 주제가 Amazon SNS에 호스팅되어 있는 경우 알림이 배달될 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 항목에서 알림이 수신되면 StorageGRID 알림에 대한 소스 버킷을 성공적으로 구성한 것입니다.

관련 정보

"버킷에 대한 알림을 이해합니다"

"S3 REST API 사용"

"플랫폼 서비스 끝점을 만듭니다"

검색 통합 서비스를 사용합니다

검색 통합 서비스는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. 오브젝트 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 오브젝트 메타데이터를 전송하도록 이 서비스를 활성화할 수 있습니다.

테넌트 관리자를 사용하여 버킷에 사용자 지정 StorageGRID 구성 XML을 적용하여 검색 통합을 구성할 수 있습니다.

> 검색 통합 서비스로 인해 개체 메타데이터가 대상으로 전송되기 때문에 해당 구성 XML을 _ 메타데이터 알림 구성 xml _ 이라고 합니다. 이 구성 XML은 이벤트 알림을 설정하는 데 사용되는 _notification 구성 xml_과 다릅니다.

를 참조하십시오 "S3 클라이언트 애플리케이션 구현 지침" 다음 사용자 지정 StorageGRID S3 REST API 작업에 대한 자세한 내용은 다음을 참조하십시오.

- 버킷 메타데이터 알림 구성을 삭제합니다
- Bucket 메타데이터 알림 구성 가져오기
- Put Bucket 메타데이터 알림 구성

관련 정보

"검색 통합을 위한 구성 XML"

"메타데이터 알림에 포함된 개체 메타데이터입니다"

"JSON이 검색 통합 서비스에 의해 생성되었습니다"

"검색 통합 서비스를 구성합니다"

"S3 REST API 사용"

검색 통합을 위한 구성 **XML**

검색 통합 서비스는 에 포함된 규칙 집합을 사용하여 구성됩니다 `<MetadataNotificationConfiguration>` 및 `</MetadataNotificationConfiguration>` 태그. 각 규칙은 규칙이 적용되는 오브젝트와 StorageGRID가 해당 오브젝트의 메타데이터를 보내야 하는 대상을 지정합니다.

개체 이름의 접두어를 기준으로 개체를 필터링할 수 있습니다. 예를 들어, 접두사가 있는 개체에 대한 메타데이터를 보낼 수 있습니다 `images` 대상이 하나인 경우 및 접두사가 있는 개체의 메타데이터입니다 `videos` 다른 사람에게. 중복되는 접두사가 있는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어, 접두사가 있는 개체에 대해 하나의 규칙을 포함하는 구성입니다 `test` 접두사가 있는 개체에 대한 두 번째 규칙입니다 `test2` 허용되지 않습니다.

검색 통합 서비스를 위해 생성된 StorageGRID 엔드포인트의 URN을 사용하여 대상을 지정해야 합니다. 이러한 엔드포인트는 Elasticsearch 클러스터에 정의된 인덱스 및 유형을 나타냅니다.

```
<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 표에서는 메타데이터 알림 구성 XML의 요소에 대해 설명합니다.

이름	설명	필수 요소입니다
MetadataNotificationConfiguration을 참조하십시오	메타데이터 알림의 개체 및 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 규칙 요소가 포함되어 있습니다.	예
규칙	메타데이터를 지정된 인덱스에 추가해야 하는 개체를 식별하는 규칙의 컨테이너 태그입니다. 접두사가 겹치는 규칙은 거부됩니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID입니다	규칙의 고유 식별자입니다. Rule 요소에 포함되어 있습니다.	아니요
상태	상태는 '활성화' 또는 '비활성화'가 될 수 있습니다. 비활성화된 규칙에 대해 어떠한 작업도 수행되지 않습니다. Rule 요소에 포함되어 있습니다.	예

이름	설명	필수 요소입니다
접두어	접두사와 일치하는 개체는 규칙의 영향을 받으며 해당 메타데이터는 지정된 대상으로 전송됩니다. 모든 오브젝트를 일치시키려면 빈 접두사를 지정합니다. Rule 요소에 포함되어 있습니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. Rule 요소에 포함되어 있습니다.	예
urn	객체 메타데이터가 전송되는 대상의 urn입니다. 다음 속성을 가진 StorageGRID 끝점의 URN이어야 합니다. • `es` 세 번째 요소여야 합니다. • URN은 메타데이터가 저장된 인덱스 및 형식으로 양식에 끝나야 합니다 `domain-name/myindex/mytype`. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 취합니다. • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 구성 XML을 제출하기 전에 끝점을 구성해야 합니다. 그렇지 않으면 404 오류로 인해 구성이 실패합니다. urn은 Destination 요소에 포함됩니다.	예

샘플 메타데이터 알림 구성 XML을 사용하여 고유한 XML을 구성하는 방법을 배웁니다.

모든 개체에 적용되는 메타데이터 알림 구성입니다

이 예제에서 모든 오브젝트의 오브젝트 메타데이터는 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>
```

두 가지 규칙을 사용하여 메타데이터 알림 구성

이 예제에서는 접두사와 일치하는 개체의 개체 메타데이터를 보여 줍니다 `/images` 은(는) 한 대상으로 전송되지만 접두사와 일치하는 오브젝트의 오브젝트 메타데이터는 전송됩니다 `/videos` 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>
```

관련 정보

"S3 REST API 사용"

"메타데이터 알림에 포함된 개체 메타데이터입니다"

"JSON이 검색 통합 서비스에 의해 생성되었습니다"

"검색 통합 서비스를 구성합니다"

검색 통합 서비스를 구성합니다

검색 통합 서비스는 개체가 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 개체 메타데이터를 보냅니다.

시작하기 전에

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 인덱싱할 콘텐츠가 있는 S3 버킷을 이미 생성했습니다.
- 검색 통합 서비스의 대상으로 사용하려는 엔드포인트가 이미 있으며 URN이 있습니다.
- 이 있는 사용자 그룹에 속해 있습니다 "모든 버킷 또는 루트 액세스 권한을 관리합니다". 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

소스 버킷에 대한 검색 통합 서비스를 구성한 후 객체를 만들거나 객체의 메타데이터 또는 태그를 업데이트하면 대상 엔드포인트로 객체 메타데이터가 전송됩니다. 이미 객체가 포함된 버킷에 대해 검색 통합 서비스를 활성화하면 기존 객체에 대한 메타데이터 알림이 자동으로 전송되지 않습니다. 이러한 기존 개체를 업데이트하여 대상 검색 인덱스에 해당 메타데이터가 추가되도록 해야 합니다.

단계

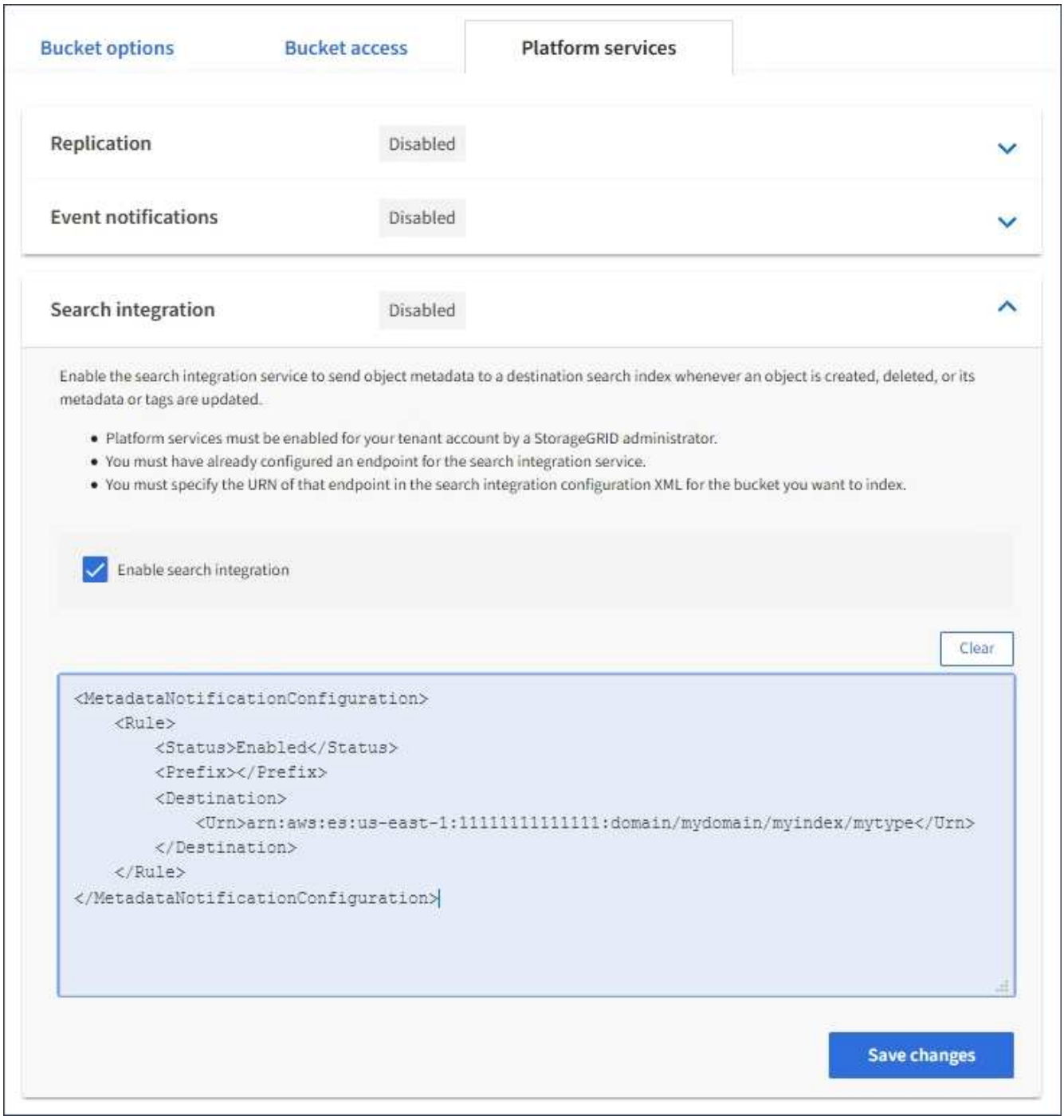
1. 텍스트 편집기를 사용하여 검색 통합을 활성화하는 데 필요한 메타데이터 알림 XML을 만듭니다.
   - 검색 통합을 위한 구성 XML에 대한 정보를 참조하십시오.
   - XML을 구성할 때는 검색 통합 끝점의 URN을 대상으로 사용합니다.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 통합 검색 * 을 선택합니다
5. 검색 통합 사용 * 확인란을 선택합니다.
6. 메타데이터 알림 구성을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



그리드 관리자 또는 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

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

      앞의 예제에서 버킷에 추가된 모든 오브젝트는 메타데이터 알림을 트리거합니다.

   b. 개체의 메타데이터와 태그가 포함된 JSON 문서가 끝점에 지정된 검색 인덱스에 추가되었는지 확인합니다.

작업을 마친 후

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

- 스토리지(S3) * > * 버킷 * 을 선택하고 * 검색 통합 활성화 * 확인란의 선택을 취소합니다.
- S3 API를 직접 사용하는 경우 Delete Bucket 메타데이터 알림 요청을 사용합니다. S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

관련 정보

"검색 통합 서비스를 이해합니다"

"검색 통합을 위한 구성 XML"

"S3 REST API 사용"

"플랫폼 서비스 끝점을 만듭니다"

JSON이 검색 통합 서비스에 의해 생성되었습니다

버킷에 대한 검색 통합 서비스를 활성화하면 개체 메타데이터 또는 태그를 추가, 업데이트 또는 삭제할 때마다 JSON 문서가 생성되어 대상 끝점으로 전송됩니다.

이 예제에서는 키가 있는 개체가 생성될 수 있는 JSON의 예를 보여 줍니다 `SGWS/Tagging.txt` 이(가) 라는 이름의 버킷에 생성됩니다 `test`. 를 클릭합니다 `test` 버킷의 버전이 지정되지 않으므로 이(가) 이(가) 필요합니다 `versionId` 태그가 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 개체 메타데이터입니다

이 표에는 검색 통합이 활성화된 경우 대상 끝점으로 전송되는 JSON 문서에 포함된 모든 필드가 나열됩니다.

문서 이름에는 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)가 포함됩니다.

유형	항목 이름 및 설명입니다
버킷 및 오브젝트 정보	`bucket`: 버킷의 이름입니다
`key`: 개체 키 이름	`versionID`: 오브젝트 버전, 버전이 있는 버킷의 오브젝트
`region`버킷 영역(예: `us-east-1`	시스템 메타데이터
`size`: HTTP 클라이언트에 표시되는 개체 크기(바이트)입니다	`md5`: 객체 해시
사용자 메타데이터	`metadata`: 오브젝트의 모든 사용자 메타데이터를 키 값 쌍으로 사용합니다 `key:value`
태그	`tags`: 객체에 대해 정의된 모든 객체 태그를 키 값 쌍으로 사용합니다 `key:value`

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