S3 REST API 사용

StorageGRID

NetApp
October 03, 2025

목차

S3을 사용합니다

클라이언트 애플리케이션이 S3 API를 사용하여 StorageGRID 시스템과 어떻게 상호 작용할 수 있는지 알아보십시오.

- "S3 REST API 지원"
- "테넌트 계정 및 연결 구성"
- "StorageGRID에서 S3 REST API를 구축하는 방법"
- "S3 REST API에서 지원되는 작업 및 제한 사항"
- "StorageGRID S3 REST API 작업"
- "버킷 및 그룹 액세스 정책"
- "REST API에 대한 보안 구성"
- "작업 모니터링 및 감사"
- "활성, 유휴 및 동시 HTTP 연결의 이점"

S3 REST API 지원

StorageGRID는 REST(Representational State Transfer) 웹 서비스 세트로 구현되는 S3(Simple Storage Service) API를 지원합니다. S3 REST API를 지원하므로 StorageGRID 시스템을 사용하는 사내 오브젝트 스토리지와 S3 웹 서비스를 위해 개발된 서비스 지향 애플리케이션을 연결할 수 있습니다. 따라서 클라이언트 애플리케이션의 현재 S3 REST API 호출 사용에 대한 변경이 최소화됩니다.

- "S3 REST API 지원으로 변경"
- "지원되는 버전"
- "StorageGRID 플랫폼 서비스 지원"

S3 REST API 지원으로 변경

S3 REST API에 대한 StorageGRID 시스템의 지원 변경사항을 알고 있어야 합니다.

놓습니다	설명
11.5	• 버킷 암호화 관리에 대한 지원이 추가되었습니다. • S3 오브젝트 잠금 및 더 이상 사용되지 않는 레거시 규정 준수 요청에 대한 지원 추가 • 버전이 있는 버킷에서 여러 오브젝트 삭제 사용에 대한 지원이 추가되었습니다. • 를 클릭합니다 `Content-MD5` 이제 요청 헤더가 올바르게 지원됩니다.

놓습니다	설명
11.4	• 버킷 태그 삭제, 버킷 태그 지정 가져오기 및 버킷 태그 지정을 위한 지원이 추가되었습니다. 비용 할당 태그는 지원되지 않습니다. • StorageGRID 11.4에서 만든 버킷의 경우 성능 모범 사례에 맞게 개체 키 이름을 제한하는 것이 더 이상 필요하지 않습니다. • 에서 버킷 알림에 대한 지원이 추가되었습니다 `s3:ObjectRestore:Post` 이벤트 유형입니다. • 이제 여러 파트에 대한 AWS 크기 제한이 적용됩니다. 멀티파트 업로드의 각 파트는 5MiB에서 5GiB 사이여야 합니다. 마지막 부분은 5MiB보다 작을 수 있습니다. • TLS 1.3에 대한 지원 및 지원되는 TLS 암호 제품군의 업데이트된 목록이 추가되었습니다. • CLB 서비스는 더 이상 사용되지 않습니다.
11.3	• 고객이 제공한 키(SSE-C)를 사용하여 오브젝트 데이터의 서버측 암호화에 대한 지원이 추가되었습니다. • 버킷 수명주기 작업(만료 작업에만 해당) 및 에 대한 삭제, 가져오기 및 Put 지원 추가 `x-amz-expiration` 응답 헤더. • 수집 시 동기식 배치를 사용하는 ILM 규칙의 영향을 설명하기 위해 PUT 개체, Put Object-Copy 및 MultiPart Upload가 업데이트되었습니다. • 지원되는 TLS 암호 그룹 목록이 업데이트되었습니다. TLS 1.1 암호가 더 이상 지원되지 않습니다.
11.2	클라우드 스토리지 풀과 함께 사용할 POST 오브젝트 복원에 대한 지원이 추가되었습니다. 그룹 및 버킷 정책에서 ARN, 정책 조건 키 및 정책 변수에 대해 AWS 구문 사용을 지원합니다. StorageGRID 구문을 사용하는 기존 그룹 및 버킷 정책은 계속 지원됩니다. • 참고: * 사용자 지정 StorageGRID 기능에 사용되는 것을 포함하여 다른 구성 JSON/XML에서 ARN/URN을 사용하는 것은 변경되지 않았습니다.
11.1	CORS(Cross-Origin Resource Sharing), 그리드 노드에 대한 S3 클라이언트 연결을 위한 HTTP 및 버킷의 규정 준수 설정에 대한 지원이 추가되었습니다.

놓습니다	설명
11.0	버킷에 대한 플랫폼 서비스(CloudMirror 복제, 알림 및 Elasticsearch 검색 통합) 구성 지원 추가 또한 버킷에 대한 객체 태그 지정 위치 제약 조건 및 사용 가능한 정합성 제어 설정에 대한 지원이 추가되었습니다.
10.4	버전 관리, 끝점 도메인 이름 페이지 업데이트, 정책, 정책 예제 및 PutOverwriteObject 권한에 대한 ILM 검색 변경 사항에 대한 지원이 추가되었습니다.
10.3	버전 관리 지원 추가.
10.2	그룹 및 버킷 액세스 정책 및 다중 파트 복제본(업로드 부분 복사)에 대한 지원이 추가되었습니다.
10.1	멀티파트 업로드, 가상 호스팅 스타일 요청 및 v4 인증에 대한 지원이 추가되었습니다.
10.0	StorageGRID 시스템에서 S3 REST API의 초기 지원. 현재 지원되는 _Simple Storage Service API Reference_는 2006-03-01입니다.

지원되는 버전

StorageGRID는 다음과 같은 S3 및 HTTP 버전을 지원합니다.

항목	버전
S3 사양	_Simple Storage Service API Reference_2006-03-01
HTTP	1.1 HTTP에 대한 자세한 내용은 HTTP/1.1(RFC 7230-35)을 참조하십시오. • 참고 *: StorageGRID는 HTTP/1.1 파이프라이닝을 지원하지 않습니다.

관련 정보

"IETF RFC 2616:HTTP/1.1(Hypertext Transfer Protocol)"

"AWS(Amazon Web Services) 문서: Amazon Simple Storage Service API Reference 를 참조하십시오"

StorageGRID 플랫폼 서비스 지원

StorageGRID 플랫폼 서비스를 사용하면 StorageGRID 테넌트 계정에서 원격 S3 버킷,

SNS(Simple Notification Service) 엔드포인트 또는 Elasticsearch 클러스터와 같은 외부 서비스를 활용하여 그리드에 의해 제공되는 서비스를 확장할 수 있습니다.

다음 표에는 사용 가능한 플랫폼 서비스와 이를 구성하는 데 사용되는 S3 API가 요약되어 있습니다.

플랫폼 서비스	목적	**S3 API**를 사용하여 서비스를 구성합니다
CloudMirror 복제	소스 StorageGRID 버킷에서 구성된 원격 S3 버킷으로 오브젝트를 복제합니다.	버킷 복제를 배치합니다
알림	소스 StorageGRID 버킷의 이벤트에 대한 알림을 구성된 SNS(Simple Notification Service) 엔드포인트로 보냅니다.	버킷 통지를 보냅니다
검색 통합	StorageGRID 버킷에 저장된 객체에 대한 객체 메타데이터를 구성된 Elasticsearch 인덱스로 전송합니다.	Bucket 메타데이터 알림을 배치합니다 • 참고: * 이것은 StorageGRID 사용자 정의 S3 API입니다.

그리드 관리자는 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 사용할 수 있습니다. 그런 다음 테넌트 관리자는 테넌트 계정의 원격 서비스를 나타내는 끝점을 만들어야 합니다. 서비스를 구성하려면 이 단계가 필요합니다.

플랫폼 서비스 사용을 위한 권장 사항

플랫폼 서비스를 사용하기 전에 다음 권장 사항을 숙지해야 합니다.

- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청을 가진 활성 테넌트 100개 이상을 허용하지 않는 것이 좋습니다. 활성 테넌트가 100개 이상인 경우 S3 클라이언트 성능이 저하될 수 있습니다.
- StorageGRID 시스템의 S3 버켓에서 버전 관리 및 CloudMirror 복제를 모두 사용하는 경우, 대상 엔드포인트에 S3 버킷 버전 관리도 활성화할 것을 권장합니다. 이를 통해 CloudMirror 복제가 엔드포인트에 비슷한 개체 버전을 생성할 수 있습니다.
- 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.
- 대상 버킷에 레거시 규정 준수 기능이 설정된 경우 CloudMirror 복제가 실패하고 AccessDenied 오류가 표시됩니다.

관련 정보

"테넌트 계정을 사용합니다"

"StorageGRID 관리"

"버킷 작업"

"PUT 버킷 메타데이터 알림 구성 요청"

테넌트 계정 및 연결 구성

클라이언트 응용 프로그램에서 연결을 허용하도록 StorageGRID를 구성하려면 하나 이상의 테넌트 계정을 만들고 연결을 설정해야 합니다.

S3 테넌트 계정 생성 및 구성

S3 API 클라이언트가 StorageGRID에 오브젝트를 저장하고 검색할 수 있으려면 먼저 S3 테넌트 계정이 필요합니다. 각 테넌트 계정에는 고유한 계정 ID, 그룹 및 사용자, 컨테이너 및 객체가 있습니다.

S3 테넌트 계정은 StorageGRID 그리드 관리자가 그리드 관리자 또는 그리드 관리 API를 사용하여 생성합니다. S3 테넌트 계정을 생성할 때 그리드 관리자는 다음 정보를 지정합니다.

- 테넌트의 표시 이름(테넌트의 계정 ID가 자동으로 할당되며 변경할 수 없음)
- 테넌트 계정이 플랫폼 서비스를 사용하도록 허용되는지 여부 플랫폼 서비스를 사용할 수 있는 경우 그리드 사용을 지원하도록 구성해야 합니다.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.
- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

S3 테넌트 계정이 생성된 후 테넌트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 소스를 그리드와 공유하지 않는 경우 ID 페더레이션을 설정하고 로컬 그룹 및 사용자를 만듭니다
- S3 액세스 키를 관리합니다
- S3 오브젝트 잠금이 설정된 버킷을 포함하여 S3 버킷을 생성하고 관리합니다
- 플랫폼 서비스 사용(활성화된 경우)
- 스토리지 사용량을 모니터링합니다

> S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 버킷을 생성 및 관리할 수 있지만, S3 액세스 키를 가지고 S3 REST API를 사용하여 오브젝트를 수집 및 관리해야 합니다.

관련 정보

"StorageGRID 관리"

"테넌트 계정을 사용합니다"

클라이언트 연결 구성 방법

그리드 관리자는 S3 클라이언트가 StorageGRID에 연결하여 데이터를 저장 및 검색하는 방법에 영향을 주는 구성을 선택합니다. 연결에 필요한 특정 정보는 선택한 구성에 따라 다릅니다.

클라이언트 응용 프로그램은 다음 중 하나를 연결하여 개체를 저장하거나 검색할 수 있습니다.

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 또는 선택적으로 관리 노드 또는 게이트웨이 노드의 고가용성(HA) 그룹의 가상 IP 주소입니다
- 게이트웨이 노드의 CLB 서비스 또는 게이트웨이 노드의 고가용성 그룹의 가상 IP 주소(선택 사항)입니다

> CLB 서비스는 더 이상 사용되지 않습니다. StorageGRID 11.3 릴리스 전에 구성된 클라이언트는 게이트웨이 노드에서 CLB 서비스를 계속 사용할 수 있습니다. 로드 밸런싱을 제공하기 위해 StorageGRID에 의존하는 다른 모든 클라이언트 애플리케이션은 로드 밸런서 서비스를 사용하여 연결해야 합니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

StorageGRID를 구성할 때 그리드 관리자는 그리드 관리자 또는 그리드 관리 API를 사용하여 다음 단계를 수행할 수 있습니다. 이 모든 단계는 선택 사항입니다.

1. 로드 밸런서 서비스의 끝점을 구성합니다.

   로드 밸런서 서비스를 사용하려면 끝점을 구성해야 합니다. 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 분산합니다. 로드 밸런서 끝점을 만들 때 StorageGRID 관리자는 포트 번호, 엔드포인트가 HTTP 또는 HTTPS 연결을 수락하는지 여부, 엔드포인트를 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 지정합니다.

2. 신뢰할 수 없는 클라이언트 네트워크를 구성합니다.

   StorageGRID 관리자가 노드의 클라이언트 네트워크를 신뢰할 수 없도록 구성하는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 클라이언트 네트워크에서 인바운드 연결만 허용합니다.

3. 고가용성 그룹을 구성합니다.

   관리자가 HA 그룹을 생성하면 여러 관리 노드 또는 게이트웨이 노드의 네트워크 인터페이스가 액티브-백업 구성에 배치됩니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.

각 옵션에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

관련 정보

"StorageGRID 관리"

요약: 클라이언트 연결을 위한 IP 주소 및 포트

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드의 서비스 포트 번호를 사용하여 StorageGRID에 접속합니다. HA(고가용성) 그룹이 구성되어 있는 경우 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소를 사용하여 연결할 수 있습니다.

클라이언트 연결을 만드는 데 필요한 정보입니다

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가 요약되어 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하거나 StorageGRID 관리 지침 에서 그리드 관리자에서 이 정보를 찾는 방법에 대한 설명을 참조하십시오.

연결 위치	클라이언트가 연결하는 서비스입니다	**IP** 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
HA 그룹	CLB 참고:** CLB 서비스는 더 이상 사용되지 않습니다.	HA 그룹의 가상 IP 주소입니다	기본 S3 포트: • HTTPS: 8082 • HTTP: 8084
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	CLB 참고:** CLB 서비스는 더 이상 사용되지 않습니다.	게이트웨이 노드의 IP 주소입니다 • 참고:** 기본적으로 CLB 및 LDR에 대한 HTTP 포트는 사용되지 않습니다.	기본 S3 포트: • HTTPS: 8082 • HTTP: 8084
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: • HTTPS: 18082 • HTTP: 18084

예

S3 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

- `https://VIP-of-HA-group:_LB-endpoint-port_`

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.5이고 S3 로드 밸런서 끝점의 포트 번호가 10443인 경우 S3 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- `https://192.0.2.5:10443`

클라이언트가 StorageGRID에 연결하는 데 사용하는 IP 주소에 대한 DNS 이름을 구성할 수 있습니다. 로컬 네트워크 관리자에게 문의하십시오.

관련 정보

"StorageGRID 관리"

HTTPS 또는 HTTP 연결 사용 결정

로드 밸런서 끝점을 사용하여 클라이언트 연결을 만들 때는 해당 끝점에 지정된 프로토콜(HTTP 또는 HTTPS)을 사용하여 연결해야 합니다. 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 대한 클라이언트 연결에 HTTP를 사용하려면 해당 사용을 설정해야 합니다.

기본적으로 클라이언트 응용 프로그램이 게이트웨이 노드의 스토리지 노드 또는 CLB 서비스에 연결할 때는 모든 연결에 암호화된 HTTPS를 사용해야 합니다. 선택적으로 Grid Manager에서 * HTTP Connection * 그리드 사용 옵션을 선택하여 보안성이 떨어지는 HTTP 연결을 활성화할 수 있습니다. 예를 들어, 클라이언트 애플리케이션은 비운영 환경에서 스토리지 노드에 대한 접속을 테스트할 때 HTTP를 사용할 수 있습니다.

> 요청은 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

HTTP 연결 사용 * 옵션을 선택한 경우 클라이언트는 HTTPS에 사용하는 것과 다른 HTTP 포트를 사용해야 합니다. StorageGRID 관리 지침을 참조하십시오.

관련 정보

"StorageGRID 관리"

"활성, 유휴 및 동시 HTTP 연결의 이점"

S3 요청에 대한 끝점 도메인 이름입니다

클라이언트 요청에 S3 도메인 이름을 사용하려면 StorageGRID 관리자가 S3 경로 스타일 및 S3 가상 호스팅 스타일 요청에서 S3 도메인 이름을 사용하는 연결을 허용하도록 시스템을 구성해야 합니다.

이 작업에 대해

S3 가상 호스팅 스타일 요청을 사용하려면 그리드 관리자가 다음 작업을 수행해야 합니다.

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서가 클라이언트에 필요한 모든 도메인 이름에 서명되었는지 확인합니다.

  예를 들어, 끝점이 인 경우 `s3.company.com`그리드 관리자는 `HTTPS` 연결에 사용되는 인증서에 가 포함되어 있는지 확인해야 합니다 `s3.company.com` 끝점 및 끝점의 와일드카드 주체 대체 이름(SAN): `*.s3.company.com`.

- 필요한 와일드카드 레코드를 포함하여 끝점 도메인 이름과 일치하는 DNS 레코드를 포함하도록 클라이언트에서 사용하는 DNS 서버를 구성합니다.

클라이언트가 로드 밸런서 서비스를 사용하여 연결하는 경우 그리드 관리자가 구성하는 인증서는 클라이언트가 사용하는 로드 밸런서 끝점에 대한 인증서입니다.

> 각 로드 밸런서 끝점마다 고유한 인증서가 있으며 각 끝점이 서로 다른 끝점 도메인 이름을 인식하도록 구성할 수 있습니다.

클라이언트가 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 연결하는 경우 그리드 관리자가 구성하는 인증서는

그리드에 사용되는 단일 사용자 지정 서버 인증서입니다.

CLB 서비스는 더 이상 사용되지 않습니다.

자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

이러한 단계를 완료한 후 가상 호스팅 스타일 요청(예: `bucket.s3.company.com`)를 클릭합니다.

관련 정보

"StorageGRID 관리"

"REST API에 대한 보안 구성"

S3 REST API 구성 테스트

AWS CLI(Amazon Web Services Command Line Interface)를 사용하여 시스템에 대한 연결을 테스트하고 시스템에 개체를 읽고 쓸 수 있는지 확인할 수 있습니다.

필요한 것

- 에서 AWS CLI를 다운로드하여 설치해야 합니다 "aws.amazon.com/cli".
- StorageGRID 시스템에서 S3 테넌트 계정을 생성해야 합니다.

단계

1. StorageGRID 시스템에서 생성한 계정을 사용하도록 Amazon 웹 서비스 설정을 구성합니다.
   a. 구성 모드 시작: `aws configure`
   b. 생성한 계정의 AWS 액세스 키 ID를 입력합니다.
   c. 생성한 계정의 AWS Secret Access 키를 입력합니다.
   d. 사용할 기본 영역을 입력합니다(예: us-east-1).
   e. 사용할 기본 출력 형식을 입력하거나 * Enter * 를 눌러 JSON을 선택합니다.
2. 버킷을 만듭니다.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   버킷이 성공적으로 생성되면 다음 예와 같이 버킷의 위치가 반환됩니다.

   ```
   "Location": "/testbucket"
   ```

3. 개체를 업로드합니다.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

객체가 성공적으로 업로드되면 객체 데이터의 해시인 Etag가 반환됩니다.

4. 버킷의 내용을 나열하여 객체가 업로드되었는지 확인합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. 개체를 삭제합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. 버킷을 삭제합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID에서 S3 REST API를 구축하는 방법

클라이언트 애플리케이션은 S3 REST API 호출을 사용하여 StorageGRID에 연결하여 버킷을 생성, 삭제 및 수정할 수 있을 뿐만 아니라 오브젝트를 저장 및 검색할 수 있습니다.

- "클라이언트 요청 충돌"
- "일관성 제어"
- "StorageGRID ILM 규칙이 개체를 관리하는 방법"
- "오브젝트 버전 관리"
- "S3 REST API 구현을 위한 권장 사항"

클라이언트 요청 충돌

같은 키에 쓰는 두 클라이언트 등 충돌하는 클라이언트 요청은 "최근 성공" 기준으로 해결됩니다.

"Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

일관성 제어

일관성 제어는 애플리케이션의 요구에 따라 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트 전체에서 오브젝트의 일관성 간에 균형을 조정합니다.

기본적으로 StorageGRID는 새로 생성된 개체에 대해 쓰기 후 읽기 일관성을 보장합니다. 성공적으로 완료된 PUT를 팔로우하면 새로 작성된 데이터를 읽을 수 있습니다. 기존 오브젝트, 메타데이터 업데이트 및 삭제를 덮어쓰는 것은 결국

일관성이 유지됩니다. 덮어쓰기는 일반적으로 전파되는 데 몇 초 또는 몇 분이 걸리지만 최대 15일이 소요될 수 있습니다.

오브젝트 작업을 다른 정합성 보장 레벨에서 수행하려는 경우 각 버킷 또는 각 API 작업에 대해 정합성 제어를 지정할 수 있습니다.

일관성 제어

정합성 보장 제어는 StorageGRID에서 객체를 추적하는 데 사용하는 메타데이터가 노드 간에 분산되므로 클라이언트 요청에 대한 객체의 가용성에 영향을 줍니다.

버킷 또는 API 작업에 대한 정합성 제어를 다음 값 중 하나로 설정할 수 있습니다.

일관성 제어	설명
모두	모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
강함 - 글로벌	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.
강력한 사이트	사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
읽기-후-새로-쓰기	(기본값) 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 Amazon S3 일관성 보장 과 일치합니다. • 참고: * 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 Amazon S3와 유사한 일관성 보장이 필요하지 않는 한 일관성 제어를 ""사용 가능""으로 설정합니다.
사용 가능(헤드 작업의 최종 일관성)	"새 쓰기 후 다시 쓰기" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다. 헤드 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

"새 쓰기 후"와 "사용 가능한" 일관성 제어 기능을 사용합니다

헤드 또는 GET 연산에서 "read-after-new-write" 정합성 제어 또는 GET 연산에서 ""Available"" 정합성 제어를 사용하는 경우 StorageGRID는 다음과 같이 여러 단계로 조회를 수행합니다.

- 먼저 낮은 일관성을 사용하여 오브젝트를 찾습니다.
- 이 조회가 실패하면 개체 메타데이터의 모든 복사본을 사용할 수 있어야 하는 가장 높은 일관성 수준, 즉 "모두"에 도달할 때까지 다음 일관성 수준에서 조회가 반복됩니다.

머리나 GET 연산에서 "재후기입" 일관성 제어를 사용하지만 개체가 없으면 개체 조회는 항상 ""모두"" 일관성 수준에 도달합니다. 이 정합성 보장 수준에서는 객체 메타데이터의 모든 복제본을 사용할 수 있어야 하므로 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 많이 발생할 수 있습니다.

Amazon S3와 유사한 일관성 보증이 필요하지 않으면 일관성 제어를 ""사용 가능""으로 설정하여 헤드 작업에서 이러한 오류를 방지할 수 있습니다. 헤드 작업에서 ""사용 가능"" 정합성 제어를 사용할 경우 StorageGRID는 최종 일관성만 제공합니다. "모두" 정합성 보장 수준에 도달할 때까지 실패한 작업을 다시 시도하지 않으므로 객체 메타데이터의 모든 복제본을 사용할 필요가 없습니다.

API 작업에 대한 정합성 제어 지정

개별 API 작업의 정합성 제어를 설정하려면 작업에 대해 정합성 보장 제어가 지원되어야 하며 요청 헤더에 정합성 제어를 지정해야 합니다. 이 예제에서는 개체 가져오기 작업을 위해 일관성 컨트롤을 "문자열 사이트"로 설정합니다.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

개체 넣기 작업과 개체 가져오기 작업 모두에 대해 동일한 일관성 컨트롤을 사용해야 합니다.

버킷의 일관성 제어 지정

버킷의 일관성 제어를 설정하려면 StorageGRID PUT 버킷 정합성 보장 요청 및 GET 버킷 정합성 보장 요청을 사용할 수 있습니다. 또는 테넌트 관리자 또는 테넌트 관리 API를 사용할 수 있습니다.

버킷의 정합성 제어 기능을 설정할 때는 다음 사항에 유의하십시오.

- 버킷의 일관성 제어를 설정하면 버킷의 오브젝트 또는 버킷 구성에 대해 수행된 S3 작업에 사용되는 일관성 제어가 결정됩니다. 버킷 자체의 작동에는 영향을 미치지 않습니다.
- 개별 API 작업의 정합성 제어는 버킷의 정합성 제어를 재정의합니다.
- 일반적으로 버킷은 기본 일관성 제어인 "read-after-new-write"를 사용해야 합니다. 요청이 올바르게 작동하지 않는 경우 가능한 경우 응용 프로그램 클라이언트 동작을 변경합니다. 또는 클라이언트가 각 API 요청에 대한 정합성 제어를 지정하도록 구성합니다. 버킷 레벨에서만 정합성 제어를 최후의 수단으로 설정하십시오.

일관성 제어 및 **ILM** 규칙이 상호 작용하여 데이터 보호에 영향을 미치는 방식

일관성 제어와 ILM 규칙 모두 오브젝트의 보호 방법에 영향을 미칩니다. 이러한 설정은 상호 작용할 수 있습니다.

예를 들어, 개체가 저장될 때 사용되는 일관성 컨트롤은 오브젝트 메타데이터의 초기 배치에 영향을 미치는 반면 ILM 규칙에 대해 선택된 수집 동작은 오브젝트 복사본의 초기 배치에 영향을 줍니다. StorageGRID에서는 클라이언트 요청을 이행하기 위해 오브젝트의 메타데이터와 해당 데이터에 모두 액세스해야 하므로 일관성 수준과 수집 동작에 적합한 보호 수준을 선택하면 초기 데이터 보호 수준을 높이고 시스템 응답을 더욱 정확하게 예측할 수 있습니다.

ILM 규칙에 대해 다음과 같은 수집 동작을 사용할 수 있습니다.

- * Strict * : ILM 규칙에 지정된 모든 사본은 클라이언트에 반환되기 전에 만들어야 합니다.

- * 균형 *: StorageGRID는 수집 시 ILM 규칙에 지정된 모든 복제본을 생성하려고 합니다. 그렇지 않을 경우 중간 복사본이 만들어지고 클라이언트에 성공적으로 반환됩니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.
- * 이중 커밋*: StorageGRID는 즉시 개체의 임시 복사본을 만들고 클라이언트에 성공을 반환합니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.

> ILM 규칙의 수집 동작을 선택하기 전에 정보 수명 주기 관리를 통해 개체를 관리하기 위한 지침에서 이러한 설정에 대한 전체 설명을 읽어보십시오.

일관성 제어 및 **ILM** 규칙이 상호 작용하는 방법의 예

다음 ILM 규칙 및 다음 일관성 수준 설정이 있는 두 사이트 그리드가 있다고 가정합니다.

- * ILM 규칙 *: 로컬 사이트와 원격 사이트에 각각 하나씩, 두 개의 오브젝트 복사본을 만듭니다. Strict 수집 동작이 선택됩니다.
- * Consistency level *: "trong-global"(개체 메타데이터가 모든 사이트에 즉시 배포됩니다.)

클라이언트가 오브젝트를 그리드에 저장할 때 StorageGRID는 오브젝트 복사본을 둘 다 만들고 메타데이터를 두 사이트에 분산한 다음 클라이언트에 성공을 반환합니다.

수집 성공 메시지가 표시된 시점에 객체가 손실로부터 완벽하게 보호됩니다. 예를 들어, 수집 직후 로컬 사이트가 손실되면 오브젝트 데이터와 오브젝트 메타데이터의 복사본이 원격 사이트에 계속 존재합니다. 개체를 완전히 검색할 수 있습니다.

대신 동일한 ILM 규칙 및 "'strong-site' 정합성 보장 수준을 사용한 경우 객체 데이터가 원격 사이트에 복제되었지만 객체 메타데이터가 그 위치에 배포되기 전에 클라이언트에 성공 메시지가 표시될 수 있습니다. 이 경우 오브젝트 메타데이터의 보호 수준이 오브젝트 데이터의 보호 수준과 일치하지 않습니다. 수집 후 곧바로 로컬 사이트가 손실되면 오브젝트 메타데이터가 손실됩니다. 객체를 검색할 수 없습니다.

일관성 수준과 ILM 규칙 간의 상호 관계는 복잡할 수 있습니다. 도움이 필요한 경우 NetApp에 문의하십시오.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"버킷 정합성 보장 요청 가져오기"

"버킷 정합성 보장 요청을 배치합니다"

StorageGRID ILM 규칙이 개체를 관리하는 방법

그리드 관리자는 정보 라이프사이클 관리(ILM) 규칙을 생성하여 S3 REST API 클라이언트 애플리케이션에서 StorageGRID 시스템으로 수집된 오브젝트 데이터를 관리합니다. 그런 다음 이러한 규칙을 ILM 정책에 추가하여 시간 경과에 따라 오브젝트 데이터가 저장되는 방법 및 위치를 결정합니다.

ILM 설정은 개체의 다음 측면을 결정합니다.

- * 지역 *

  StorageGRID 시스템(스토리지 풀) 또는 클라우드 스토리지 풀 내에서 오브젝트 데이터의 위치입니다.

- * 스토리지 등급 *

  오브젝트 데이터를 저장하는 데 사용되는 스토리지의 유형(예: 플래시 또는 회전식 디스크)

- * 손실 방지 *

  복제, 삭제 코딩 또는 두 가지 유형의 복사본을 만들 수와 복사본 유형을 지정합니다.

- * 보존 *

  오브젝트의 데이터 관리 방식, 저장 위치 및 데이터 손실을 보호하는 방법에 대한 시간이 지나면서 변동합니다.

- * 수집 중 보호 *

  수집 중에 오브젝트 데이터를 보호하는 데 사용되는 방법: 동기 배치(Ingest 동작에 대한 균형 또는 엄격 옵션 사용) 또는 중간 복사본 만들기(이중 커밋 옵션 사용).

ILM 규칙을 사용하여 개체를 필터링 및 선택할 수 있습니다. S3을 사용하여 수집된 개체의 경우 ILM 규칙을 통해 다음 메타데이터를 기반으로 개체를 필터링할 수 있습니다.

- 테넌트 계정
- 버킷 이름
- 수집 시간
- 키
- 마지막 액세스 시간입니다

> 기본적으로 마지막 액세스 시간에 대한 업데이트는 모든 S3 버킷에 대해 비활성화됩니다. StorageGRID 시스템에 마지막 액세스 시간 옵션을 사용하는 ILM 규칙이 포함된 경우 해당 규칙에 지정된 S3 버킷의 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다. Tenant Manager의 [버킷 최종 액세스 시간] 요청, [S3 * > * Bucket * > * [마지막 액세스 시간 구성] * 확인란을 사용하거나 Tenant Management API를 사용하여 마지막 액세스 시간 업데이트를 활성화할 수 있습니다. 마지막 액세스 시간 업데이트를 설정할 때는 특히 작은 오브젝트가 있는 시스템에서 StorageGRID 성능이 저하될 수 있다는 점에 유의하십시오.

- 위치 제약 조건
- 개체 크기
- 사용자 메타데이터
- 개체 태그

ILM에 대한 자세한 내용은 정보 수명 주기 관리를 통해 개체 관리 지침을 참조하십시오.

관련 정보

"테넌트 계정을 사용합니다"

"ILM을 사용하여 개체를 관리합니다"

"버킷 최종 액세스 시간 요청"

오브젝트 버전 관리

버전 관리를 사용하면 개체의 여러 버전을 유지하여 실수에 의한 개체 삭제로부터 보호하고 이전 버전의 개체를 검색하고 복원할 수 있습니다.

StorageGRID 시스템은 대부분의 기능을 지원하는 버전 관리를 구현하지만 몇 가지 제한 사항이 있습니다. StorageGRID는 각 오브젝트의 버전을 최대 1,000개까지 지원합니다.

오브젝트 버전 관리를 StorageGRID ILM(정보 라이프사이클 관리) 또는 S3 버킷 라이프사이클 구성과 결합할 수 있습니다. 버킷에 대해 이 기능을 설정하려면 각 버킷에 대해 버전 관리를 명시적으로 활성화해야 합니다. 버킷의 각 오브젝트에는 StorageGRID 시스템에서 생성되는 버전 ID가 할당됩니다.

MFA(다중 요소 인증) 삭제 사용은 지원되지 않습니다.

> 버전 관리는 StorageGRID 버전 10.3 이상으로 생성된 버킷에서만 사용할 수 있습니다.

ILM 및 버전 관리

ILM 정책은 개체의 각 버전에 적용됩니다. ILM 스캔 프로세스는 모든 개체를 지속적으로 스캔하고 현재 ILM 정책에 대해 다시 평가합니다. ILM 정책에 대한 모든 변경 사항은 이전에 수집된 모든 개체에 적용됩니다. 여기에는 버전 관리가 활성화된 경우 이전에 수집된 버전이 포함됩니다. ILM 스캐닝은 이전에 수집된 개체에 새로운 ILM 변경 사항을 적용합니다.

버전 관리가 활성화된 버킷의 S3 오브젝트에서 버전 관리를 지원하므로 비현재 시간을 참조 시간으로 사용하는 ILM 규칙을 생성할 수 있습니다. 개체가 업데이트되면 이전 버전은 업데이트되지 않습니다. 비현재 시간 필터를 사용하면 이전 버전의 오브젝트에 대한 스토리지 영향을 줄이는 정책을 생성할 수 있습니다.

> 다중 파트 업로드 작업을 사용하여 새 버전의 개체를 업로드할 때 개체의 원래 버전에 대한 비현재 시간은 다중 파트 업로드가 완료될 때가 아닌 새 버전에 대해 다중 파트 업로드가 생성된 시점을 반영합니다. 제한된 경우 원래 버전의 비현재 시간이 현재 버전의 시간보다 몇 시간 또는 며칠 빨라질 수 있습니다.

S3 버전 오브젝트에 대한 ILM 정책 예제를 보려면 정보 수명 주기 관리로 오브젝트를 관리하는 지침을 참조하십시오.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

S3 REST API 구현을 위한 권장 사항

StorageGRID와 함께 사용할 S3 REST API를 구현할 때는 다음 권장 사항을 따라야 합니다.

존재하지 않는 객체에 대한 헤드 권장 사항

응용 프로그램에서 개체가 실제로 존재하지 않을 것으로 예상되는 경로에 개체가 있는지 정기적으로 확인하는 경우 ""사용 가능한"" 일관성 제어를 사용해야 합니다. 예를 들어, 응용 프로그램이 해당 위치에 배치되기 전에 위치를 지정할 경우 ""사용 가능"" 정합성 제어를 사용해야 합니다.

그렇지 않으면 헤드 작업에서 개체를 찾지 못할 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다.

PUT Bucket 정합성 보장 요청을 사용하여 각 버킷에 대해 ""사용 가능" 정합성 제어를 설정하거나 개별 API 작업에 대한 요청 헤더에서 정합성 제어를 지정할 수 있습니다.

개체 키에 대한 권장 사항

StorageGRID 11.4 이상에서 생성된 버킷의 경우 성능 모범 사례에 맞게 오브젝트 키 이름을 제한하는 것은 더 이상 필요하지 않습니다. 예를 들어, 이제 개체 키 이름의 처음 4개 문자에 임의의 값을 사용할 수 있습니다.

StorageGRID 11.4 이전 릴리스에서 생성된 버킷의 경우 객체 키 이름에 대한 다음 권장 사항을 계속 따르십시오.

- 개체 키의 처음 네 문자로 임의 값을 사용하면 안 됩니다. 이는 이전 AWS에서 권장하는 키 접두사와 다릅니다. 대신 와 같이 고유하지 않은 비무작위 접두사를 사용해야 합니다 `image`.
- 이전 AWS 권장 사항에 따라 키 접두사에 임의의 고유 문자를 사용하려면 객체 키에 디렉토리 이름을 접두사로 지정해야 합니다. 즉, 다음 형식을 사용합니다.

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  이 형식 대신:

  ```
  mybucket/f8e3-image3132.jpg
  ```

""범위 읽기" 권장 사항

저장된 오브젝트 압축 * 옵션을 선택한 경우(* 구성 * > * 그리드 옵션 *) S3 클라이언트 응용 프로그램은 바이트 범위를 지정하는 오브젝트 가져오기 작업을 수행하지 않아야 합니다. 이러한 ""범위 읽기"" 작업은 StorageGRID가 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 바이트 범위를 요청하는 Get Object 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축 개체에서 10MB 범위를 읽는 것은 매우 비효율적입니다.

압축된 개체에서 범위를 읽으면 클라이언트 요청이 시간 초과될 수 있습니다.

> ⓘ 개체를 압축해야 하고 클라이언트 응용 프로그램에서 범위 읽기를 사용해야 하는 경우 응용 프로그램의 읽기 시간 초과를 늘리십시오.

관련 정보

"일관성 제어"

"버킷 정합성 보장 요청을 배치합니다"

"StorageGRID 관리"

S3 REST API에서 지원되는 작업 및 제한 사항

StorageGRID 시스템은 대부분의 작업을 지원하고 몇 가지 제한 사항이 있는 간단한 스토리지 서비스 API(API 버전 2006-03-01)를 구현합니다. S3 REST API 클라이언트 애플리케이션을 통합할 때 구현 세부 정보를 이해해야 합니다.

StorageGRID 시스템은 가상 호스팅 방식의 요청과 경로 스타일 요청을 모두 지원합니다.

- "요청을 인증하는 중입니다"
- "서비스에 대한 작업"
- "버킷 작업"
- "버킷에 대한 사용자 지정 작업"
- "객체에 대한 작업"
- "멀티파트 업로드 작업"
- "오류 응답"

날짜 처리

S3 REST API의 StorageGRID 구현은 유효한 HTTP 날짜 형식만 지원합니다.

StorageGRID 시스템은 날짜 값을 허용하는 모든 헤더에 대해 유효한 HTTP 날짜 형식만 지원합니다. 날짜의 시간 부분은 그리니치 표준시(GMT) 형식 또는 표준 시간대 오프셋 없이 UTC(국제 표준시) 형식으로 지정할 수 있습니다(+0000을 지정해야 함). 을 포함하는 경우 `x-amz-date` 헤더 요청의 날짜 요청 헤더에 지정된 모든 값을 재정의합니다. AWS 서명 버전 4를 사용하는 경우 `x-amz-date` 날짜 헤더가 지원되지 않으므로 서명된 요청에 헤더가 있어야 합니다.

공통 요청 헤더

StorageGRID 시스템은 한 가지 예외를 제외하고 _Simple Storage Service API Reference_에 의해 정의된 공통 요청 헤더를 지원합니다.

요청 헤더	구축
권한 부여	AWS Signature 버전 2에 대한 전체 지원 다음 경우를 제외하고 AWS Signature 버전 4 지원: • 요청 본문에 대한 SHA256 값이 계산되지 않습니다. 사용자가 제출한 값은 마치 값이 있는 것처럼 유효성 검사 없이 승인됩니다 `UNSIGNED-PAYLOAD` 에 대한 정보가 제공되었습니다 `x-amz-content-sha256` 머리글.
X-amz-security-token	구현되지 않았습니다. 반환 `XNotImplemented`.

공통 응답 헤더

StorageGRID 시스템은 한 가지 예외를 제외하고 _Simple Storage Service API Reference_에 의해 정의된 모든 공통 응답 헤더를 지원합니다.

응답 헤더	구축
X-amz-id-2	사용 안 합니다

관련 정보

"AWS(Amazon Web Services) 문서: Amazon Simple Storage Service API Reference 를 참조하십시오"

요청을 인증하는 중입니다

StorageGRID 시스템은 S3 API를 사용하여 오브젝트에 대한 인증된 액세스와 익명 액세스를 모두 지원합니다.

S3 API는 S3 API 요청을 인증하는 데 서명 버전 2 및 서명 버전 4를 지원합니다.

인증된 요청은 액세스 키 ID 및 비밀 액세스 키를 사용하여 서명해야 합니다.

StorageGRID 시스템은 HTTP라는 두 가지 인증 방법을 지원합니다 `Authorization` 머리글 및 쿼리 매개 변수 사용

HTTP 인증 헤더를 사용합니다

HTTP `Authorization` 헤더는 버킷 정책에서 허용하는 익명 요청을 제외한 모든 S3 API 작업에서 사용됩니다. 를 클릭합니다 `Authorization` Header 요청을 인증하는 데 필요한 모든 서명 정보를 포함합니다.

쿼리 매개 변수 사용

쿼리 매개 변수를 사용하여 URL에 인증 정보를 추가할 수 있습니다. 이를 URL 사전 서명 이라고 하며, 이 URL을 사용하여 특정 리소스에 대한 임시 액세스 권한을 부여할 수 있습니다. 미리 지정된 URL을 가진 사용자는 리소스에 액세스하기 위해 비밀 액세스 키를 알 필요가 없습니다. 이 키를 사용하면 타사에 리소스에 대한 제한된 액세스를 제공할 수 있습니다.

서비스에 대한 작업

StorageGRID 시스템은 서비스에 대해 다음 작업을 지원합니다.

작동	구축
서비스 받기	모든 Amazon S3 REST API 동작으로 구현됩니다.
스토리지 사용량을 가져옵니다	Get Storage Usage 요청은 계정이 사용하는 총 스토리지 양과 계정과 연결된 각 버킷에 대해 알려줍니다. 이 작업은 /path 및 사용자 지정 쿼리 매개 변수가 있는 서비스에 대한 작업입니다 (`?x-ntap-sg-usage`)가 추가되었습니다.

작동	구축
옵션 /	클라이언트 응용 프로그램을 실행할 수 있습니다 `OPTIONS /` 스토리지 노드의 사용 가능 여부를 결정하기 위해 S3 인증 자격 증명을 제공하지 않고 스토리지 노드의 S3 포트에 대한 요청입니다. 이 요청을 사용하여 모니터링을 수행하거나, 외부 로드 밸런서가 스토리지 노드가 다운된 시점을 식별하도록 할 수 있습니다.

관련 정보

"스토리지 사용 요청 가져오기"

버킷 작업

StorageGRID 시스템은 각 S3 테넌트 계정에 대해 최대 1,000개의 버킷을 지원합니다.

버킷 이름 제한은 AWS US 표준 지역 제한을 따르지만, S3 가상 호스팅 스타일 요청을 지원하려면 이러한 제한을 DNS 명명 규칙으로 제한해야 합니다.

"AWS(Amazon Web Services) 문서: 버킷 제한 및 제한 사항"

"S3 요청에 대한 끝점 도메인 이름입니다"

버킷 가져오기(개체 나열) 및 버킷 버전 가져오기 작업은 StorageGRID 정합성 보장 제어를 지원합니다.

개별 버킷에 대해 마지막 액세스 시간에 대한 업데이트가 설정되었는지 여부를 확인할 수 있습니다.

다음 표에서는 StorageGRID에서 S3 REST API 버킷 작업을 구축하는 방법을 설명합니다. 이러한 작업을 수행하려면 계정에 필요한 액세스 자격 증명을 제공해야 합니다.

작동	구축
버킷 삭제	모든 Amazon S3 REST API 동작으로 구현됩니다.
버킷 CORS를 삭제합니다	이 작업은 버킷에 대한 CORS 구성을 삭제합니다.
Bucket 암호화를 삭제합니다	이 작업은 버킷에서 기본 암호화를 삭제합니다. 암호화된 기존 개체는 암호화된 상태로 유지되지만 버킷에 추가된 새 개체는 암호화되지 않습니다.
버킷 수명 주기를 삭제합니다	이 작업은 버킷에서 라이프사이클 구성을 삭제합니다.
버킷 정책을 삭제합니다	이 작업은 버킷에 연결된 정책을 삭제합니다.
버킷 복제를 삭제합니다	이 작업은 버킷에 연결된 복제 구성을 삭제합니다.
버킷 태그 지정을 삭제합니다	이 작업은 를 사용합니다 `tagging` 버킷에서 모든 태그를 제거하는 하위 리소스입니다.

작동	구축
버킷(목록 오브젝트), 버전 1 및 버전 2를 가져옵니다	이 작업은 버킷에 있는 오브젝트의 일부 또는 전체(최대 1,000개)를 반환합니다. 오브젝트를 에 인제스트한 경우에도 오브젝트에 대한 스토리지 클래스는 두 값 중 하나를 가질 수 있습니다 `REDUCED_REDUNDANCY` 스토리지 클래스 옵션: • `STANDARD`는 객체가 스토리지 노드로 구성된 스토리지 풀에 저장되었음을 나타냅니다. • `GLACIER`가 표시됩니다. 이는 해당 객체가 Cloud Storage Pool에 지정된 외부 버킷으로 이동되었음을 나타냅니다. 버킷에 동일한 접두사가 있는 삭제된 키의 많은 수가 포함된 경우 응답에 몇 가지 항목이 포함될 수 있습니다 `CommonPrefixes` 키가 없는 경우
버킷 ACL 가져오기	이 작업은 양수 응답 및 버킷 소유자의 ID, DisplayName 및 권한을 반환하며, 이는 소유자가 버킷에 대한 모든 액세스 권한을 가지고 있음을 나타냅니다.
버킷 CORS를 가져옵니다	이 작업은 를 반환합니다 `cors` 버킷에 대한 구성.
버킷 암호화 가져오기	이 작업은 버킷의 기본 암호화 구성을 반환합니다.
버킷 수명 주기 가져오기	이 작업은 버킷의 수명 주기 구성을 반환합니다.
버킷 위치를 가져옵니다	이 작업은 를 사용하여 설정된 영역을 반환합니다 `LocationConstraint` PUT 버킷 요청에 있는 요소입니다. 버킷 영역이 인 경우 `us-east-1`영역에 대해 빈 문자열이 반환됩니다.
버킷 알림을 받습니다	이 작업은 버킷에 연결된 알림 구성을 반환합니다.
버킷 객체 버전을 가져옵니다	버킷에 대한 읽기 액세스에서 이 작업은 를 통해 수행됩니다 `versions` 하위 리소스는 버킷에 있는 모든 버전의 오브젝트의 메타데이터를 나열합니다.
버킷 정책 가져오기	이 작업은 버킷에 연결된 정책을 반환합니다.
버킷 복제를 가져옵니다	이 작업은 버킷에 연결된 복제 구성을 반환합니다.
버킷 태그 지정을 가져옵니다	이 작업은 를 사용합니다 `tagging` 버킷에 대한 모든 태그를 반환하는 하위 리소스입니다.

작동	구축
버킷 버전 관리 가져오기	이 구현에서는 을 사용합니다 `versioning` 버킷의 버전 관리 상태를 반환하는 하위 리소스입니다. 반환된 버전 관리 상태는 버킷이 "비버전"인지 또는 버킷이 "사용" 또는 "일시 중단" 버전인지 여부를 나타냅니다.
개체 잠금 구성을 가져옵니다	이 작업은 버킷에 대해 S3 오브젝트 잠금이 설정되었는지 여부를 결정합니다. "S3 오브젝트 잠금 사용"
헤드 버킷	이 작업은 버킷이 있는지 그리고 버킷에 액세스할 권한이 있는지 여부를 결정합니다.

작동	구축
버킷 을 놓습니다	이 작업은 새 버킷을 생성합니다. 버킷을 만들면 버켓 소유자가 됩니다. • 버킷 이름은 다음 규칙을 준수해야 합니다. ◦ 각 StorageGRID 시스템에서 고유해야 합니다(테넌트 계정에서만 고유한 것은 아님). ◦ DNS를 준수해야 합니다. ◦ 3자 이상 63자 이하여야 합니다. ◦ 인접한 레이블이 마침표로 구분된 하나 이상의 레이블일 수 있습니다. 각 레이블은 소문자 또는 숫자로 시작하고 끝나야 하며 소문자, 숫자 및 하이픈만 사용할 수 있습니다. ◦ 텍스트 형식의 IP 주소처럼 보이지 않아야 합니다. ◦ 가상 호스팅 스타일 요청에서 기간을 사용하지 않아야 합니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다. • 기본적으로 버킷은 에서 생성됩니다 `us-east-1` 지역. 그러나 을 사용할 수 있습니다 `LocationConstraint` 다른 영역을 지정할 요청 본문의 요청 요소입니다. 를 사용할 때 `LocationConstraint` 요소, 그리드 관리자 또는 그리드 관리 API를 사용하여 정의된 영역의 정확한 이름을 지정해야 합니다. 사용할 지역 이름을 모르는 경우 시스템 관리자에게 문의하십시오. * 참고 *: PUT 버킷 요청이 StorageGRID에 정의되지 않은 지역을 사용하는 경우 오류가 발생합니다. • 을 포함할 수 있습니다 `x-amz-bucket-object-lock-enabled` S3 오브젝트 잠금이 활성화된 버킷을 생성하도록 헤더를 요청합니다. 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 버킷을 생성한 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다. S3 오브젝트 잠금에는 버킷 버전 관리가 필요하며, 이 버전은 버킷을 생성할 때 자동으로 활성화됩니다. "S3 오브젝트 잠금 사용"

작동	구축
버킷 CORS를 넣습니다	이 작업은 버킷이 오리진 간 요청을 처리할 수 있도록 버킷에 대한 CORS 구성을 설정합니다. CORS(Cross-origin Resource Sharing)는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, 이라는 S3 버킷을 사용한다고 가정합니다 `images` 그래픽을 저장합니다. 에 대한 CORS 구성을 설정합니다 `images` 버킷을 사용하면 버켓의 이미지를 웹 사이트에 표시할 수 있습니다 `http://www.example.com`.
Bucket 암호화를 적용합니다	이 작업은 기존 버킷의 기본 암호화 상태를 설정합니다. 버킷 수준 암호화가 활성화된 경우 버킷에 추가된 모든 새 오브젝트는 암호화됩니다. StorageGRID는 StorageGRID 관리 키로 서버 측 암호화를 지원합니다. 서버 측 암호화 구성 규칙을 지정할 때 를 설정합니다 `SSEAlgorithm` 매개 변수 대상 `AES256`, 및 은 사용하지 마십시오 `KMSMasterKeyID` 매개 변수. 객체 업로드 요청이 이미 암호화를 지정한 경우(즉, 요청에 가 포함된 경우) 버킷 기본 암호화 구성은 무시됩니다 `x-amz-server-side-encryption-*` 요청 헤더 참조).

작동	구축
버킷 수명 주기를 놓습니다	이 작업은 버킷에 대한 새 수명 주기 구성을 생성하거나 기존 수명 주기 구성을 대체합니다. StorageGRID는 수명 주기 구성에서 최대 1,000개의 수명 주기 규칙을 지원합니다. 각 규칙에는 다음 XML 요소가 포함될 수 있습니다. • 만료(일, 날짜) • NoncurrentVersionExpiration(NoncurrentDays) • 필터(접두사, 태그) • 상태 • ID입니다 StorageGRID는 다음 작업을 지원하지 않습니다. • AbortIncompleteMultipartUpload를 중단합니다 • ExpiredObjectDeleteMarker 를 참조하십시오 • 전환 버킷 수명 주기의 만료 작업이 ILM 배치 명령과 상호 작용하는 방법을 이해하려면 정보 수명 주기 관리를 통해 개체를 관리하기 위한 지침에서 ""ILM이 개체의 수명 내내 작동하는 방식""을 참조하십시오. • 참고 *: 버킷 수명 주기 구성은 S3 오브젝트 잠금이 활성화된 버킷과 함께 사용할 수 있지만 레거시 준수 버킷에서는 버킷 수명 주기 구성이 지원되지 않습니다.

작동	구축

버킷 통지를 보냅니다	이 작업은 요청 본문에 포함된 알림 구성 XML을 사용하여 버킷에 대한 알림을 구성합니다. 다음과 같은 구현 세부 사항에 유의해야 합니다.
	
	• StorageGRID는 SNS(Simple Notification Service) 항목을 대상으로 지원합니다. SQS(Simple Queue Service) 또는 Amazon Lambda 엔드포인트는 지원되지 않습니다.
	• 알림 대상은 StorageGRID 엔드포인트의 URN으로 지정해야 합니다. 테넌트 관리자 또는 테넌트 관리 API를 사용하여 엔드포인트를 생성할 수 있습니다.
	
	알림 설정을 성공적으로 하려면 끝점이 있어야 합니다. 끝점이 없는 경우, 를 클릭합니다 `400 Bad Request` 코드와 함께 오류가 반환됩니다 `InvalidArgument`.
	
	• 다음 이벤트 유형에 대한 알림을 구성할 수 없습니다. 이러한 이벤트 유형은 * 지원되지 않습니다 *.
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• StorageGRID에서 보낸 이벤트 알림은 다음 목록과 같이 일부 키를 포함하지 않고 다른 키에 대해 특정 값을 사용한다는 점을 제외하고 표준 JSON 형식을 사용합니다.
	• * eventSource * 를 선택합니다
	
	`sgws:s3`
	
	• * awsRegion *
	
	포함되지 않음
	
	• x-amz-id-2 *
	
	포함되지 않음
	
	• * 표시 *
	
	`urn:sgws:s3:::bucket_name`

버킷 정책을 적용합니다	이 작업은 버킷에 연결된 정책을 설정합니다.

작동	구축
버킷 복제를 배치합니다	이 작업은 요청 본문에 제공된 복제 구성 XML을 사용하여 버킷에 대한 StorageGRID CloudMirror 복제를 구성합니다. CloudMirror 복제의 경우 다음과 같은 구축 세부 정보를 알고 있어야 합니다. • 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. • 버킷 복제는 버전 관리되거나 버전이 지정되지 않은 버킷에서 구성할 수 있습니다. • 복제 구성 XML의 각 규칙에서 다른 대상 버킷을 지정할 수 있습니다. 소스 버킷은 둘 이상의 대상 버킷에 복제할 수 있습니다. • 대상 버킷은 테넌트 관리자 또는 테넌트 관리 API에 지정된 StorageGRID 엔드포인트의 URN으로 지정해야 합니다. 복제 구성이 성공하려면 엔드포인트가 있어야 합니다. 엔드포인트가 없으면 요청이 로 실패합니다 `400 Bad Request`. 오류 메시지는 다음과 같습니다. `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • 을 지정할 필요가 없습니다 `Role` 구성 XML에서. 이 값은 StorageGRID에서 사용되지 않으며 제출될 경우 무시됩니다. • 구성 XML에서 스토리지 클래스를 생략하면 StorageGRID에서 를 사용합니다 `STANDARD` 기본적으로 스토리지 클래스입니다. • 소스 버킷에서 객체를 삭제하거나 소스 버킷 자체를 삭제하는 경우 지역 간 복제 동작은 다음과 같습니다. ◦ 복제되기 전에 오브젝트 또는 버킷을 삭제하면 객체/버킷이 복제되지 않으므로 사용자에게 통보되지 않습니다. ◦ 복제된 후 오브젝트 또는 버킷을 삭제하면 StorageGRID는 지역 간 복제 V1에 대한 표준 Amazon S3 삭제 동작을 따릅니다.

작동	구축
Bucket 태그 달기	이 작업은 를 사용합니다 `tagging` 하위 리소스로서 버킷에 대한 태그 집합을 추가하거나 업데이트합니다. 버킷 태그를 추가할 때 다음과 같은 제한 사항을 숙지하십시오. • StorageGRID 및 Amazon S3 모두 각 버킷당 최대 50개의 태그를 지원합니다. • 버킷과 연결된 태그에는 고유한 태그 키가 있어야 합니다. 태그 키의 길이는 최대 128자의 유니코드 문자일 수 있습니다. • 태그 값의 길이는 최대 256자의 유니코드 문자일 수 있습니다. • 키와 값은 대/소문자를 구분합니다.
버킷 버전 관리	이 구현에서는 을 사용합니다 `versioning` 기존 버킷의 버전 관리 상태를 설정하는 하위 리소스입니다. 다음 값 중 하나를 사용하여 버전 관리 상태를 설정할 수 있습니다. • Enabled(사용): 버킷의 오브젝트에 대한 버전 관리를 활성화합니다. 버킷에 추가된 모든 오브젝트는 고유한 버전 ID를 받습니다. • Suspended(일시 중지됨): 버킷의 오브젝트에 대한 버전 관리를 비활성화합니다. 버킷에 추가된 모든 오브젝트는 버전 ID를 수신합니다 `null`.

관련 정보

"AWS(Amazon Web Services) 문서: 지역 간 복제"

"일관성 제어"

"버킷 최종 액세스 시간 요청 가져오기"

"버킷 및 그룹 액세스 정책"

"S3 오브젝트 잠금 사용"

"감사 로그에서 S3 작업을 추적했습니다"

"ILM을 사용하여 개체를 관리합니다"

"테넌트 계정을 사용합니다"

S3 라이프사이클 구성 생성

S3 라이프사이클 구성을 생성하여 StorageGRID 시스템에서 특정 오브젝트 삭제 시기를 제어할 수 있습니다.

이 섹션의 간단한 예는 S3 라이프사이클 구성에서 특정 S3 버킷에서 특정 객체가 삭제(만료)되는 시기를 제어하는

방법을 보여줍니다. 이 섹션의 예제는 설명을 위한 것입니다. S3 라이프사이클 구성 생성에 대한 자세한 내용은 _Amazon Simple Storage Service Developer Guide_에서 오브젝트 라이프사이클 관리에 대한 섹션을 참조하십시오. StorageGRID는 만료 작업만 지원하며 전환 작업은 지원하지 않습니다.

"Amazon Simple Storage Service 개발자 가이드: 개체 수명 주기 관리"

문서 수정 상태 설정은 무엇입니까

라이프사이클 구성은 특정 S3 버킷의 오브젝트에 적용되는 규칙 세트입니다. 각 규칙은 영향을 받는 개체와 해당 개체가 만료되는 시기(특정 날짜 또는 특정 일 수 이후)를 지정합니다.

StorageGRID는 수명 주기 구성에서 최대 1,000개의 수명 주기 규칙을 지원합니다. 각 규칙에는 다음 XML 요소가 포함될 수 있습니다.

- 만료: 지정된 날짜에 도달하거나 지정된 일 수에 도달할 때 개체를 인제스트할 때로부터 개체를 삭제합니다.
- NoncurrentVersionExpiration: 지정된 일 수에 도달할 때 개체가 비전류가 되었을 때부터 개체를 삭제합니다.
- 필터(접두사, 태그)
- 상태
- ID입니다

버킷에 라이프사이클 구성을 적용하는 경우 버킷의 라이프사이클 설정은 항상 StorageGRID ILM 설정을 재정의합니다. StorageGRID는 ILM이 아닌 버킷의 만료 설정을 사용하여 특정 개체의 삭제 또는 유지 여부를 결정합니다.

따라서 ILM 규칙의 배치 지침이 개체에 계속 적용되더라도 그리드에서 개체를 제거할 수 있습니다. 또는 개체에 대한 ILM 배치 지침이 만료된 후에도 개체가 그리드에 남아 있을 수 있습니다. 자세한 내용은 정보 수명 주기 관리를 통해 개체를 관리하는 지침에 있는 ""ILM이 개체의 수명 내내 작동하는 방법"을 참조하십시오.

> 버킷 수명 주기 구성은 S3 오브젝트 잠금이 활성화된 버킷과 함께 사용할 수 있지만 버킷 수명 주기 구성은 레거시 준수 버킷에서 지원되지 않습니다.

StorageGRID는 다음 버킷 작업을 사용하여 라이프사이클 구성을 관리합니다.

- 버킷 수명 주기를 삭제합니다
- 버킷 수명 주기 가져오기
- 버킷 수명 주기를 놓습니다

문서 수정 상태 설정 작성

라이프사이클 구성을 만드는 첫 번째 단계에서는 하나 이상의 규칙이 포함된 JSON 파일을 만듭니다. 예를 들어 이 JSON 파일에는 다음과 같은 세 가지 규칙이 포함되어 있습니다.

1. 규칙 1은 접두사와 일치하는 객체에만 적용됩니다 `category1/` 및 이(가) 있습니다 `key2` 의 값 `tag2`. 를 클릭합니다 `Expiration` 매개 변수는 필터와 일치하는 개체가 2020년 8월 22일 자정에 만료되도록 지정합니다.
2. 규칙 2는 접두사와 일치하는 객체에만 적용됩니다 `category2/`. 를 클릭합니다 `Expiration` 매개 변수는 필터와 일치하는 개체가 수집된 후 100일이 경과하도록 지정합니다.

일 수를 지정하는 규칙은 오브젝트가 수집된 시점을 기준으로 합니다. 현재 날짜가 수집 날짜와 일 수를 더한 값을 초과하면 라이프사이클 구성이 적용되는 즉시 일부 객체가 버킷에서 제거될 수 있습니다.

3. 규칙 3은 접두사와 일치하는 객체에만 적용됩니다 `category3/`. 를 클릭합니다 `Expiration` 매개 변수 일치하는 개체의 현재 버전이 아닌 버전이 최신 상태가 아닌 후 50일 후에 만료되도록 지정합니다.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

버킷에 라이프사이클 구성 적용

문서 수정 상태 구성 파일을 작성한 후 PUT Bucket 수명주기 요청을 실행하여 이를 버킷에 적용합니다.

이 요청은 예제 파일의 문서 수정 상태 구성을 이름이 인 버킷의 오브젝트에 적용합니다 `testbucket`버킷

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

라이프사이클 구성이 버킷에 성공적으로 적용되었는지 확인하려면 Get Bucket 수명주기 요청을 실행합니다. 예를 들면 다음과 같습니다.

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

성공적으로 응답하면 방금 적용한 문서 수정 상태 설정이 나열됩니다.

버킷 수명 주기 만료가 객체에 적용되는지 검증합니다

Put Object, Head Object 또는 Get Object 요청을 실행할 때 수명 주기 구성의 만료 규칙이 특정 개체에 적용되는지 확인할 수 있습니다. 규칙이 적용될 경우 응답에는 가 포함됩니다 `Expiration` 객체가 만료되는 시간과 일치하는 만료 규칙을 나타내는 매개 변수입니다.

> 버킷 라이프사이클이 ILM, 을 무시하기 때문입니다 `expiry-date` 객체가 삭제될 실제 날짜가 표시됩니다. 자세한 내용은 StorageGRID 관리 수행 지침에서 "개체 보존 결정 방법"을 참조하십시오.

예를 들어, 이 PUT 오브젝트 요청은 2020년 6월 22일에 발행되었으며 에 오브젝트를 두었습니다 `testbucket` 버킷.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

성공 응답은 개체가 100일(2020년 10월 1일) 내에 만료되고 라이프사이클 구성의 규칙 2와 일치함을 나타냅니다.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

예를 들어, 이 head Object 요청은 testbucket 버킷에서 동일한 객체에 대한 메타데이터를 가져오는 데 사용되었습니다.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

성공 응답에는 개체의 메타데이터가 포함되며 개체가 100일 후에 만료되고 규칙 2와 일치함을 나타냅니다.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

관련 정보

"버킷 작업"

"ILM을 사용하여 개체를 관리합니다"

버킷에 대한 사용자 지정 작업

StorageGRID 시스템은 S3 REST API에 추가되고 시스템에 고유한 맞춤형 버킷 작업을 지원합니다.

다음 표에는 StorageGRID에서 지원하는 사용자 지정 버킷 작업이 나열되어 있습니다.

작동	설명	를 참조하십시오
버킷 일관성 확보	특정 버킷에 적용되는 정합성 보장 레벨을 반환합니다.	"버킷 정합성 보장 요청 가져오기"
버킷 일관성을 유지합니다	특정 버킷에 적용되는 정합성 수준을 설정합니다.	"버킷 정합성 보장 요청을 배치합니다"
버킷 최종 액세스 시간 가져오기	특정 버킷에 대해 마지막 액세스 시간 업데이트를 사용할 수 있는지 여부를 반환합니다.	"버킷 최종 액세스 시간 요청 가져오기"
버킷 최종 접근 시간	특정 버킷에 대한 마지막 액세스 시간 업데이트를 활성화하거나 비활성화할 수 있습니다.	"버킷 최종 액세스 시간 요청"

작동	설명	를 참조하십시오
버킷 메타데이터 알림 구성을 삭제합니다	특정 버킷과 연결된 메타데이터 알림 구성 XML을 삭제합니다.	"버킷 메타데이터 알림 구성 요청을 삭제합니다"
Bucket 메타데이터 알림 구성 가져오기	특정 버킷과 연결된 메타데이터 알림 구성 XML을 반환합니다.	"버킷 메타데이터 알림 구성 요청을 가져옵니다"
Put Bucket 메타데이터 알림 구성	버킷에 대한 메타데이터 알림 서비스를 구성합니다.	"PUT 버킷 메타데이터 알림 구성 요청"
규정 준수를 위해 버킷 수정 작업을 수행합니다	더 이상 사용되지 않으며 지원되지 않음: Compliance를 사용하는 새 버킷을 더 이상 생성할 수 없습니다.	"사용되지 않음: 규정 준수를 위해 버킷 요청 수정을 배치합니다"
버킷 규정 준수	더 이상 사용되지 않지만 지원됨: 기존 레거시 준수 버킷에 대해 현재 적용되는 규정 준수 설정을 반환합니다.	"사용되지 않음: 버킷 준수 요청 가져오기"
버킷 규정 준수	사용되지 않지만 지원됨: 기존 레거시 준수 버킷의 준수 설정을 수정할 수 있습니다.	"폐기됨: 버킷 준수 요청을 넣으십시오"

관련 정보

"감사 로그에서 S3 작업을 추적했습니다"

객체에 대한 작업

이 섹션에서는 StorageGRID 시스템이 객체에 대해 S3 REST API 작업을 구축하는 방법에 대해 설명합니다.

- "S3 오브젝트 잠금 사용"
- "서버 측 암호화 사용"
- "객체 가져오기"
- "헤드 개체"
- "사후 개체 복원"
- "개체 를 넣습니다"
- "개체 - 복사 를 선택합니다"

다음 조건은 모든 개체 작업에 적용됩니다.

- StorageGRID 정합성 보장 제어는 다음을 제외하고 객체에 대한 모든 작업에서 지원됩니다.
  - 객체 ACL을 가져옵니다

    - OPTIONS /
    - 개체를 법적 증거 자료 보관
    - 개체 보존

- 같은 키에 쓰는 두 클라이언트 등 충돌하는 클라이언트 요청은 "최근 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.
- StorageGRID 버킷의 모든 오브젝트는 익명 사용자 또는 다른 계정에서 만든 오브젝트를 포함하여 버킷 소유자가 소유합니다.
- Swift를 통해 StorageGRID 시스템으로 수집된 데이터 오브젝트는 S3를 통해 액세스할 수 없습니다.

다음 표에서는 StorageGRID에서 S3 REST API 오브젝트 작업을 구현하는 방법을 설명합니다.

작동	구축
개체 삭제	MFA(Multi-Factor Authentication) 및 응답 헤더입니다 `x-amz-mfa` 지원되지 않습니다. 오브젝트 삭제 요청을 처리할 때 StorageGRID는 저장된 모든 위치에서 오브젝트의 모든 복사본을 즉시 제거하려고 시도합니다. 성공하면 StorageGRID는 즉시 클라이언트에 응답을 반환합니다. 위치를 일시적으로 사용할 수 없기 때문에 30초 이내에 모든 복사본을 제거할 수 없는 경우 StorageGRID는 제거할 복사본을 대기시킨 다음 클라이언트에 성공 여부를 표시합니다. • 버전 관리 * 특정 버전을 제거하려면 요청자가 버킷 소유자여야 하며 를 사용해야 합니다 `versionId` 하위 리소스. 이 하위 리소스를 사용하면 버전이 영구적으로 삭제됩니다. 를 누릅니다 `versionId` 삭제 마커인 응답 헤더에 해당합니다 `x-amz-delete-marker` 가 로 설정된 상태로 반환됩니다 `true`. • 를 사용하지 않고 개체를 삭제한 경우 `versionId` 버전 지원 버킷의 하위 리소스에서는 삭제 마커가 생성됩니다. 를 클릭합니다 `versionId` 삭제 마커는 를 사용하여 반환됩니다 `x-amz-version-id` 응답 헤더 및 `x-amz-delete-marker` 로 설정된 응답 헤더가 반환됩니다 `true`. • 를 사용하지 않고 개체를 삭제한 경우 `versionId` 버전 일시 중지된 버킷의 하위 리소스는 기존 'null' 버전 또는 'null' 삭제 표식을 영구적으로 삭제하고 새 'null' 삭제 표식을 생성합니다. 를 클릭합니다 `x-amz-delete-marker` 로 설정된 응답 헤더가 반환됩니다 `true`. • 참고 *: 경우에 따라 객체에 대해 여러 개의 삭제 마커가 존재할 수 있습니다.

작동	구축
여러 개체를 삭제합니다	MFA(Multi-Factor Authentication) 및 응답 헤더입니다 `x-amz-mfa` 지원되지 않습니다. 동일한 요청 메시지에서 여러 객체를 삭제할 수 있습니다.
개체 태그 지정 삭제	를 사용합니다 `tagging` 개체에서 모든 태그를 제거하는 하위 리소스입니다. 모든 Amazon S3 REST API 동작으로 구현됩니다. • 버전 관리 * 를 누릅니다 `versionId` 쿼리 매개 변수가 요청에 지정되지 않았습니다. 이 작업은 버전이 지정된 버킷에 있는 개체의 최신 버전에서 모든 태그를 삭제합니다. 개체의 현재 버전이 삭제 표식이면 " MethodNotAllowed " 상태가 과 함께 반환됩니다 `x-amz-delete-marker` 응답 헤더가 로 설정되었습니다 `true`.
객체 가져오기	"객체 가져오기"
객체 ACL을 가져옵니다	계정에 필요한 액세스 자격 증명이 제공된 경우 이 작업은 개체 소유자의 ID, DisplayName 및 사용 권한과 함께 긍정적인 응답을 반환합니다. 이는 소유자가 개체에 대한 모든 액세스 권한을 가지고 있음을 나타냅니다.
객체 법적 증거 자료 보관	"S3 오브젝트 잠금 사용"
개체 보존 가져오기	"S3 오브젝트 잠금 사용"
객체 태그 지정 가져오기	를 사용합니다 `tagging` 개체의 모든 태그를 반환하는 하위 리소스입니다. 모든 Amazon S3 REST API 동작으로 구현됩니다 • 버전 관리 * 를 누릅니다 `versionId` 쿼리 매개 변수가 요청에 지정되지 않았습니다. 이 작업은 버전 관리되는 버킷에서 가장 최신 버전의 개체에 있는 모든 태그를 반환합니다. 개체의 현재 버전이 삭제 표식이면 " MethodNotAllowed " 상태가 과 함께 반환됩니다 `x-amz-delete-marker` 응답 헤더가 로 설정되었습니다 `true`.
헤드 개체	"헤드 개체"
사후 개체 복원	"사후 개체 복원"

작동	구축
개체 를 넣습니다	"개체 를 넣습니다"
개체 - 복사 를 선택합니다	"개체 - 복사 를 선택합니다"
개체를 법적 증거 자료 보관	"S3 오브젝트 잠금 사용"
개체 보존	"S3 오브젝트 잠금 사용"
개체 태그 지정	를 사용합니다 `tagging` 기존 개체에 태그 집합을 추가하는 하위 리소스입니다. 모든 Amazon S3 REST API 동작으로 구현됩니다 • 태그 업데이트 및 수집 동작 * 오브젝트 태그 지정을 사용하여 개체의 태그를 업데이트하는 경우 StorageGRID에서는 개체를 다시 수집하지 않습니다. 즉, 일치하는 ILM 규칙에 지정된 Ingest 동작 옵션이 사용되지 않습니다. ILM이 정상적인 백그라운드 ILM 프로세스에 의해 다시 평가될 때 업데이트로 인해 트리거되는 개체 배치에 대한 모든 변경 사항이 발생합니다. 즉, ILM 규칙이 수집 동작에 Strict 옵션을 사용하는 경우 필요한 개체 배치를 만들 수 없는 경우(예: 새로 필요한 위치를 사용할 수 없음) 작업이 수행되지 않습니다. 업데이트된 오브젝트는 필요한 배치가 가능할 때까지 현재 위치를 유지합니다. • 충돌 해결 * 같은 키에 쓰는 두 클라이언트 등 충돌하는 클라이언트 요청은 "최근 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다. • 버전 관리 * 를 누릅니다 `versionId` 쿼리 매개 변수가 요청에 지정되지 않았습니다. 작업에서 버전 관리되는 버킷의 가장 최근 개체 버전에 태그를 추가합니다. 개체의 현재 버전이 삭제 표식이면 " MethodNotAllowed " 상태가 과 함께 반환됩니다 `x-amz-delete-marker` 응답 헤더가 로 설정되었습니다 `true`.

관련 정보

"일관성 제어"

"감사 로그에서 S3 작업을 추적했습니다"

S3 오브젝트 잠금 사용

StorageGRID 시스템에서 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 오브젝트 잠금이 설정된 버킷을 생성한 다음 해당 버켓에 추가하는 각 오브젝트 버전에 대한 보관 기한 및 법적 보류 설정을 지정할 수 있습니다.

S3 오브젝트 잠금을 사용하면 고정된 시간 또는 무기한으로 오브젝트를 삭제 또는 덮어쓰는 것을 방지하기 위해 오브젝트 레벨 설정을 지정할 수 있습니다.

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3 규정 준수 모드에 상응하는 단일 보존 모드를 제공합니다. 기본적으로 보호된 개체 버전은 사용자가 덮어쓰거나 삭제할 수 없습니다. StorageGRID S3 오브젝트 잠금 기능은 거버넌스 모드를 지원하지 않으며, 특별한 권한이 있는 사용자가 보존 설정을 무시하거나 보호된 오브젝트를 삭제할 수 없습니다.

버킷에 대해 S3 오브젝트 잠금 설정

StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 각 버킷을 생성할 때 선택적으로 S3 오브젝트 잠금을 활성화할 수 있습니다. 다음 방법 중 하나를 사용할 수 있습니다.

- 테넌트 관리자를 사용하여 버킷을 생성합니다.

  "테넌트 계정을 사용합니다"

- 과 함께 PUT 버킷 요청을 사용하여 버킷을 작성합니다 `x-amz-bucket-object-lock_enabled` 요청 헤더.

  "버킷 작업"

버킷이 생성된 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다. S3 오브젝트 잠금에는 버킷 버전 관리가 필요하며, 이 버전은 버킷을 생성할 때 자동으로 활성화됩니다.

S3 오브젝트 잠금이 활성화된 버킷에는 S3 오브젝트 잠금 설정이 있는 오브젝트와 없는 오브젝트의 조합이 포함될 수 있습니다. StorageGRID는 S3 오브젝트 잠금 버킷의 오브젝트에 대한 기본 보존을 지원하지 않으므로 오브젝트 잠금 구성 버킷 작업은 지원되지 않습니다.

버킷에 대해 S3 오브젝트 잠금이 설정되었는지 확인

S3 오브젝트 잠금이 활성화되었는지 확인하려면 오브젝트 잠금 구성 가져오기 요청을 사용하십시오.

"버킷 작업"

S3 오브젝트 잠금 설정으로 오브젝트 생성

S3 오브젝트 잠금이 활성화된 버킷에 오브젝트 버전을 추가할 때 S3 오브젝트 잠금 설정을 지정하려면 오브젝트 넣기, 오브젝트 복사 넣기 또는 다중 파트 업로드 요청을 시작합니다. 다음 요청 헤더를 사용하십시오.

> 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 버킷을 생성한 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다.

- `x-amz-object-lock-mode`, 규정 준수(대소문자 구분)여야 합니다.

를 지정할 경우 `x-amz-object-lock-mode`, 또한 을 지정해야 합니다 `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - 보존 기간 값은 형식이어야 합니다 `2020-08-10T21:46:00Z`. 소수 자릿수는 허용되지만 소수점 이하 자릿수는 3자리만 유지됩니다(밀리초 단위). 다른 ISO 8601 형식은 허용되지 않습니다.
  - 보존 종료 날짜는 미래여야 합니다.
- `x-amz-object-lock-legal-hold`

  법적 증거 자료 보관(대소문자 구분)이 켜져 있는 경우, 해당 물체는 법적 증거 자료 보관 하에 배치됩니다. 법적 증거 자료 보관 기능이 꺼져 있는 경우 법적 증거 자료 보관 작업이 없습니다. 다른 값을 사용하면 400개의 잘못된 요청(InvalidArgument) 오류가 발생합니다.

이러한 요청 헤더를 사용하는 경우 다음과 같은 제한 사항에 유의하십시오.

- 를 클릭합니다 `Content-MD5` 요청 헤더가 필요한 경우 `x-amz-object-lock-*` 요청 헤더가 Put Object 요청에 있습니다. `Content-MD5` Put Object(개체 저장) - Copy(복사) 또는 Initiate MultiPart Upload(다중 파트 업로드)에는 필요하지 않습니다.
- 버킷에 S3 오브젝트 잠금이 설정되어 있지 않은 경우 및 가 활성화되어 있어야 합니다 `x-amz-object-lock-*` 요청 헤더가 있으면 400개의 잘못된 요청(InvalidRequest) 오류가 반환됩니다.
- Put Object 요청은 의 사용을 지원합니다 `x-amz-storage-class: REDUCED_REDUNDANCY` AWS 동작과 일치시킵니다. 하지만 오브젝트가 S3 오브젝트 잠금이 설정된 버킷으로 수집되면 StorageGRID는 항상 이중 커밋 수집을 수행합니다.
- 후속 Get 또는 Head Object 버전 응답에는 헤더가 포함됩니다 `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, 및 `x-amz-object-lock-legal-hold`, 구성된 경우 및 요청 보낸 사람이 올바른 경우 `s3:Get*` 권한.
- 이후 개체 버전 삭제 또는 개체 버전 삭제 요청은 보존 기한 이전이거나 법적 보류가 켜져 있는 경우 실패합니다.

S3 오브젝트 잠금 설정을 업데이트하는 중입니다

기존 개체 버전에 대한 법적 증거 자료 보관 또는 보존 설정을 업데이트해야 하는 경우 다음 개체 하위 리소스 작업을 수행할 수 있습니다.

- `PUT Object legal-hold`

  새 법적 증거 자료 보관 값이 켜져 있으면 해당 개체는 법적 증거 자료 보관 아래에 배치됩니다. 법적 증거 자료 보관 가치가 없는 경우 법적 구속이 해제됩니다.

- `PUT Object retention`
  - 모드 값은 규정 준수(대/소문자 구분)여야 합니다.
  - 보존 기간 값은 형식이어야 합니다 `2020-08-10T21:46:00Z`. 소수 자릿수는 허용되지만 소수점 이하 자릿수는 3자리만 유지됩니다(밀리초 단위). 다른 ISO 8601 형식은 허용되지 않습니다.
  - 개체 버전에 기존 보존 기한이 있는 경우 개체 버전을 늘릴 수만 있습니다. 새 값은 미래여야 합니다.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"테넌트 계정을 사용합니다"

"개체 를 넣습니다"

"개체 - 복사 를 선택합니다"

"멀티파트 업로드를 시작합니다"

"오브젝트 버전 관리"

"Amazon Simple Storage Service 사용자 가이드: S3 Object Lock 사용"

서버 측 암호화 사용

서버측 암호화를 통해 유휴 개체 데이터를 보호할 수 있습니다. StorageGRID는 개체를 쓸 때 데이터를 암호화하고 개체에 액세스할 때 데이터를 해독합니다.

서버측 암호화를 사용하려면 암호화 키가 관리되는 방식에 따라 상호 배타적인 두 가지 옵션 중 하나를 선택할 수 있습니다.

- * SSE(StorageGRID 관리 키를 사용한 서버 측 암호화) *: S3 요청을 발행하여 오브젝트를 저장할 때 StorageGRID는 고유 키를 사용하여 오브젝트를 암호화합니다. S3 요청을 통해 오브젝트를 검색할 때 StorageGRID는 저장된 키를 사용하여 오브젝트를 해독합니다.
- * SSE-C(고객이 제공한 키를 사용한 서버측 암호화) *: S3 요청을 발행하여 오브젝트를 저장할 때 사용자는 자신만의 암호화 키를 제공합니다. 오브젝트를 검색할 때 요청의 일부로 동일한 암호화 키를 제공합니다. 두 암호화 키가 일치하면 해당 개체는 해독되고 개체 데이터는 반환됩니다.

  StorageGRID는 모든 개체 암호화 및 암호 해독 작업을 관리하지만 사용자가 제공하는 암호화 키를 관리해야 합니다.

  > 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다.

  > 개체가 SSE 또는 SSE-C로 암호화된 경우 버킷 수준 또는 그리드 수준 암호화 설정은 무시됩니다.

SSE 사용

StorageGRID에서 관리하는 고유 키를 사용하여 개체를 암호화하려면 다음 요청 헤더를 사용합니다.

```
x-amz-server-side-encryption
```

SSE 요청 헤더는 다음 오브젝트 작업에서 지원됩니다.

- 개체 를 넣습니다
- 개체 - 복사 를 선택합니다
- 멀티파트 업로드를 시작합니다

SSE-C 사용

관리하는 고유 키로 개체를 암호화하려면 다음 세 가지 요청 헤더를 사용합니다.

요청 헤더	설명
`x-amz-server-side-encryption-customer-algorithm`	암호화 알고리즘을 지정합니다. 헤더 값은 이어야 합니다 `AES256`.
`x-amz-server-side-encryption-customer-key`	개체를 암호화하거나 해독하는 데 사용할 암호화 키를 지정합니다. 키의 값은 256비트 base64로 인코딩되어야 합니다.
`x-amz-server-side-encryption-customer-key-MD5`	RFC 1321에 따라 암호화 키의 MD5 다이제스트를 지정합니다. RFC 1321은 암호화 키가 오류 없이 전송되도록 하는 데 사용됩니다. MD5 다이제스트 값은 base64로 인코딩된 128비트여야 합니다.

SSE-C 요청 헤더는 다음 개체 작업에서 지원됩니다.

- 객체 가져오기
- 헤드 개체
- 개체 를 넣습니다
- 개체 - 복사 를 선택합니다
- 멀티파트 업로드를 시작합니다
- 부품 업로드
- 업로드 부품 - 복사

고객이 제공한 키**(SSE-C)**와 함께 서버측 암호화 사용 시 고려 사항

SSE-C를 사용하기 전에 다음 사항을 고려하십시오.

- https를 사용해야 합니다.

> StorageGRID는 SSE-C를 사용할 때 http를 통해 이루어진 요청을 거부합니다 보안을 위해 실수로 http를 사용하여 보낸 모든 키가 손상되지 않도록 고려해야 합니다. 키를 폐기하고 필요에 따라 회전합니다.

- 응답의 ETag는 객체 데이터의 MD5가 아닙니다.
- 암호화 키를 개체에 매핑하는 작업을 관리해야 합니다. StorageGRID는 암호화 키를 저장하지 않습니다. 각 개체에 대해 제공하는 암호화 키를 추적할 책임은 사용자에게 있습니다.
- 버킷을 버전 관리가 활성화된 경우 각 오브젝트 버전에는 고유한 암호화 키가 있어야 합니다. 각 개체 버전에 사용되는 암호화 키를 추적할 책임은 사용자에게 있습니다.
- 클라이언트 측에서 암호화 키를 관리하기 때문에 클라이언트 측에서 키 회전과 같은 추가 보호 수단을 관리해야 합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다.

- CloudMirror 복제가 버킷에 대해 구성된 경우 SSE-C 객체를 수집할 수 없습니다. 수집 작업이 실패합니다.

관련 정보

"객체 가져오기"

"헤드 개체"

"개체 를 넣습니다"

"개체 - 복사 를 선택합니다"

"멀티파트 업로드를 시작합니다"

"부품 업로드"

"업로드 부품 - 복사"

"Amazon S3 개발자 가이드: 고객 제공 암호화 키(SSE-C)를 사용하여 서버측 암호화를 사용하여 데이터 보호"

객체 가져오기

S3 오브젝트 가져오기 요청을 사용하여 S3 버킷에서 오브젝트를 검색할 수 있습니다.

PARTNUMBER 요청 매개 변수는 지원되지 않습니다

를 클릭합니다 `partNumber` 객체 가져오기 요청에 대해 요청 매개 변수가 지원되지 않습니다. 다중 파트 개체의 특정 부분을 검색하기 위한 가져오기 요청을 수행할 수 없습니다. 다음 메시지와 함께 501 미구현 오류가 반환됩니다.

```
GET Object by partNumber is not implemented
```

고객이 제공한 암호화 키**(SSE-C)**를 사용하여 서버측 암호화를 위한 요청 헤더

사용자가 제공한 고유 키로 개체를 암호화한 경우 머리글 3개를 모두 사용합니다.

- `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
- `x-amz-server-side-encryption-customer-key`: 오브젝트의 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 오브젝트의 암호화 키에 대한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

사용자 메타데이터의 **UTF-8** 문자

StorageGRID는 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자가 있는 개체에 대한 요청을 가져오면 가 반환되지 않습니다 `x-amz-missing-meta` 머리글 키 이름이나 값에 인쇄할 수 없는 문자가 포함된 경우.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 반환됩니다 `XNotImplemented`:

- `x-amz-website-redirect-location`

버전 관리

가 있는 경우 `versionId` 하위 리소스가 지정되지 않았습니다. 작업이 버전 관리되는 버킷에서 개체의 최신 버전을 가져옵니다. 객체의 현재 버전이 삭제 마커인 경우 와 함께 ""찾을 수 없음" 상태가 반환됩니다 `x-amz-delete-marker` 응답 헤더가 로 설정되었습니다 `true`.

Get Object for Cloud Storage Pool 개체의 동작

개체가 클라우드 스토리지 풀에 저장된 경우(정보 수명 주기 관리를 통해 개체 관리 지침 참조) 오브젝트 가져오기 요청의 동작은 개체의 상태에 따라 달라집니다. 자세한 내용은 " 헤드 개체 "를 참조하십시오.

> 객체가 클라우드 스토리지 풀에 저장되고 오브젝트 복사본이 하나 이상 그리드에 존재하는 경우, 객체 가져오기 요청은 클라우드 스토리지 풀에서 데이터를 검색하기 전에 그리드에서 데이터를 검색하려고 시도합니다.

개체의 상태입니다	**Get Object**의 동작입니다
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	`200 OK` 개체의 복사본이 검색됩니다.
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	`200 OK` 개체의 복사본이 검색됩니다.
개체가 검색할 수 없는 상태로 전환되었습니다	`403 Forbidden, InvalidObjectState` 개체를 검색 가능한 상태로 복원하려면 POST 개체 복원 요청을 사용합니다.
복구할 수 없는 상태에서 복원 중인 개체입니다	`403 Forbidden, InvalidObjectState` POST 개체 복원 요청이 완료될 때까지 기다립니다.
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	`200 OK` 개체의 복사본이 검색됩니다.

클라우드 스토리지 풀에서 다중 또는 분할 오브젝트

여러 부분 개체를 업로드했거나 StorageGRID가 큰 개체를 세그먼트로 분할한 경우 StorageGRID는 개체의 부분 또는 세그먼트의 하위 집합을 샘플링하여 클라우드 저장소 풀에서 개체를 사용할 수 있는지 여부를 결정합니다. 경우에 따라 Get Object 요청이 잘못 반환될 수 있습니다 `200 OK` 개체의 일부 부분이 이미 복구할 수 없는 상태로 전환되었거나 개체의 일부 부분이 아직 복원되지 않은 경우

다음과 같은 경우:

- Get Object 요청이 일부 데이터를 반환하지만 전송 도중에 중지될 수 있습니다.
- 후속 Get Object 요청이 반환될 수 있습니다 `403 Forbidden`.

관련 정보

"서버 측 암호화 사용"

"ILM을 사용하여 개체를 관리합니다"

"사후 개체 복원"

"감사 로그에서 S3 작업을 추적했습니다"

헤드 개체

S3 헤드 오브젝트 요청을 사용하여 오브젝트 자체를 반환하지 않고 오브젝트에서 메타데이터를 검색할 수 있습니다. 객체가 클라우드 스토리지 풀에 저장된 경우 헤드 객체를 사용하여 객체의 전환 상태를 확인할 수 있습니다.

고객이 제공한 암호화 키**(SSE-C)**를 사용하여 서버측 암호화를 위한 요청 헤더

사용자가 제공한 고유 키로 개체를 암호화한 경우 이 헤더 3개를 모두 사용합니다.

- `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
- `x-amz-server-side-encryption-customer-key`: 오브젝트의 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 오브젝트의 암호화 키에 대한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

사용자 메타데이터의 **UTF-8** 문자

StorageGRID는 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자가 있는 개체에 대한 head 요청은 을 반환하지 않습니다 `x-amz-missing-meta` 머리글 키 이름이나 값에 인쇄할 수 없는 문자가 포함된 경우.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 반환됩니다 `XNotImplemented`:

- `x-amz-website-redirect-location`

클라우드 스토리지 풀 객체에 대한 응답 헤더입니다

객체가 클라우드 스토리지 풀에 저장된 경우(정보 수명 주기 관리를 통해 객체 관리 지침 참조) 다음 응답 헤더가 반환됩니다.

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

응답 헤더는 클라우드 스토리지 풀로 이동되는 오브젝트의 상태에 대한 정보를 제공하며, 선택적으로 검색할 수 없는 상태로 전환된 후 복구됩니다.

개체의 상태입니다	헤드 객체에 대한 응답
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	`200 OK` (특별한 응답 헤더가 반환되지 않습니다.)

Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	개체가 검색할 수 없는 상태로 전환될 때까지 의 값은 입니다 `expiry-date` 앞으로 어느 정도 먼 시간으로 설정됩니다. 정확한 전환 시간은 StorageGRID 시스템에 의해 제어되지 않습니다.

개체가 검색할 수 없는 상태로 전환되었지만 하나 이상의 복사본이 그리드에 있습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	의 값 `expiry-date` 앞으로 어느 정도 먼 시간으로 설정됩니다.
	
	• 참고 *: 그리드의 복사본을 사용할 수 없는 경우(예: 스토리지 노드가 다운된 경우), 객체를 성공적으로 검색하기 전에 POST 객체 복원 요청을 발행하여 클라우드 스토리지 풀에서 복제본을 복원해야 합니다.

개체가 검색할 수 없는 상태로 전환되었으며 그리드에 복사본이 없습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`

개체의 상태입니다	헤드 객체에 대한 응답

복구할 수 없는 상태에서 복원 중인 개체입니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	를 클릭합니다 `expiry-date` 클라우드 스토리지 풀의 객체가 검색 불가능한 상태로 반환되는 시점을 나타냅니다.

클라우드 스토리지 풀에서 다중 또는 분할 오브젝트

여러 부분 개체를 업로드했거나 StorageGRID가 큰 개체를 세그먼트로 분할한 경우 StorageGRID는 개체의 부분 또는 세그먼트의 하위 집합을 샘플링하여 클라우드 저장소 풀에서 개체를 사용할 수 있는지 여부를 결정합니다. 경우에 따라 헤드 객체 요청이 잘못 반환될 수 있습니다 `x-amz-restore: ongoing-request="false"` 개체의 일부 부분이 이미 복구할 수 없는 상태로 전환되었거나 개체의 일부 부분이 아직 복원되지 않은 경우

버전 관리

가 있는 경우 `versionId` 하위 리소스가 지정되지 않았습니다. 작업이 버전 관리되는 버킷에서 개체의 최신 버전을 가져옵니다. 객체의 현재 버전이 삭제 마커인 경우 와 함께 ""찾을 수 없음" 상태가 반환됩니다 `x-amz-delete-marker` 응답 헤더가 로 설정되었습니다 `true`.

관련 정보

"서버 측 암호화 사용"

"ILM을 사용하여 개체를 관리합니다"

"사후 개체 복원"

"감사 로그에서 S3 작업을 추적했습니다"

사후 개체 복원

S3 POST 오브젝트 복원 요청을 사용하여 클라우드 스토리지 풀에 저장된 오브젝트를 복원할 수 있습니다.

지원되는 요청 유형입니다

StorageGRID는 개체 복원을 위한 POST 개체 복원 요청만 지원합니다. 는 지원하지 않습니다 `SELECT` 복원 유형.

반품 요청을 선택합니다 `XNotImplemented`.

버전 관리

필요에 따라 를 지정합니다 `versionId` 버전 관리되는 버킷에서 특정 버전의 오브젝트 복원 를 지정하지 않을 경우 `versionId`, 개체의 최신 버전이 복원됩니다

클라우드 스토리지 풀 객체에 대한 **POST** 객체 복구의 동작

개체가 클라우드 스토리지 풀에 저장된 경우(정보 수명 주기 관리를 통해 개체 관리 지침 참조) POST 개체 복원 요청은 개체의 상태에 따라 다음과 같은 동작을 수행합니다. 자세한 내용은 " 헤드 개체 "를 참조하십시오.

> 객체가 클라우드 스토리지 풀에 저장되어 있고 하나 이상의 오브젝트 복제본도 그리드에 있는 경우 POST 객체 복원 요청을 실행하여 객체를 복원할 필요가 없습니다. 대신 Get Object 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

개체의 상태입니다	**POST** 개체 복원 동작
StorageGRID로 수집되었지만 ILM에서 아직 평가되지 않은 오브젝트 또는 클라우드 스토리지 풀에 없는 오브젝트	`403 Forbidden`, `InvalidObjectState`
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	`200 OK` 변경 사항이 없습니다. • 참고 *: 개체가 검색할 수 없는 상태로 전환되기 전에는 해당 상태를 변경할 수 없습니다 `expiry-date`.
개체가 검색할 수 없는 상태로 전환되었습니다	`202 Accepted` 요청 본문에서 지정한 일 수에 대해 검색할 수 있는 객체 복제본을 클라우드 스토리지 풀에 복구합니다. 이 기간이 끝나면 객체는 복구할 수 없는 상태로 돌아갑니다. 필요에 따라 를 사용합니다 `Tier` 복원 작업을 완료하는 데 걸리는 시간을 결정하는 요청 요소입니다 (`Expedited`, `Standard`, 또는 `Bulk`)를 클릭합니다. 를 지정하지 않을 경우 `Tier`, `Standard` 계층이 사용됩니다. • 주의 *: 오브젝트가 S3 Glacier Deep Archive로 전환된 경우 또는 Cloud Storage Pool에서 Azure Blob Storage를 사용하는 경우 를 사용하여 복원할 수 없습니다 `Expedited` 계층. 다음 오류가 반환됩니다 `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.
복구할 수 없는 상태에서 복원 중인 개체입니다	`409 Conflict`, `RestoreAlreadyInProgress`

개체의 상태입니다	**POST** 개체 복원 동작
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	`200 OK` • 참고: * 개체가 검색 가능한 상태로 복원되면 이를 변경할 수 있습니다 `expiry-date` 에 대한 새 값을 사용하여 POST 개체 복원 요청을 다시 발행합니다 `Days`. 복원 날짜는 요청 시간을 기준으로 업데이트됩니다.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"헤드 개체"

"감사 로그에서 S3 작업을 추적했습니다"

개체 를 넣습니다

S3 PUT 오브젝트 요청을 사용하여 오브젝트를 버킷에 추가할 수 있습니다.

충돌 해결

같은 키에 쓰는 두 클라이언트 등 충돌하는 클라이언트 요청은 "최근 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

개체 크기

StorageGRID는 최대 5TB의 오브젝트를 지원합니다.

사용자 메타데이터 크기입니다

Amazon S3는 각 PUT 요청 헤더 내의 사용자 정의 메타데이터 크기를 2KB로 제한합니다. StorageGRID는 사용자 메타데이터를 24KiB로 제한합니다. 사용자 정의 메타데이터의 크기는 각 키와 값의 UTF-8 인코딩에서 바이트 수의 합계를 구하여 측정됩니다.

사용자 메타데이터의 **UTF-8** 문자

요청에 사용자 정의 메타데이터의 키 이름이나 값에 UTF-8 값이 포함되어 있으면 StorageGRID 동작이 정의되지 않습니다.

StorageGRID는 사용자 정의 메타데이터의 키 이름이나 값에 포함된 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 이스케이프된 UTF-8 문자는 ASCII 문자로 처리됩니다.

- 사용자 정의 메타데이터에 이스케이프된 UTF-8 문자가 포함된 경우 Put, Put Object-Copy, Get 및 head 요청이 성공합니다.
- StorageGRID는 을 반환하지 않습니다 `x-amz-missing-meta` 머리글 키 이름이나 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우.

개체 태그 제한

새 개체를 업로드할 때 태그를 추가하거나 기존 개체에 태그를 추가할 수 있습니다. StorageGRID 및 Amazon S3 모두 각 오브젝트에 대해 최대 10개의 태그를 지원합니다. 개체와 관련된 태그에는 고유한 태그 키가 있어야 합니다. 태그 키의 길이는 최대 128자의 유니코드 문자이고 태그 값의 길이는 최대 256자의 유니코드 문자일 수 있습니다. 키와 값은 대/소문자를 구분합니다.

개체 소유권

StorageGRID에서는 소유자가 아닌 계정 또는 익명 사용자가 만든 개체를 포함하여 모든 개체가 버킷 소유자 계정에 의해 소유됩니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  를 지정할 때 `aws-chunked` 용 `Content-Encoding`StorageGRID는 다음 항목을 확인하지 않습니다.

  - StorageGRID에서 를 확인하지 않습니다 `chunk-signature` 청크 데이터를 기준으로 합니다.
  - StorageGRID는 사용자가 제공하는 값을 확인하지 않습니다 `x-amz-decoded-content-length` 반대.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  청크된 전송 인코딩이 지원되는 경우 `aws-chunked` 페이로드 서명도 사용됩니다.

- `x-amz-meta-`사용자 정의 메타데이터를 포함하는 이름-값 쌍이 뒤에 옵니다.

  사용자 정의 메타데이터에 대한 이름 값 쌍을 지정할 때 다음 일반 형식을 사용합니다.

  ```
  x-amz-meta-<em>name</em>: <em>value</em>
  ```

  ILM 규칙의 참조 시간으로 * 사용자 정의 작성 시간 * 옵션을 사용하려면 을 사용해야 합니다 `creation-time` 오브젝트를 만들 때 기록하는 메타데이터의 이름입니다. 예를 들면 다음과 같습니다.

  ```
  x-amz-meta-creation-time: 1443399726
  ```

의 값 `creation-time` 1970년 1월 1일 이후 초 단위로 평가됩니다.

> ILM 규칙은 참조 시간에 * 사용자 정의 작성 시간 * 과 수집 동작에 대한 균형 또는 엄격 옵션을 모두 사용할 수 없습니다. ILM 규칙을 만들면 오류가 반환됩니다.

- `x-amz-tagging`
- S3 오브젝트 잠금 요청 헤더
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"S3 오브젝트 잠금 사용"

- SSE 요청 헤더:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

"S3 REST API에서 지원되는 작업 및 제한 사항"

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- 를 클릭합니다 `x-amz-acl` 요청 헤더가 지원되지 않습니다.
- 를 클릭합니다 `x-amz-website-redirect-location` 요청 헤더가 지원되지 않으며 반환됩니다 `XNotImplemented`.

스토리지 클래스 옵션

를 클릭합니다 `x-amz-storage-class` 요청 헤더가 지원됩니다. 에 대해 제출된 값입니다 `x-amz-storage-class` ILM을 통해 결정되는 StorageGRID 시스템에 저장된 개체의 영구 복사본 수가 아닌 수집 중에 StorageGRID이 오브젝트 데이터를 보호하는 방법에 영향을 미칩니다.

인제스트 개체와 일치하는 ILM 규칙이 Ingest 동작에 대해 Strict 옵션을 사용하는 경우, 를 참조하십시오 `x-amz-storage-class` 머리글은 효과가 없습니다.

에 사용할 수 있는 값은 다음과 같습니다 `x-amz-storage-class`:

- `STANDARD` (기본값)
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우, 개체가 수집되는 즉시 해당 개체의 두 번째 복사본이 생성되어 다른 스토리지 노드(이중 커밋)에 배포됩니다. ILM을 평가할 때 StorageGRID는 이러한 초기 중간 복사본이 규칙의 배치 지침을 충족하는지 여부를 결정합니다. 그렇지 않으면 새 오브젝트 복사본을 다른 위치에 만들어야 하고 초기 중간 복사본을 삭제해야 할 수 있습니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하고 StorageGRID이 규칙에 지정된 모든 복사본을 즉시 만들 수 없는

경우 StorageGRID은 다른 스토리지 노드에 두 개의 임시 복사본을 만듭니다.

StorageGRID에서 ILM 규칙(동기식 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있는 경우 를 참조하십시오 `x-amz-storage-class` 머리글은 효과가 없습니다.

- `REDUCED_REDUNDANCY`
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우 StorageGRID는 오브젝트가 수집될 때(단일 커밋) 단일 임시 복사본을 만듭니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하는 경우 StorageGRID은 시스템에서 규칙에 지정된 모든 사본을 즉시 만들 수 없는 경우에만 단일 중간 복사본을 만듭니다. StorageGRID에서 동기 배치를 수행할 수 있는 경우 이 머리글은 영향을 주지 않습니다. 를 클릭합니다 `REDUCED_REDUNDANCY` 옵션은 개체와 일치하는 ILM 규칙이 복제된 단일 복사본을 만들 때 가장 적합합니다. 이 경우 를 사용합니다 `REDUCED_REDUNDANCY` 모든 수집 작업에 대해 불필요한 오브젝트 복사본을 생성 및 삭제할 필요가 없습니다.

  를 사용합니다 `REDUCED_REDUNDANCY` 다른 상황에서는 옵션을 사용하지 않는 것이 좋습니다. `REDUCED_REDUNDANCY` 수집 중에 오브젝트 데이터가 손실될 위험이 증가합니다. 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.

- 주의 *: 한 번에 하나의 복제 사본만 있으면 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

지정 `REDUCED_REDUNDANCY` 오브젝트를 처음 인제스트할 때 생성되는 복사본 수에만 영향을 줍니다. 활성 ILM 정책에 따라 개체를 평가할 때 개체의 복사본 수에 영향을 주지 않으며 StorageGRID 시스템에서 낮은 수준의 중복성에 데이터가 저장되지 않습니다.

- 참고 *: S3 오브젝트 잠금이 활성화된 버킷으로 오브젝트를 인제스트하는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷으로 인스팅하는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션을 사용하면 오류가 반환됩니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

서버측 암호화에 대한 요청 헤더

다음 요청 헤더를 사용하여 서버측 암호화를 사용하여 개체를 암호화할 수 있습니다. SSE 및 SSE-C 옵션은 상호 배타적입니다.

- * SSE *: StorageGRID에서 관리하는 고유 키를 사용하여 오브젝트를 암호화하려면 다음 헤더를 사용하십시오.
  - `x-amz-server-side-encryption`
- * SSE-C *: 사용자가 제공 및 관리하는 고유 키로 객체를 암호화하려면 이 헤더 세 개를 모두 사용합니다.
  - `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
  - `x-amz-server-side-encryption-customer-key`새 오브젝트의 암호화 키를 지정합니다.
  - `x-amz-server-side-encryption-customer-key-MD5`: 새 개체의 암호화 키에 대한 MD5 다이제스트를 지정합니다.
- 주의: * 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.
- 참고 *: 오브젝트가 SSE 또는 SSE-C로 암호화된 경우 버킷 수준 또는 그리드 수준 암호화 설정은 무시됩니다.

버전 관리

버켓에 대해 버전 관리가 활성화된 경우 고유한 가 사용됩니다 `versionId` 는 저장 중인 개체의 버전에 대해 자동으로 생성됩니다. 여기 `versionId` 를 사용하여 응답에서도 반환됩니다 `x-amz-version-id` 응답 헤더.

버전 관리가 일시 중단된 경우 개체 버전은 null로 저장됩니다 `versionId` null 버전이 이미 있는 경우 덮어쓰기가 됩니다.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"버킷 작업"

"감사 로그에서 S3 작업을 추적했습니다"

"서버 측 암호화 사용"

"클라이언트 연결 구성 방법"

개체 - 복사 를 선택합니다

S3 PUT 오브젝트 복사 요청을 사용하여 S3에 이미 저장된 오브젝트 복사본을 생성할 수 있습니다. Put Object - Copy 작업은 GET 및 PUT를 수행하는 작업과 동일합니다.

충돌 해결

같은 키에 쓰는 두 클라이언트 등 충돌하는 클라이언트 요청은 "최근 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

개체 크기

StorageGRID는 최대 5TB의 오브젝트를 지원합니다.

사용자 메타데이터의 **UTF-8** 문자

요청에 사용자 정의 메타데이터의 키 이름이나 값에 UTF-8 값이 포함되어 있으면 StorageGRID 동작이 정의되지 않습니다.

StorageGRID는 사용자 정의 메타데이터의 키 이름이나 값에 포함된 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 이스케이프된 UTF-8 문자는 ASCII 문자로 처리됩니다.

- 사용자 정의 메타데이터에 이스케이프된 UTF-8 문자가 포함된 경우 요청이 성공합니다.
- StorageGRID는 을 반환하지 않습니다 `x-amz-missing-meta` 머리글 키 이름이나 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `Content-Type`

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`사용자 정의 메타데이터를 포함하는 이름-값 쌍이 뒤에 옵니다
- `x-amz-metadata-directive`기본값은 입니다 `COPY`, 개체 및 관련 메타데이터를 복사할 수 있습니다.

  지정할 수 있습니다 `REPLACE` 오브젝트를 복사할 때 기존 메타데이터를 덮어쓰거나 오브젝트 메타데이터를 업데이트합니다.

- `x-amz-storage-class`
- `x-amz-tagging-directive`기본값은 입니다 `COPY`, 개체 및 모든 태그를 복사할 수 있습니다.

  지정할 수 있습니다 `REPLACE` 개체를 복사할 때 기존 태그를 덮어쓰거나 태그를 업데이트합니다.

- S3 오브젝트 잠금 요청 헤더:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"S3 오브젝트 잠금 사용"

- SSE 요청 헤더:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

"서버측 암호화에 대한 요청 헤더"

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

스토리지 클래스 옵션

를 클릭합니다 `x-amz-storage-class` 요청 헤더가 지원되며 일치하는 ILM 규칙에서 이중 커밋 또는 균형 조정의 수집 동작을 지정하는 경우 StorageGRID에서 만드는 개체 복사본 수에 영향을 줍니다.

- `STANDARD`

  (기본값) ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 이중 커밋 수집 작업을 지정합니다.

- `REDUCED_REDUNDANCY`

  ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 단일 커밋 수집 작업을 지정합니다.

  > S3 오브젝트 잠금이 설정된 버킷으로 오브젝트를 밀어넣는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷으로 인스팅하는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션을 사용하면 오류가 반환됩니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

Put Object - Copy에서 **x-amz-copy-source** 사용

소스 버킷과 키가 에 지정된 경우 `x-amz-copy-source` 헤더 는 대상 버킷 및 키와 다르며 소스 오브젝트 데이터의 복제본이 대상에 기록됩니다.

소스 및 대상이 일치하면, 및 입니다 `x-amz-metadata-directive` 머리글은 로 지정됩니다 `REPLACE`오브젝트의 메타데이터는 요청에 제공된 메타데이터 값으로 업데이트됩니다. 이 경우 StorageGRID는 오브젝트를 다시 수집하지 않습니다. 여기에는 두 가지 중요한 결과가 있습니다.

- Put Object-Copy를 사용하여 기존 개체를 현재 위치에서 암호화하거나 기존 개체의 암호화를 변경할 수 없습니다. 를 공급하는 경우 `x-amz-server-side-encryption` 머리글 또는 을 선택합니다 `x-amz-server-side-encryption-customer-algorithm` header, StorageGRID가 요청을 거부하고 반환합니다 `XNotImplemented`.
- 일치하는 ILM 규칙에 지정된 Ingest 동작 옵션은 사용되지 않습니다. ILM이 정상적인 백그라운드 ILM 프로세스에 의해 다시 평가될 때 업데이트로 인해 트리거되는 개체 배치에 대한 모든 변경 사항이 발생합니다.

  즉, ILM 규칙이 수집 동작에 Strict 옵션을 사용하는 경우 필요한 개체 배치를 만들 수 없는 경우(예: 새로 필요한 위치를 사용할 수 없음) 작업이 수행되지 않습니다. 업데이트된 오브젝트는 필요한 배치가 가능할 때까지 현재 위치를 유지합니다.

서버측 암호화에 대한 요청 헤더

서버 측 암호화를 사용하는 경우 소스 개체가 암호화되었는지 여부 및 대상 개체를 암호화할 계획인지에 따라 요청 헤더가 제공됩니다.

- 소스 객체가 SSE-C(customer-provided key)를 사용하여 암호화된 경우, 객체를 해독한 다음 복사할 수 있도록 객체 복사 요청(Put Object-Copy request)에 다음 세 개의 헤더를 포함해야 합니다.
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` 를 지정합니다 `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key` 소스 객체를 만들 때 제공한 암호화 키를 지정합니다.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: 소스 개체를 만들 때 제공한 MD5 다이제스트를 지정합니다.
- 제공 및 관리하는 고유 키를 사용하여 대상 개체(복사본)를 암호화하려면 다음 세 개의 머리글을 포함합니다.
  - `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
  - `x-amz-server-side-encryption-customer-key`: 대상 오브젝트의 새 암호화 키를 지정합니다.
  - `x-amz-server-side-encryption-customer-key-MD5`: 새 암호화 키의 MD5 다이제스트를 지정합니다.
- 주의: * 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.
- SSE(StorageGRID)에서 관리되는 고유 키로 대상 객체(사본)를 암호화하려면 객체 복사 요청(Put Object-Copy request)에 이 헤더를 포함시킵니다.
  - `x-amz-server-side-encryption`
- 참고: * `server-side-encryption` 개체의 값을 업데이트할 수 없습니다. 대신 새 로 복사본을 만듭니다 `server-side-encryption` 값 사용 `x-amz-metadata-directive`: `REPLACE`.

버전 관리

소스 버킷의 버전이 있는 경우 를 사용할 수 있습니다 `x-amz-copy-source` Header - 개체의 최신 버전을 복사합니다. 특정 버전의 개체를 복사하려면 을 사용하여 복사할 버전을 명시적으로 지정해야 합니다 `versionId` 하위 리소스. 대상 버킷의 버전이 지정된 경우 생성된 버전이 에서 반환됩니다 `x-amz-version-id` 응답 헤더. 타겟 버킷에 대한 버전 관리가 일시 중지된 경우 `x-amz-version-id` ""null"" 값을 반환합니다.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"서버 측 암호화 사용"

"감사 로그에서 S3 작업을 추적했습니다"

"개체 를 넣습니다"

멀티파트 업로드 작업

이 섹션에서는 StorageGRID가 멀티파트 업로드 작업을 지원하는 방법에 대해 설명합니다.

- "여러 부분 업로드를 나열합니다"
- "멀티파트 업로드를 시작합니다"
- "부품 업로드"
- "업로드 부품 - 복사"

- "멀티파트 업로드를 완료합니다"

다음 조건 및 참고 사항은 모든 다중 파트 업로드 작업에 적용됩니다.

- 해당 버킷에 대한 다중 파트 업로드 나열 쿼리 결과는 불완전한 결과를 반환할 수 있으므로 단일 버킷에 대한 동시 다중 파트 업로드 1,000개를 초과할 수 없습니다.
- StorageGRID는 여러 파트에 대해 AWS 크기 제한을 적용합니다. S3 클라이언트는 다음 지침을 따라야 합니다.
  - 멀티파트 업로드의 각 파트는 5MiB(5,242,880바이트)와 5GiB(5,368,709,120바이트) 사이여야 합니다.
  - 마지막 부분은 5MiB(5,242,880바이트)보다 작을 수 있습니다.
  - 일반적으로 파트 크기는 가능한 한 커야합니다. 예를 들어, 100GiB 개체의 경우 5GiB의 파트 크기를 사용합니다. 각 파트는 고유한 개체로 간주되므로 큰 파트 크기를 사용하면 StorageGRID 메타데이터 오버헤드가 줄어듭니다.
  - 5GiB보다 작은 오브젝트의 경우 대신 비다중 파트 업로드를 사용하는 것이 좋습니다.
- ILM 규칙이 Strict 또는 Balanced 수집 동작을 사용하는 경우 ILM은 다중 파트 개체의 각 부분을 인제스트할 때 계산되고 다중 파트 업로드가 완료될 때 전체 개체에 대해 평가됩니다. 이 사항이 개체 및 파트 배치에 미치는 영향에 대해 알고 있어야 합니다.
  - S3 멀티파트 업로드가 진행 중인 동안 ILM이 변경되면 멀티파트 업로드가 완료될 때 개체의 일부 부분이 현재 ILM 요구 사항을 충족하지 못할 수 있습니다. 올바르게 배치되지 않은 모든 부품은 ILM 재평가를 위해 대기 중이며 나중에 올바른 위치로 이동됩니다.
  - 파트에 대한 ILM을 평가할 때 StorageGRID은 개체의 크기가 아닌 파트 크기를 필터링합니다. 즉, 개체의 일부를 개체의 ILM 요구 사항을 전체가 충족하지 않는 위치에 저장할 수 있습니다. 예를 들어, 규칙이 모든 오브젝트 10GB 이상이 DC1에 저장되는 반면 모든 작은 오브젝트는 DC2에 저장되는 것으로 지정하는 경우 10개 부분 멀티파트 업로드의 각 1GB 부분은 DC2에 저장됩니다. 개체에 대한 ILM을 전체적으로 평가할 때 개체의 모든 부분이 DC1로 이동합니다.
- 모든 멀티파트 업로드 작업은 StorageGRID 정합성 제어를 지원합니다.
- 필요한 경우 다중 파트 업로드와 함께 서버측 암호화를 사용할 수 있습니다. SSE(StorageGRID 관리 키 사용 시 서버 측 암호화)를 사용하려면 를 포함합니다 `x-amz-server-side-encryption` 다중 파트 업로드 시작 요청의 요청 헤더만 SSE-C(고객이 제공한 키와 함께 서버측 암호화)를 사용하려면 다중 파트 업로드 시작 요청 및 각 후속 업로드 파트 요청에서 동일한 세 가지 암호화 키 요청 헤더를 지정합니다.

작동	구축
다중 파트 업로드 나열	을 참조하십시오 "다중 파트 업로드 나열"
멀티파트 업로드를 시작합니다	을 참조하십시오 "멀티파트 업로드를 시작합니다"
부품 업로드	을 참조하십시오 "부품 업로드"
업로드 부품 - 복사	을 참조하십시오 "업로드 부품 - 복사"
멀티파트 업로드를 완료합니다	을 참조하십시오 "멀티파트 업로드를 완료합니다"
멀티파트 업로드를 중단합니다	모든 Amazon S3 REST API 동작으로 구현됩니다

작동	구축
파트 목록	모든 Amazon S3 REST API 동작으로 구현됩니다

관련 정보

"일관성 제어"

"서버 측 암호화 사용"

다중 파트 업로드 나열

다중 파트 업로드 나열 작업은 버킷에 대해 진행 중인 다중 파트 업로드를 나열합니다.

지원되는 요청 매개 변수는 다음과 같습니다.

- `encoding-type`
- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

를 클릭합니다 `delimiter` 요청 매개 변수가 지원되지 않습니다.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. 전체 다중 파트 업로드 작업이 수행되는 경우, 즉 개체가 작성되는 시점(해당되는 경우 버전)입니다.

멀티파트 업로드를 시작합니다

다중 파트 업로드 시작 작업은 개체에 대한 다중 파트 업로드를 시작하고 업로드 ID를 반환합니다.

를 클릭합니다 `x-amz-storage-class` 요청 헤더가 지원됩니다. 에 대해 제출된 값입니다 `x-amz-storage-class` ILM을 통해 결정되는 StorageGRID 시스템에 저장된 개체의 영구 복사본 수가 아닌 수집 중에 StorageGRID이 오브젝트 데이터를 보호하는 방법에 영향을 미칩니다.

인제스트 개체와 일치하는 ILM 규칙이 Ingest 동작에 대해 Strict 옵션을 사용하는 경우, 를 참조하십시오 `x-amz-storage-class` 머리글은 효과가 없습니다.

에 사용할 수 있는 값은 다음과 같습니다 `x-amz-storage-class`:

- `STANDARD` (기본값)
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우, 개체가 수집되는 즉시 해당 개체의 두 번째 복사본이 생성되어 다른 스토리지 노드(이중 커밋)에 배포됩니다. ILM을 평가할 때 StorageGRID는 이러한 초기 중간 복사본이 규칙의 배치 지침을 충족하는지 여부를 결정합니다. 그렇지 않으면 새 오브젝트 복사본을 다른 위치에 만들어야 하고 초기 중간 복사본을 삭제해야 할 수 있습니다.

◦ * 균형 *: ILM 규칙이 균형 옵션을 지정하고 StorageGRID이 규칙에 지정된 모든 복사본을 즉시 만들 수 없는 경우 StorageGRID은 다른 스토리지 노드에 두 개의 임시 복사본을 만듭니다.

StorageGRID에서 ILM 규칙(동기식 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있는 경우 를 참조하십시오 `x-amz-storage-class` 머리글은 효과가 없습니다.

- `REDUCED_REDUNDANCY`

◦ * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우 StorageGRID는 오브젝트가 수집될 때(단일 커밋) 단일 임시 복사본을 만듭니다.

◦ * 균형 *: ILM 규칙이 균형 옵션을 지정하는 경우 StorageGRID은 시스템에서 규칙에 지정된 모든 사본을 즉시 만들 수 없는 경우에만 단일 중간 복사본을 만듭니다. StorageGRID에서 동기 배치를 수행할 수 있는 경우 이 머리글은 영향을 주지 않습니다. 를 클릭합니다 `REDUCED_REDUNDANCY` 옵션은 개체와 일치하는 ILM 규칙이 복제된 단일 복사본을 만들 때 가장 적합합니다. 이 경우 를 사용합니다 `REDUCED_REDUNDANCY` 모든 수집 작업에 대해 불필요한 오브젝트 복사본을 생성 및 삭제할 필요가 없습니다.

를 사용합니다 `REDUCED_REDUNDANCY` 다른 상황에서는 옵션을 사용하지 않는 것이 좋습니다. `REDUCED_REDUNDANCY` 수집 중에 오브젝트 데이터가 손실될 위험이 증가합니다. 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.

- 주의 *: 한 번에 하나의 복제 사본만 있으면 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

지정 `REDUCED_REDUNDANCY` 오브젝트를 처음 인제스트할 때 생성되는 복사본 수에만 영향을 줍니다. 활성 ILM 정책에 따라 개체를 평가할 때 개체의 복사본 수에 영향을 주지 않으며 StorageGRID 시스템에서 낮은 수준의 중복성에 데이터가 저장되지 않습니다.

- 참고 *: S3 오브젝트 잠금이 활성화된 버킷으로 오브젝트를 인제스트하는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷으로 인스팅하는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션을 사용하면 오류가 반환됩니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

지원되는 요청 헤더는 다음과 같습니다.

- `Content-Type`
- `x-amz-meta-`사용자 정의 메타데이터를 포함하는 이름-값 쌍이 뒤에 옵니다

사용자 정의 메타데이터에 대한 이름 값 쌍을 지정할 때 다음 일반 형식을 사용합니다.

```
x-amz-meta-_name_: `value`
```

ILM 규칙의 참조 시간으로 * 사용자 정의 작성 시간 * 옵션을 사용하려면 을 사용해야 합니다 `creation-time` 오브젝트를 만들 때 기록하는 메타데이터의 이름입니다. 예를 들면 다음과 같습니다.

```
x-amz-meta-creation-time: 1443399726
```

의 값 `creation-time` 1970년 1월 1일 이후 초 단위로 평가됩니다.

추가 중 `creation-time` 레거시 규정 준수 기능이 설정된 버킷에 오브젝트를 추가할 경우 사용자 정의 메타데이터가 허용되지 않습니다. 오류가 반환됩니다.

- S3 오브젝트 잠금 요청 헤더:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"S3 오브젝트 잠금 사용"

- SSE 요청 헤더:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

"S3 REST API에서 지원되는 작업 및 제한 사항"

StorageGRID에서 UTF-8 문자를 처리하는 방법에 대한 자세한 내용은 Put Object 설명서를 참조하십시오.

서버측 암호화에 대한 요청 헤더

다음 요청 헤더를 사용하여 서버측 암호화를 사용하여 다중 파트 개체를 암호화할 수 있습니다. SSE 및 SSE-C 옵션은 상호 배타적입니다.

- * SSE *: StorageGRID에서 관리하는 고유 키로 객체를 암호화하려면 다중 파트 업로드 시작 요청에서 다음 헤더를 사용하십시오. 업로드 부품 요청에 이 헤더를 지정하지 마십시오.
  - `x-amz-server-side-encryption`
- * SSE-C *: 사용자가 제공 및 관리하는 고유 키를 사용하여 개체를 암호화하려는 경우 다중 파트 업로드 시작 요청(및 각 후속 업로드 파트 요청)에서 이 헤더 세 개를 모두 사용합니다.
  - `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
  - `x-amz-server-side-encryption-customer-key`새 오브젝트의 암호화 키를 지정합니다.
  - `x-amz-server-side-encryption-customer-key-MD5`: 새 개체의 암호화 키에 대한 MD5 다이제스트를 지정합니다.
- 주의: * 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 반환됩니다 `XNotImplemented`

- `x-amz-website-redirect-location`

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. MultiPart Upload 작업이 완료되면 개체가 만들어지고 버전이 적용됩니다(해당하는 경우).

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"서버 측 암호화 사용"

"개체 를 넣습니다"

부품 업로드

파트 업로드 작업은 개체에 대해 여러 부분으로 업로드되는 파트를 업로드합니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `Content-Length`
- `Content-MD5`

서버측 암호화에 대한 요청 헤더

다중 파트 업로드 시작 요청에 대해 SSE-C 암호화를 지정한 경우 각 업로드 파트 요청에 다음 요청 헤더를 포함해야 합니다.

- `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
- `x-amz-server-side-encryption-customer-key`[다중 파트 업로드 시작] 요청에서 제공한 암호화 키와 동일한 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 다중 파트 업로드 시작 요청에서 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. MultiPart Upload 작업이 완료되면 개체가 만들어지고 버전이 적용됩니다(해당하는 경우).

관련 정보

"서버 측 암호화 사용"

업로드 부품 - 복사

파트 업로드 - 복사 작업은 기존 개체의 데이터를 데이터 소스로 복사하여 개체의 일부를 업로드합니다.

Part-Copy 업로드 작업은 모든 Amazon S3 REST API 동작으로 구현됩니다.

이 요청은 에 지정된 오브젝트 데이터를 읽고 씁니다 `x-amz-copy-source-range` StorageGRID 시스템 내에서

지원되는 요청 헤더는 다음과 같습니다.

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

서버측 암호화에 대한 요청 헤더

다중 파트 업로드 시작 요청에 대해 SSE-C 암호화를 지정한 경우 각 업로드 파트 - 복사 요청에 다음 요청 헤더를 포함해야 합니다.

- `x-amz-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
- `x-amz-server-side-encryption-customer-key`[다중 파트 업로드 시작] 요청에서 제공한 암호화 키와 동일한 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 다중 파트 업로드 시작 요청에서 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

소스 객체가 SSE-C(customer-provided key)를 사용하여 암호화된 경우, 객체가 해독되고 복사될 수 있도록 업로드 파트 - 복사 요청에 다음 세 개의 헤더를 포함해야 합니다.

- `x-amz-copy-source-server-side-encryption-customer-algorithm`을 지정합니다 `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: 소스 객체를 만들 때 제공한 암호화 키를 지정합니다.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: 소스 개체를 만들 때 제공한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. MultiPart Upload 작업이 완료되면 개체가 만들어지고 버전이 적용됩니다(해당하는 경우).

멀티파트 업로드를 완료합니다

전체 다중 파트 업로드 작업은 이전에 업로드한 파트를 조립하여 개체의 여러 부분 업로드를 완료합니다.

충돌 해결

같은 키에 쓰는 두 클라이언트 등 충돌하는 클라이언트 요청은 "최근 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로

합니다.

개체 크기

StorageGRID는 최대 5TB의 오브젝트를 지원합니다.

요청 헤더

를 클릭합니다 `x-amz-storage-class` 요청 헤더가 지원되며 일치하는 ILM 규칙에서 이중 커밋 또는 균형 조정의 수집 동작을 지정하는 경우 StorageGRID에서 만드는 개체 복사본 수에 영향을 줍니다.

- `STANDARD`

  (기본값) ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 이중 커밋 수집 작업을 지정합니다.

- `REDUCED_REDUNDANCY`

  ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 단일 커밋 수집 작업을 지정합니다.

  > S3 오브젝트 잠금이 설정된 버킷으로 오브젝트를 밀어넣는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷으로 인스팅하는 경우, 를 참조하십시오 `REDUCED_REDUNDANCY` 옵션을 사용하면 오류가 반환됩니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

> 15일 이내에 여러 부분 업로드가 완료되지 않으면 작업이 비활성으로 표시되고 모든 관련 데이터가 시스템에서 삭제됩니다.

> 를 클릭합니다 `ETag` 반환된 값은 MD5 합계가 아니라 의 Amazon S3 API 구현을 따릅니다 `ETag` 다중 파트 개체에 대한 값입니다.

버전 관리

이 작업은 여러 부분 업로드를 완료합니다. 버켓에 대해 버전 관리가 활성화된 경우 다중 파트 업로드가 완료되면 개체 버전이 생성됩니다.

버켓에 대해 버전 관리가 활성화된 경우 고유한 가 사용됩니다 `versionId` 는 저장 중인 개체의 버전에 대해 자동으로 생성됩니다. 여기 `versionId` 를 사용하여 응답에서도 반환됩니다 `x-amz-version-id` 응답 헤더.

버전 관리가 일시 중단된 경우 개체 버전은 null로 저장됩니다 `versionId` null 버전이 이미 있는 경우 덮어쓰기가 됩니다.

> 버켓에 대해 버전 관리가 활성화된 경우, 같은 개체 키에서 동시 다중 파트 업로드가 완료된 경우에도 다중 파트 업로드를 완료하면 항상 새 버전이 생성됩니다. 버켓에 대해 버전 관리를 사용하지 않으면 다중 파트 업로드를 시작한 다음 다른 다중 파트 업로드를 시작하여 동일한 개체 키에서 먼저 완료할 수 있습니다. 비버전 버킷에서는 마지막으로 완료한 다중 파트 업로드가 우선 적용됩니다.

플랫폼 서비스에 대해 다중 파트 업로드가 발생하는 버킷이 구성된 경우 연결된 복제 또는 알림 작업이 실패한 경우에도 다중 파트 업로드가 성공합니다.

이 경우 SMTT(Grid Manager on Total Events)에서 경보가 발생합니다. 마지막 이벤트 메시지는 알림이 실패한 마지막 객체에 대해 "버킷 이름 오브젝트 키에 대한 알림을 게시하지 못했습니다"라고 표시됩니다. (이 메시지를 보려면 * 노드 * > * 스토리지 노드 * > * 이벤트 * 를 선택합니다. 테이블 상단의 마지막 이벤트 보기) 이벤트 메시지는 에도 나열됩니다 `/var/local/log/bycast-err.log`.

테넌트는 개체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 트리거할 수 있습니다. 테넌트는 불필요한 변경을 방지하기 위해 기존 값을 다시 제출할 수 있습니다.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

오류 응답

StorageGRID 시스템은 적용되는 모든 표준 S3 REST API 오류 응답을 지원합니다. 또한 StorageGRID 구현에는 여러 개의 사용자 지정 응답이 추가됩니다.

지원되는 **S3 API** 오류 코드입니다

이름	**HTTP** 상태입니다
액세스가 거부되었습니다	403 사용 금지
배다이제스트	400 잘못된 요청
BuckketAlreadyExists를 참조하십시오	409 충돌
BuckketNotEmpty	409 충돌
IncompleteBody	400 잘못된 요청
내부 오류입니다	500 내부 서버 오류입니다
InvalidAccessKeyId 입니다	403 사용 금지
InvalidArgument 를 선택합니다	400 잘못된 요청
InvalidBuckName입니다	400 잘못된 요청
InvalidBuckketState입니다	409 충돌
InvalidDigest 를 선택합니다	400 잘못된 요청

이름	**HTTP** 상태입니다
InvalidEncryptionAlgorithmError 가 발생합니다	400 잘못된 요청
InvalidPart 를 선택합니다	400 잘못된 요청
InvalidPartOrder를 선택합니다	400 잘못된 요청
InvalidRange 를 선택합니다	416 요청된 범위가 충분하지 않습니다
InvalidRequest 입니다	400 잘못된 요청
InvalidStorageClass 의 값을 반환합니다	400 잘못된 요청
InvalidTag 를 선택합니다	400 잘못된 요청
InvalidURI입니다	400 잘못된 요청
키투롱	400 잘못된 요청
MalformedXML을 참조하십시오	400 잘못된 요청
MetadataTooLarge를 참조하십시오	400 잘못된 요청
MethodNotAllowed 를 참조하십시오	405 메서드를 사용할 수 없습니다
MissingContentLength를 참조하십시오	411 길이 필요
MissingRequestBodyError가 발생합니다	400 잘못된 요청
MissingSecurityHeader 를 참조하십시오	400 잘못된 요청
NoSuchBucket	404를 찾을 수 없습니다
NoSuchKey를 클릭합니다	404를 찾을 수 없습니다
NoSuchUpload 를 클릭합니다	404를 찾을 수 없습니다
구현되지 않았습니다	501 구현되지 않음
NoSuchBuckketPolicy를 참조하십시오	404를 찾을 수 없습니다
ObjectLockConfigurationNotFoundError 가 발생합니다	404를 찾을 수 없습니다

이름	**HTTP** 상태입니다
사전 조건에 실패했습니다	412 전제 조건 실패
RequestTimeTooSkewed 를 참조하십시오	403 사용 금지
서비스를 사용할 수 없습니다	503 서비스를 사용할 수 없습니다
SignatureDoesNotMatch 를 참조하십시오	403 사용 금지
투만이버킷	400 잘못된 요청
UserKeyMustBeSpecified 를 선택합니다	400 잘못된 요청

StorageGRID 사용자 지정 오류 코드

이름	설명	**HTTP** 상태입니다
XBuckketLifecycleNotAllowed를 참조하십시오	버킷 수명 주기 구성은 레거시 준수 버킷에서 허용되지 않습니다	400 잘못된 요청
XBuckketPolicyParseException 을 참조하십시오	수신된 버킷 정책 JSON을 구문 분석하지 못했습니다.	400 잘못된 요청
XComplianceConflictt	레거시 준수 설정으로 인해 작업이 거부되었습니다.	403 사용 금지
XComplianceRedundancyForbidden을 선택합니다	레거시 준수 버킷에서는 감소된 중복성이 허용되지 않습니다	400 잘못된 요청
XMaxBuckketPolicyLengthExceeded 를 참조하십시오	정책이 허용되는 최대 버킷 정책 길이를 초과합니다.	400 잘못된 요청
XMissingInternalRequestHeader를 참조하십시오	내부 요청의 헤더가 누락되었습니다.	400 잘못된 요청
XNoSuchBuckketCompliance	지정된 버킷에 레거시 준법 기능이 설정되어 있지 않습니다.	404를 찾을 수 없습니다
XNotAcceptable(X 허용 가능)	요청에 충족되지 않은 하나 이상의 수락 헤더가 있습니다.	406 허용되지 않습니다
XNotImplemented(XNotImplemented)	제공한 요청은 구현되지 않은 기능을 의미합니다.	501 구현되지 않음

StorageGRID S3 REST API 작업

StorageGRID 시스템별 S3 REST API에 작업이 추가됩니다.

버킷 정합성 보장 요청 가져오기

Get Bucket 정합성 보장 요청을 사용하면 특정 버킷에 적용되는 정합성 보장 수준을 확인할 수 있습니다.

기본 정합성 보장 컨트롤은 새로 생성된 객체에 대해 읽기/쓰기 작업을 보장하도록 설정됩니다.

이 작업을 완료하려면 S3:GetBucketConsistency 권한이 있거나 계정 루트여야 합니다.

요청 예

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

응답

응답 XML에서 `<Consistency>` 다음 값 중 하나를 반환합니다.

일관성 제어	설명
모두	모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
강함 - 글로벌	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.
강력한 사이트	사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
읽기-후-새로-쓰기	(기본값) 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 Amazon S3 일관성 보장 과 일치합니다. • 참고: * 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 Amazon S3와 유사한 일관성 보장이 필요하지 않는 한 일관성 제어를 ""사용 가능""으로 설정합니다.

일관성 제어	설명
사용 가능(헤드 작업의 최종 일관성)	"새 쓰기 후 다시 쓰기" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다. 헤드 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

응답 예

```
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 제어"

버킷 정합성 보장 요청을 배치합니다

PUT 버킷 정합성 보장 요청을 사용하면 버킷에서 수행된 작업에 적용할 정합성 수준을 지정할 수 있습니다.

기본 정합성 보장 컨트롤은 새로 생성된 객체에 대해 읽기/쓰기 작업을 보장하도록 설정됩니다.

이 작업을 완료하려면 S3:PutBucketConsistency 권한이 있거나 계정 루트여야 합니다.

요청하십시오

를 클릭합니다 `x-ntap-sg-consistency` 매개 변수는 다음 값 중 하나를 포함해야 합니다.

일관성 제어	설명
모두	모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
강함 - 글로벌	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.

일관성 제어	설명
강력한 사이트	사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
읽기-후-새로-쓰기	(기본값) 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 Amazon S3 일관성 보장 과 일치합니다. • 참고: * 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 Amazon S3와 유사한 일관성 보장이 필요하지 않는 한 일관성 제어를 ""사용 가능""으로 설정합니다.
사용 가능(헤드 작업의 최종 일관성)	"새 쓰기 후 다시 쓰기" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다. 헤드 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

- 참고: * 일반적으로 "새 쓰기 후" 정합성 보장 제어 값을 사용해야 합니다. 요청이 올바르게 작동하지 않는 경우 가능한 경우 응용 프로그램 클라이언트 동작을 변경합니다. 또는 클라이언트가 각 API 요청에 대한 정합성 제어를 지정하도록 구성합니다. 버킷 레벨에서만 정합성 제어를 최후의 수단으로 설정하십시오.

요청 예

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

관련 정보

"일관성 제어"

버킷 최종 액세스 시간 요청 가져오기

[버킷 최종 액세스 시간 가져오기(Get Bucket Last Access Time) 요청 을 사용하면 개별 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되거나 비활성화되었는지 확인할 수 있습니다.

이 작업을 완료하려면 S3:GetBucketLastAccessTime 권한이 있거나 계정 루트여야 합니다.

요청 예

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

응답 예

이 예에서는 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되어 있음을 보여 줍니다.

```
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>
```

버킷 최종 액세스 시간 요청

Put Bucket Last Access Time 요청을 사용하면 개별 버킷에 대한 마지막 액세스 시간 업데이트를 활성화하거나 비활성화할 수 있습니다. 마지막 액세스 시간 업데이트를 비활성화하면 성능이 향상되고 버전 10.3.0 이상으로 생성된 모든 버킷의 기본 설정이 됩니다.

이 작업을 완료하려면 버킷에 대한 S3:PutBuckketLastAccessTime 권한이 있거나 계정 루트여야 합니다.

> StorageGRID 버전 10.3부터는 모든 새 버킷에 대해 마지막 액세스 시간에 대한 업데이트가 기본적으로 비활성화됩니다. 이전 버전의 StorageGRID를 사용하여 만든 버킷이 있고 새 기본 동작과 일치시키려면 이전의 각 버킷에 대해 마지막 액세스 시간 업데이트를 명시적으로 비활성화해야 합니다. 테넌트 관리자의 Put Bucket Last Access Time 요청, * S3 * > * Bucket * > * Change Last Access Setting * 확인란 또는 테넌트 관리 API를 사용하여 마지막 액세스 시간에 대한 업데이트를 활성화하거나 비활성화할 수 있습니다.

버킷에 대해 마지막 액세스 시간 업데이트가 비활성화된 경우 버킷의 작업에 다음 동작이 적용됩니다.

- 객체 가져오기, 객체 ACL 가져오기, 객체 태그 지정 가져오기 및 헤드 객체 요청은 마지막 액세스 시간을 업데이트하지 않습니다. ILM(정보 수명 주기 관리) 평가를 위해 객체가 대기열에 추가되지 않습니다.
- Put Object - 메타데이터만 업데이트하는 객체 태그 지정 요청을 복사하고 배치하면 마지막 액세스 시간도 업데이트됩니다. ILM 평가를 위해 오브젝트가 대기열에 추가됩니다.
- 소스 버킷에 대해 마지막 액세스 시간에 대한 업데이트를 사용할 수 없는 경우 객체 복사 요청을 소스 버킷의 마지막 액세스 시간을 업데이트하지 않습니다. 복사된 객체는 소스 버킷에 대한 ILM 평가를 위해 대기열에 추가되지 않습니다. 그러나 대상의 경우, 개체 복사 요청은 항상 마지막 액세스 시간을 업데이트합니다. ILM 평가를 위해 개체의 복사본이 대기열에 추가됩니다.

- 완료 다중 파트 업로드 요청 마지막 액세스 시간 업데이트 완료된 객체가 ILM 평가를 위해 대기열에 추가됩니다.

예를 요청하십시오

이 예제에서는 버킷의 마지막 액세스 시간을 설정합니다.

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

이 예제에서는 버킷의 마지막 액세스 시간을 비활성화합니다.

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

관련 정보

"테넌트 계정을 사용합니다"

버킷 메타데이터 알림 구성 요청을 삭제합니다

Delete Bucket 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 예

이 예제에서는 버킷에 대한 검색 통합 서비스를 비활성화하는 방법을 보여 줍니다.

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

버킷 메타데이터 알림 구성 요청을 가져옵니다

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

이 작업을 완료하려면 S3:GetBuckMetadataNotification 권한이 있거나 계정 루트여야 합니다.

요청 예

이 요청은 이름이 인 버킷에 대한 메타데이터 알림 구성을 검색합니다 `bucket`.

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

응답

응답 본문에는 버킷에 대한 메타데이터 알림 구성이 포함됩니다. 메타데이터 알림 구성을 사용하면 버킷이 검색 통합을 위해 구성되는 방식을 결정할 수 있습니다. 즉, 인덱싱된 개체와 해당 개체 메타데이터가 전송되는 끝점을 확인할 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 적용되는 오브젝트와 StorageGRID가 오브젝트 메타데이터를 보내야 하는 대상을 지정합니다. 대상은 StorageGRID 끝점의 URN을 사용하여 지정해야 합니다.

이름	설명	필수 요소입니다
MetadataNotificationConfiguration을 참조하십시오	메타데이터 알림의 개체 및 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 규칙 요소가 포함되어 있습니다.	예

이름	설명	필수 요소입니다
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
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

이름	설명	필수 요소입니다
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

응답 예

사이에 포함된 XML `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` 태그는 버킷에 대해 검색 통합 끝점과의 통합이 어떻게 구성되어 있는지 보여줍니다. 이 예제에서는 개체 메타데이터가 라는 Elasticsearch 인덱스에 전송되고 있습니다 `current` 이름을 입력합니다 `2017` 라는 AWS 도메인에서 호스팅됩니다 `records`.

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

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

관련 정보

"테넌트 계정을 사용합니다"

PUT 버킷 메타데이터 알림 구성 요청

Put Bucket 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대한 검색 통합 서비스를 활성화할 수 있습니다. 요청 본문에 제공하는 메타데이터 알림 구성 XML은 대상 검색 인덱스에 메타데이터가 전송되는 개체를 지정합니다.

이 작업을 완료하려면 버킷에 대한 S3:PutBucketMetadataNotification 권한이 있거나 계정 루트여야 합니다.

요청하십시오

요청 본문에는 메타데이터 알림 구성이 포함되어야 합니다. 각 메타데이터 알림 구성에는 하나 이상의 규칙이 포함됩니다. 각 규칙은 적용되는 오브젝트와 StorageGRID가 오브젝트 메타데이터를 보내야 하는 대상을 지정합니다.

개체 이름의 접두어를 기준으로 개체를 필터링할 수 있습니다. 예를 들어, 접두사가 있는 개체에 대한 메타데이터를 보낼 수 있습니다 `/images` 목적지 하나와 접두사가 있는 오브젝트 `/videos` 다른 사람에게.

중복되는 접두사가 있는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어, 접두사가 있는 개체에 대해 하나의 규칙이 포함된 구성입니다 `test` 접두사가 있는 개체에 대한 두 번째 규칙입니다 `test2` 허용되지 않습니다.

대상은 StorageGRID 끝점의 URN을 사용하여 지정해야 합니다. 메타데이터 알림 구성이 제출되거나 요청이 로 실패하는 경우 엔드포인트가 있어야 합니다 `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 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

예를 요청하십시오

이 예제에서는 버킷에 대한 검색 통합을 활성화하는 방법을 보여 줍니다. 이 예제에서 모든 오브젝트의 오브젝트 메타데이터는 동일한 대상으로 전송됩니다.

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

<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 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.

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

<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

"테넌트 계정을 사용합니다"

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	설명
버킷 및 오브젝트 정보	버킷	버킷의 이름입니다
버킷 및 오브젝트 정보	키	개체 키 이름입니다
버킷 및 오브젝트 정보	버전 ID	오브젝트 버전, 버전 버킷 내 오브젝트
버킷 및 오브젝트 정보	지역	버킷 영역(예 `us-east-1`
시스템 메타데이터	크기	HTTP 클라이언트에 표시되는 개체 크기(바이트)입니다

유형	항목 이름	설명
시스템 메타데이터	MD5	개체 해시
사용자 메타데이터	메타데이터 *key:value*	객체에 대한 모든 사용자 메타데이터를 키 값 쌍으로 사용합니다
태그	태그 *key:value*	개체에 대해 정의된 모든 개체 태그를 키 값 쌍으로 사용합니다

- 참고: * 태그 및 사용자 메타데이터의 경우 StorageGRID는 날짜 및 숫자를 Elasticsearch에 문자열로 전달하거나 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.

스토리지 사용 요청 가져오기

Get Storage Usage 요청은 계정이 사용하는 총 스토리지 양과 계정과 연결된 각 버킷에 대해 알려줍니다.

계정 및 해당 버킷에서 사용되는 스토리지의 양은 을 사용하여 수정된 Get Service 요청을 통해 얻을 수 있습니다 `x-ntap-sg-usage` 쿼리 매개 변수입니다. 시스템에서 처리하는 PUT 및 삭제 요청과는 별도로 버킷 스토리지 사용량을 추적합니다. 특히 시스템이 과부하 상태인 경우, 사용 값이 요청 처리를 기준으로 예상 값과 일치하기 전에 약간의 지연이 있을 수 있습니다.

기본적으로 StorageGRID는 강력한 글로벌 일관성을 사용하여 사용 정보 검색을 시도합니다. 강력한 글로벌 일관성을 달성할 수 없는 경우 StorageGRID는 강력한 사이트 일관성으로 사용 정보를 검색합니다.

이 작업을 완료하려면 S3:ListAllMyBucket 권한이 있거나 계정 루트여야 합니다.

요청 예

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

응답 예

이 예에서는 두 버킷에 4개의 오브젝트와 12바이트의 데이터가 있는 계정을 보여 줍니다. 각 버킷에는 2개의 오브젝트와 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 개체 버전은 에 기여합니다 `ObjectCount` 및 `DataBytes` 응답의 값입니다. Delete markers(마커 삭제)는 에 추가되지 않습니다 `ObjectCount` 합계.

관련 정보

"일관성 제어"

레거시 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청

StorageGRID S3 REST API를 사용하여 레거시 규정 준수 기능을 사용하여 생성된 버킷을 관리해야 할 수 있습니다.

규정 준수 기능이 사용되지 않습니다

이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

이전에 글로벌 규정 준수 설정을 활성화한 경우 StorageGRID 11.5로 업그레이드하면 글로벌 S3 오브젝트 잠금 설정이 자동으로 활성화됩니다. Compliance를 사용하도록 설정한 상태에서 새 버킷을 더 이상 생성할 수 없지만, 필요에 따라

StorageGRID S3 REST API를 사용하여 기존의 규정을 준수하는 버킷을 관리할 수 있습니다.

"S3 오브젝트 잠금 사용"

"ILM을 사용하여 개체를 관리합니다"

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

사용되지 않음: 규정 준수를 위해 버킷 요청 수정을 배치합니다

SGCompliance XML 요소는 사용되지 않습니다. 이전 버전에서는 이 StorageGRID 사용자 정의 요소를 PUT 버킷 요청의 선택적 XML 요청 본문에 포함하여 준수 버킷을 생성할 수 있었습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

"S3 오브젝트 잠금 사용"

"ILM을 사용하여 개체를 관리합니다"

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

Compliance가 설정된 새 버킷을 더 이상 생성할 수 없습니다. 새 준수 버킷을 생성하기 위해 준수 준수를 위해 Put Bucket 요청 수정을 사용하려는 경우 다음 오류 메시지가 반환됩니다.

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

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"테넌트 계정을 사용합니다"

사용되지 않음: 버킷 준수 요청 가져오기

Get Bucket 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷에 현재 적용되는 준수 설정을 확인할 수 있습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

"S3 오브젝트 잠금 사용"

"ILM을 사용하여 개체를 관리합니다"

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

이 작업을 완료하려면 S3:GetBucketCompliance 권한이 있거나 계정 루트여야 합니다.

요청 예

이 요청 예제를 통해 이름이 인 버킷의 준수 설정을 확인할 수 있습니다 `mybucket`.

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

응답 예

응답 XML에서 `<SGCompliance>` 에는 버킷에 적용되는 준수 설정이 나와 있습니다. 이 예제 응답에서는 오브젝트를 그리드에 인제스트하는 시점을 시작으로 각 오브젝트를 1년(525,600분)동안 보존할 버킷의 규정 준수 설정을 보여 줍니다. 현재 이 버킷에 대한 법적 보류가 없습니다. 각 개체는 1년 후에 자동으로 삭제됩니다.

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

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

이름	설명
RetenionPeriodMinutes(주기적 지연 시간)	이 버킷에 추가된 객체의 보존 기간(분)입니다. 보존 기간은 객체가 그리드에 수집될 때 시작됩니다.
LegalHold	• 참: 이 버킷은 현재 법적 증거 자료 보관 중입니다. 이 버킷의 오브젝트는 보존 기간이 만료된 경우에도 법적 보류가 해제될 때까지 삭제할 수 없습니다. • 거짓: 이 버킷은 현재 법적 증거 자료 보관 중이 아닙니다. 이 버킷의 오브젝트는 보존 기간이 만료되면 삭제할 수 있습니다.

이름	설명
자동 삭제	• 참: 버킷이 법적 보존 상태에 있지 않는 한, 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제됩니다. • False: 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제되지 않습니다. 이러한 개체를 삭제하려면 해당 개체를 수동으로 삭제해야 합니다.

오류 응답

버킷이 규정을 준수하도록 생성되지 않은 경우 응답에 대한 HTTP 상태 코드는 입니다 `404 Not Found`, 의 S3 오류 코드 포함 `XNoSuchBucketCompliance`.

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"테넌트 계정을 사용합니다"

폐기됨: 버킷 준수 요청을 넣으십시오

PUT 버킷 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷의 준수 설정을 수정할 수 있습니다. 예를 들어, 기존 버킷을 법적 보존 상태로 놓거나 보존 기간을 늘릴 수 있습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

"S3 오브젝트 잠금 사용"

"ILM을 사용하여 개체를 관리합니다"

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

이 작업을 완료하려면 S3:PutBucketCompliance 권한이 있거나 계정 루트 권한이 있어야 합니다.

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

요청 예

이 예제 요청은 이름이 인 버킷의 준수 설정을 수정합니다 `mybucket`. 이 예제에서는 의 개체를 보여 줍니다 `mybucket` 이제 오브젝트를 그리드로 인제스트하는 시점을 시작으로 1년이 아닌 2년(1,051,200분) 동안 보존됩니다. 이 버킷에는 법적 구속이 없습니다. 각 개체는 2년 후에 자동으로 삭제됩니다.

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

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

이름	설명
RetenionPeriodMinutes(주기적 지연 시간)	이 버킷에 추가된 객체의 보존 기간(분)입니다. 보존 기간은 객체가 그리드에 수집될 때 시작됩니다. • 주의: * RetenitionPeriodMinutes에 새 값을 지정할 때는 버킷의 현재 보존 기간과 같거나 큰 값을 지정해야 합니다. 버킷의 보존 기간이 설정된 후에는 해당 값을 줄일 수 없으며 증가만 가능합니다.
LegalHold	• 참: 이 버킷은 현재 법적 증거 자료 보관 중입니다. 이 버킷의 오브젝트는 보존 기간이 만료된 경우에도 법적 보류가 해제될 때까지 삭제할 수 없습니다. • 거짓: 이 버킷은 현재 법적 증거 자료 보관 중이 아닙니다. 이 버킷의 오브젝트는 보존 기간이 만료되면 삭제할 수 있습니다.
자동 삭제	• 참: 버킷이 법적 보존 상태에 있지 않는 한, 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제됩니다. • False: 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제되지 않습니다. 이러한 개체를 삭제하려면 해당 개체를 수동으로 삭제해야 합니다.

규정 준수 설정을 위한 정합성 보장 레벨

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

데이터 센터 사이트 또는 사이트의 여러 스토리지 노드를 사용할 수 없기 때문에 StorageGRID가 * 강력한 글로벌 * 정합성 보장 수준을 달성할 수 없는 경우 응답에 대한 HTTP 상태 코드는 입니다 `503 Service Unavailable.`

이 응답을 받으면 그리드 관리자에게 문의하여 필요한 스토리지 서비스를 가능한 빨리 사용할 수 있도록 해야 합니다.

그리드 관리자가 각 사이트에서 충분한 스토리지 노드를 사용할 수 없는 경우, 기술 지원 부서에서 * strong-site * 정합성 보장 수준을 강제로 진행하여 실패한 요청을 다시 시도하도록 할 수 있습니다.

> 기술 지원 부서의 지시가 있는 경우를 제외하고, 이 레벨을 사용할 경우 발생할 수 있는 결과를 이해하지 않는 한 * 강력한 사이트 * 일관성 수준을 강제로 버킷 규정 준수를 강제하지 마십시오.

정합성 보장 수준을 * strong-site * 로 축소하면 StorageGRID는 업데이트된 규정 준수 설정이 사이트 내의 클라이언트 요청에 대해서만 읽기/쓰기 후 일관성을 갖게 됩니다. 즉, 모든 사이트 및 스토리지 노드를 사용할 수 있을 때까지 StorageGRID 시스템에 이 버킷에 대한 여러 개의 일관되지 않은 설정이 일시적으로 있을 수 있습니다. 설정이 일치하지 않으면 예기치 않거나 원치 않는 동작이 발생할 수 있습니다. 예를 들어, 버킷을 법적 증거 자료 보관 아래에 놓고 정합성 보장 수준을 낮추면 버킷의 이전 규정 준수 설정(즉, 법적 증거 자료 보관)이 일부 데이터 센터 사이트에서 계속 적용될 수 있습니다. 따라서 보존 기간이 만료되면 사용자나 자동 삭제(활성화된 경우)에 의해 법적 보류라고 생각하는 개체가 삭제될 수 있습니다.

strong-site * 정합성 보장 레벨을 강제로 사용하려면 Put Bucket 준수 요청을 다시 발행하고 을 포함합니다 `Consistency-Control` HTTP 요청 헤더는 다음과 같습니다.

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

오류 응답

- 버킷이 규정을 준수하도록 생성되지 않은 경우 응답에 대한 HTTP 상태 코드는 입니다 `404 Not Found`.
- If(경우 `RetentionPeriodMinutes` 요청이 버킷의 현재 보존 기간보다 작은 경우 HTTP 상태 코드는 입니다 `400 Bad Request`.

관련 정보

"사용되지 않음: 규정 준수를 위해 버킷 요청 수정을 배치합니다"

"테넌트 계정을 사용합니다"

"ILM을 사용하여 개체를 관리합니다"

버킷 및 그룹 액세스 정책

StorageGRID은 AWS(Amazon Web Services) 정책 언어를 사용하여 S3 테넌트가 해당 버킷 및 오브젝트 내의 버킷에 대한 액세스를 제어할 수 있도록 합니다. StorageGRID 시스템은 S3 REST API 정책 언어의 하위 집합을 구현합니다. S3 API에 대한 액세스 정책은 JSON으로 기록됩니다.

액세스 정책 개요

StorageGRID에서 지원하는 액세스 정책에는 두 가지 유형이 있습니다.

- * 버킷 정책 * - 버킷 정책 가져오기, 버킷 정책 적용 및 버킷 정책 삭제 S3 API 작업을 사용하여 구성됩니다. 버킷 정책은 버킷에 첨부되므로 버킷 소유자 계정 또는 버킷에 대한 다른 계정 및 버킷에 있는 오브젝트에 대한 사용자의 액세스를 제어하도록 구성됩니다. 버킷 정책은 하나의 버킷과 여러 그룹에만 적용됩니다.

- 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성된 * 그룹 정책 * 입니다. 그룹 정책은 계정의 그룹에 연결되므로 해당 그룹이 해당 계정이 소유한 특정 리소스에 액세스할 수 있도록 구성됩니다. 그룹 정책은 하나의 그룹에만 적용되고 여러 버킷에 적용될 수 있습니다.

StorageGRID 버킷 및 그룹 정책은 아마존에서 정의한 특정 문법을 따릅니다. 각 정책 안에는 정책 문의 배열이 들어 있으며 각 문에는 다음 요소가 포함되어 있습니다.

- 정책 ID(SID)(선택 사항)
- 효과
- Principal/NotPrincipal입니다
- 리소스/NotResource입니다
- 작업/NotAction
- 조건(선택 사항)

정책 문은 이 구조를 사용하여 권한을 지정합니다. pert <effect> <principal>이(가) <condition>이(가) 적용될 때 <Resource>에서 <Action>을(를) 수행하도록 허용/거부합니다.

각 정책 요소는 특정 함수에 사용됩니다.

요소	설명
SID	SID 요소는 선택 사항입니다. SID는 사용자에 대한 설명으로만 제공됩니다. StorageGRID 시스템에서 저장하지만 해석되지 않습니다.
효과	Effect 요소를 사용하여 지정된 작업의 허용 여부를 설정합니다. 지원되는 작업 요소 키워드를 사용하여 버킷 또는 오브젝트에 대해 허용(또는 거부)하는 작업을 식별해야 합니다.
Principal/NotPrincipal입니다	사용자, 그룹 및 계정이 특정 리소스에 액세스하고 특정 작업을 수행하도록 허용할 수 있습니다. 요청에 S3 서명이 포함되지 않은 경우 와일드카드 문자(*)를 보안 주체에 지정하여 익명 액세스가 허용됩니다. 기본적으로 계정 루트만 해당 계정이 소유한 리소스에 액세스할 수 있습니다. 버킷 정책에서 Principal 요소만 지정하면 됩니다. 그룹 정책의 경우 정책이 연결된 그룹이 암시적 Principal 요소입니다.
리소스/NotResource입니다	Resource 요소는 버킷 및 오브젝트를 식별합니다. ARN(Amazon Resource Name)을 사용하여 리소스를 식별하는 버킷 및 객체에 대한 권한을 허용하거나 거부할 수 있습니다.

요소	설명
작업/NotAction	Action 및 Effect 요소는 권한의 두 구성 요소입니다. 그룹이 리소스를 요청하면 리소스에 대한 액세스가 부여되거나 거부됩니다. 명시적으로 권한을 할당하지 않는 한 액세스가 거부되지만 명시적 DENY를 사용하여 다른 정책이 부여한 권한을 재정의할 수 있습니다.
조건	Condition 요소는 선택 요소입니다. 조건을 사용하면 식을 만들어 정책을 적용해야 하는 시기를 결정할 수 있습니다.

Action 요소에서 와일드카드 문자(*)를 사용하여 모든 작업이나 작업의 하위 집합을 지정할 수 있습니다. 예를 들어 이 작업은 S3:GetObject , S3:PutObject 및 S3:DeleteObject 와 같은 사용 권한을 일치시킵니다.

```
s3:*Object
```

Resource 요소에서 와일드카드 문자(\ **)** 및 **(?)**를 사용할 수 있습니다**.** 별표**(**)가 0개 이상의 문자와 일치하면 물음표(?)가 모든 단일 문자와 일치합니다.

Principal 요소에서 모든 사용자에게 권한을 부여하는 익명 액세스를 설정하는 경우를 제외하고 와일드카드 문자는 지원되지 않습니다. 예를 들어 와일드카드(*)를 Principal 값으로 설정합니다.

```
"Principal":"*"
```

다음 예제에서는 Effect , Principal , Action 및 Resource 요소를 사용합니다. 이 예제에서는 "Allow" 효과를 사용하여 Principals, 즉 admin 그룹에 제공하는 전체 버킷 정책 문을 보여 줍니다 `federated-group/admin` 재무그룹을 의미합니다 `federated-group/finance`, 작업 수행 권한 `s3:ListBucket` 을(를) 버킷에 표시합니다 `mybucket` 및 조치 `s3:GetObject` 버킷에 있는 모든 물체

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

버킷 정책은 크기 제한이 20,480바이트이고 그룹 정책은 크기 제한이 5,120바이트입니다.

관련 정보

"테넌트 계정을 사용합니다"

정책에 대한 정합성 보장 제어 설정입니다

기본적으로 그룹 정책에 대한 모든 업데이트는 최종적으로 일치합니다. 그룹 정책이 일관되면 정책 캐싱 때문에 변경 내용이 적용되는 데 15분 정도 더 걸릴 수 있습니다. 기본적으로 버킷 정책에 대한 모든 업데이트도 최종적으로 일치합니다.

필요에 따라 버킷 정책 업데이트의 일관성 보장을 변경할 수 있습니다. 예를 들어, 보안상의 이유로 버킷 정책을 최대한 빨리 변경할 수 있습니다.

이 경우 를 설정할 수 있습니다 `Consistency-Control` PUT 버킷 정책 요청의 헤더나 PUT 버킷 정합성 보장 요청을 사용할 수 있습니다. 이 요청에 대한 정합성 제어를 변경할 때는 읽기 후 쓰기 정합성을 보장하는 * All * 값을 사용해야 합니다. Put Bucket 정합성 보장 요청의 헤더에 다른 정합성 보장 제어 값을 지정하면 요청이 거부됩니다. Put Bucket 정책 요청에 대해 다른 값을 지정하면 값이 무시됩니다. 버킷 정책이 일관되면 정책 캐싱으로 인해 변경 사항이 적용되는 데 8초가 더 걸릴 수 있습니다.

> 정합성 수준을 * All * 로 설정하면 새 버킷 정책이 더 빨리 발효되도록 하려면 작업이 완료되면 버킷 수준 제어를 원래 값으로 다시 설정해야 합니다. 그렇지 않으면 이후의 모든 버킷 요청은 * All * 설정을 사용합니다.

정책 설명에 **ARN** 사용

정책 문에서 ARN은 Principal 및 Resource 요소에서 사용됩니다.

- 이 구문을 사용하여 S3 리소스 ARN을 지정합니다.

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

- 이 구문을 사용하여 ID 리소스 ARN(사용자 및 그룹)을 지정합니다.

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

기타 고려 사항:

- 별표(*)를 와일드카드로 사용하여 개체 키 안에 0개 이상의 문자를 일치시킬 수 있습니다.
- 개체 키에 지정할 수 있는 국제 문자는 JSON UTF-8 또는 JSON\u 이스케이프 시퀀스를 사용하여 인코딩해야 합니다. 퍼센트 인코딩은 지원되지 않습니다.

  "RFC 2141 URN 구문"

  Put Bucket 정책 작업의 HTTP 요청 본문은 charset=UTF-8로 인코딩되어야 합니다.

정책에서 리소스 지정

정책 문에서 Resource 요소를 사용하여 사용 권한이 허용되거나 거부되는 버킷 또는 개체를 지정할 수 있습니다.

- 각 정책 문에는 Resource 요소가 필요합니다. 정책에서 리소스는 요소로 표시됩니다 `Resource`또는 `NotResource` 제외.
- S3 리소스 ARN을 사용하여 리소스를 지정합니다. 예를 들면 다음과 같습니다.

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 개체 키 내에서 정책 변수를 사용할 수도 있습니다. 예를 들면 다음과 같습니다.

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 리소스 값은 그룹 정책이 생성될 때 아직 존재하지 않는 버킷을 지정할 수 있습니다.

관련 정보

"정책에서 변수 지정"

정책의 보안 주체 지정

Principal 요소를 사용하여 policy 문에 의해 리소스에 대한 액세스가 허용/거부된 사용자, 그룹 또는 테넌트 계정을 식별합니다.

- 버킷 정책의 각 정책 선언에는 Principal 요소가 포함되어야 합니다. 그룹 정책의 정책 설명은 그룹이 보안 주체로 인식되기 때문에 Principal 요소가 필요하지 않습니다.
- 정책에서 교장은 제외에 대해 "Principal" 또는 "NotPrincipal" 요소로 표시됩니다.
- 계정 기반 ID는 ID 또는 ARN을 사용하여 지정해야 합니다.

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 이 예에서는 계정 루트 및 계정의 모든 사용자를 포함하는 테넌트 계정 ID 27233906934684427525를 사용합니다.

```
 "Principal": { "AWS": "27233906934684427525" }
```

- 계정 루트만 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 특정 페더레이션 사용자("Alex")를 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 특정 통합 그룹("관리자")을 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- 익명 보안 주체를 지정할 수 있습니다.

```
"Principal": "*"
```

- 모호함을 방지하려면 사용자 이름 대신 사용자 UUID를 사용할 수 있습니다.

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

예를 들어 Alex가 조직과 사용자 이름을 그대로 두고 있다고 가정해 보겠습니다 `Alex` 이(가) 삭제됩니다. 새로운 Alex가 조직에 합류하여 동일한 권한이 할당된 경우 `Alex` 사용자 이름, 새 사용자는 의도하지 않게 원래 사용자에게 부여된 권한을 상속할 수 있습니다.

- Principal 값은 버킷 정책이 생성될 때 아직 존재하지 않는 그룹/사용자 이름을 지정할 수 있습니다.

정책에서 사용 권한 지정

정책에서 Action 요소는 리소스에 대한 권한을 허용/거부하는 데 사용됩니다. 정책에서 지정할 수 있는 사용 권한 집합이 있으며, 이러한 권한은 "작업" 또는 "NotAction" 요소로 표시됩니다. 각 요소는 특정 S3 REST API 작업에 매핑됩니다.

이 표에는 버킷에 적용되는 사용 권한과 객체에 적용되는 사용 권한이 나열되어 있습니다.

Amazon S3는 이제 PUT 및 DELETE Bucket 복제 작업 모두에 S3:PutReplicationConfiguration 권한을 사용합니다. StorageGRID는 원래 Amazon S3 사양과 일치하는 각 작업에 대해 별도의 권한을 사용합니다.

기존 값을 덮어쓰는 데 PUT를 사용할 때 삭제가 수행됩니다.

버킷에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:생성 버킷	버킷 을 놓습니다	
S3:삭제 버킷	버킷 삭제	
S3:DeleteBucketMetadataNotification	버킷 메타데이터 알림 구성을 삭제합니다	예
S3:삭제 BucketPolicy	버킷 정책을 삭제합니다	
S3:DeleteReplicationConfiguration	버킷 복제를 삭제합니다	예, PUT 및 DELETE에 대한 별도의 권한 *
S3:GetBuckketAcl	버킷 ACL 가져오기	
S3:GetBucketCompliance	버킷 규정 준수 가져오기(더 이상 사용되지 않음)	예
S3:GetBuckketConsistency	버킷 일관성 확보	예

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:GetBuckketCORS	버킷 CORS를 가져옵니다	
S3:GetEncryptionConfiguration	버킷 암호화 가져오기	
S3:GetBucketLastAccessTime	버킷 최종 액세스 시간 가져오기	예
S3:GetBucketLocation	버킷 위치를 가져옵니다	
S3:GetBuckMetadataNotification 을 참조하십시오	Bucket 메타데이터 알림 구성 가져오기	예
S3:GetBucketNotification 을 참조하십시오	버킷 알림을 받습니다	
S3:GetBuckketObjectLockConfiguration	개체 잠금 구성을 가져옵니다	
S3:GetBuckketPolicy를 참조하십시오	버킷 정책 가져오기	
S3:GetBucketTagging	버킷 태그 지정을 가져옵니다	
S3:GetBucketVersioning	버킷 버전 관리 가져오기	
S3:GetLifecycleConfiguration	버킷 수명 주기 가져오기	
S3:GetReplicationConfiguration	버킷 복제를 가져옵니다	
S3:ListAllMyBucket	• 서비스 받기 • 스토리지 사용량을 가져옵니다	예, 스토리지 사용량 가져오에 대해 가능합니다
S3:목록 버킷	• 버킷 가져오기(객체 나열) • 헤드 버킷 • 사후 개체 복원	
S3:ListBuckketMultipartUploads	• 다중 파트 업로드 나열 • 사후 개체 복원	
S3:목록 BuckketVersions	버킷 버전 가져오기	
S3: PutBucketCompliance	버킷 규정 준수(폐기됨)	예

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3: PutBucketConsistency	버킷 일관성을 유지합니다	예
S3: PutBucketCORS	• 버킷 CORS† 삭제 • 버킷 CORS를 넣습니다	
S3:PutEncryptionConfiguration	• Bucket 암호화를 삭제합니다 • Bucket 암호화를 적용합니다	
S3:PutBucketLastAccessTime	버킷 최종 접근 시간	예
S3:PutBucketMetadataNotification	Put Bucket 메타데이터 알림 구성	예
S3: PutBucketNotification	버킷 통지를 보냅니다	
S3:PutBucketObjectLockConfiguration	에 Bucket 을 놓습니다 `x-amz-bucket-object-lock-enabled: true` 요청 헤더(S3:CreateBucket 권한도 필요함)	
S3: PutBucketPolicy	버킷 정책을 적용합니다	
S3: PutBucketTagging	• 버킷 태그 표시 삭제† • Bucket 태그 달기	
S3: PutBucketVersioning	버킷 버전 관리	
S3: PutLifecycleConfiguration	• 버킷 수명 주기 삭제† • 버킷 수명 주기를 놓습니다	
S3:PutReplicationConfiguration	버킷 복제를 배치합니다	예, PUT 및 DELETE에 대한 별도의 권한 *

객체에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:중단멀티업로드입니다	• 멀티파트 업로드를 중단합니다 • 사후 개체 복원	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:DeleteObject 를 선택합니다	• 개체 삭제 • 여러 개체를 삭제합니다 • 사후 개체 복원	
S3:삭제 ObjectTagging	개체 태그 지정을 삭제합니다	
S3:DeleteObjectVersionTagging	개체 태그 지정 삭제(개체의 특정 버전)	
S3:DeleteObjectVersion	개체 삭제(개체의 특정 버전)	
S3:GetObject	• 객체 가져오기 • 헤드 개체 • 사후 개체 복원	
S3:GetObjectAcl	객체 ACL을 가져옵니다	
S3:GetObjectLegalHold	객체 법적 증거 자료 보관	
S3:GetObjectRetention	개체 보존 가져오기	
S3:GetObjectTagging	개체 태그 지정을 가져옵니다	
S3:GetObjectVersionTagging	개체 태그 지정 가져오기(개체의 특정 버전)	
S3:GetObjectVersion	개체 가져오기(개체의 특정 버전)	
S3:ListMultipartUploadParts(S3:List MultimpartUploadParts) 를	부품 나열, POST 개체 복원	
S3:PutObject	• 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 사후 개체 복원 • 멀티파트 업로드를 시작합니다 • 멀티파트 업로드를 완료합니다 • 부품 업로드 • 업로드 부품 - 복사	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:PutObjectLegalHold	개체를 법적 증거 자료 보관	
S3:PutObjectRetention	개체 보존	
S3:PutObjectTagging	개체 태깅을 넣습니다	
S3:PutObjectVersionTagging	개체 태그 지정(개체의 특정 버전)	
S3:PutOverwriteObject	• 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 개체 태그 지정 • 개체 태그 지정 삭제 • 멀티파트 업로드를 완료합니다	예
S3:RestoreObject	사후 개체 복원	

PutOverwriteObject 권한 사용

S3:PutOverwriteObject 권한은 개체를 만들거나 업데이트하는 작업에 적용되는 사용자 지정 StorageGRID 권한입니다. 이 사용 권한의 설정에 따라 클라이언트가 개체의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 덮어쓸 수 있는지 여부가 결정됩니다.

이 권한에 사용할 수 있는 설정은 다음과 같습니다.

- * 허용 *: 클라이언트가 개체를 덮어쓸 수 있습니다. 기본 설정입니다.
- * 거부 *: 클라이언트가 개체를 덮어쓸 수 없습니다. Deny 로 설정된 경우 PutOverwriteObject 권한은 다음과 같이 작동합니다.
  - 기존 객체가 같은 경로에 있는 경우:
    - 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태깅을 덮어쓸 수 없습니다.
    - 진행 중인 모든 수집 작업이 취소되고 오류가 반환됩니다.
    - S3 버전 관리가 활성화된 경우 거부 설정을 사용하면 개체 태그 지정 또는 개체 삭제 태그 지정 작업에서 개체 및 현재 버전이 아닌 개체의 TagSet을 수정할 수 없습니다.
  - 기존 개체를 찾을 수 없으면 이 권한은 적용되지 않습니다.
- 이 권한이 없으면 Allow가 설정된 것과 효과가 같습니다.

> 현재 S3 정책이 덮어쓰기를 허용하고 PutOverwriteObject 권한이 Deny 로 설정된 경우 클라이언트는 개체의 데이터, 사용자 정의 메타데이터 또는 개체 태그를 덮어쓸 수 없습니다. 또한 * 클라이언트 수정 방지 * 확인란이 선택된 경우(* 구성 * > * 그리드 옵션 *) 해당 설정은 PutOverwriteObject 권한 설정보다 우선합니다.

관련 정보

"S3 그룹 정책의 예"

정책에서 조건 지정

조건은 정책이 적용되는 시점을 정의합니다. 조건은 연산자 및 키 값 쌍으로 구성됩니다.

조건은 평가에 키 값 쌍을 사용합니다. 조건 요소에는 여러 조건이 포함될 수 있으며 각 조건에는 여러 키 값 쌍이 포함될 수 있습니다. 조건 블럭은 다음 형식을 사용합니다:

```
Condition: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

다음 예제에서 IPAddress 조건은 SOURCEIP 조건 키를 사용합니다.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

지원되는 조건 연산자

조건 연산자는 다음과 같이 분류됩니다.

- 문자열
- 숫자
- 부울
- IP 주소입니다
- Null 확인

조건 연산자	설명
StringEquals	정확한 일치(대/소문자 구분)를 기반으로 문자열 값과 키를 비교합니다.
StringNotEquals	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다.
StringEqualsIgnoreCase 를 참조하십시오	정확한 일치를 기준으로 문자열 값과 키를 비교합니다(대/소문자 무시).

조건 연산자	설명
StringNotEqualsIgnoreCase 를 참조하십시오	Negated matching (대소문자 무시)을 기준으로 문자열 값과 키를 비교합니다.
StringLike 를 선택합니다	정확한 일치(대/소문자 구분)를 기반으로 문자열 값과 키를 비교합니다. 및 * 를 포함할 수 있습니까? 와일드카드 문자.
StringNotLike 를 참조하십시오	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다. 및 * 를 포함할 수 있습니까? 와일드카드 문자.
NumericEquals	정확한 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericNotEquals	키를 부정 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThan	키를 ""보다 큼"" 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThanEquals	키를 ""크거나 같음"" 일치를 기준으로 숫자 값과 비교합니다.
NumericLessThan	""보다 작음" 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericLessThanEquals	키를 ""보다 작음 또는 같음" 일치를 기준으로 숫자 값과 비교합니다.
불입니다	"true 또는 false" 일치를 기준으로 키를 부울 값과 비교합니다.
IP 주소	키를 IP 주소 또는 IP 주소 범위와 비교합니다.
NotIpAddress 를 참조하십시오	부정 일치를 기준으로 IP 주소 또는 IP 주소 범위와 키를 비교합니다.
null입니다	현재 요청 컨텍스트에 조건 키가 있는지 확인합니다.

지원되는 조건 키

범주	적용 가능한 조건 키	설명
IP 연산자	AWS: SOURCEIP	요청이 전송된 IP 주소와 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다. • 참고: * S3 요청이 관리 노드 및 게이트웨이 노드의 로드 밸런서 서비스를 통해 전송된 경우 로드 밸런서 서비스의 IP 주소 업스트림과 비교됩니다. • 참고 *: 타사, 비투명 로드 밸런서가 사용되는 경우 이 로드 밸런서의 IP 주소와 비교합니다. 모두 `X-Forwarded-For` 헤더의 유효성을 확인할 수 없기 때문에 헤더가 무시됩니다.
리소스/ID입니다	AWS: 사용자 이름	요청이 전송된 보낸 사람의 사용자 이름과 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 구분 기호	버킷 가져오기 또는 버킷 오브젝트 버전 가져오기 요청에 지정된 구분 기호 매개변수와 비교합니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 최대 키	버킷 가져오기 또는 버킷 객체 버전 가져오기 요청에 지정된 최대 키 매개변수와 비교합니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 접두어	Get Bucket 또는 Get Bucket Object Versions 요청에 지정된 접두사 매개변수와 비교합니다.

정책에서 변수 지정

정책의 변수를 사용하여 사용 가능한 정책 정보를 채울 수 있습니다. 에서 정책 변수를 사용할 수 있습니다 `Resource` 의 요소 및 문자열 비교 `Condition` 요소.

이 예제에서 변수는 입니다 `${aws:username}` 은(는) Resource 요소의 일부입니다.

```
"Resource": "arn:aws:s3:::_bucket-name/home_/${aws:username}/*"
```

이 예제에서 변수는 입니다 `${aws:username}` 조건 블럭의 조건 값의 일부입니다:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

변수	설명
`${aws:SourceIp}`	SOURCEIP 키를 제공된 변수로 사용합니다.
`${aws:username}`	제공된 변수로 사용자 이름 키를 사용합니다.
`${s3:prefix}`	서비스별 prefix key를 제공된 variable 로 사용한다.
`${s3:max-keys}`	서비스별 최대 키 키를 제공된 변수로 사용합니다.
`${*}`	특수 문자. 문자를 리터럴 * 문자로 사용합니다.
`${?}`	특수 문자. 문자를 리터럴로 사용합니까? 문자.
`${$}`	특수 문자. 문자를 리터럴 $ 문자로 사용합니다.

특별한 처리가 필요한 정책 생성

때로는 정책에 따라 보안이 위험하거나 계정 루트 사용자를 잠그는 등 지속적인 작업에 위험한 사용 권한을 부여할 수 있습니다. StorageGRID S3 REST API 구현은 Amazon보다 정책 검증 중에 덜 제한적이지만 정책 평가 중에도 동일하게 엄격합니다.

정책 설명입니다	정책 유형입니다	아마존 행동	**StorageGRID** 동작
루트 계정에 대한 모든 권한을 스스로 거부합니다	버킷	유효하고 적용되지만 루트 사용자 계정은 모든 S3 버킷 정책 작업에 대한 권한을 보유합니다	동일합니다
사용자/그룹에 대한 모든 권한을 스스로 거부합니다	그룹	유효하고 시행되었습니다	동일합니다
외부 계정 그룹에 모든 권한을 허용합니다	버킷	주체가 잘못되었습니다	유효하지만 모든 S3 버킷 정책 작업에 대한 권한은 정책에서 허용하는 경우 405 메서드 허용되지 않음 오류를 반환합니다

정책 설명입니다	정책 유형입니다	아마존 행동	**StorageGRID** 동작
외부 계정 루트 또는 사용자에게 모든 권한을 허용합니다	버킷	유효하지만 모든 S3 버킷 정책 작업에 대한 권한은 정책에서 허용하는 경우 405 메서드 허용되지 않음 오류를 반환합니다	동일합니다
모든 사용자에게 모든 작업에 대한 사용 권한을 허용합니다	버킷	유효하지만 모든 S3 버킷 정책 작업에 대한 사용 권한이 외국 계정 루트 및 사용자에 대해 405 메서드 허용 안 됨 오류를 반환합니다	동일합니다
모든 작업에 대한 모든 사용자의 권한을 거부합니다	버킷	유효하고 적용되지만 루트 사용자 계정은 모든 S3 버킷 정책 작업에 대한 권한을 보유합니다	동일합니다
보안 주체는 존재하지 않는 사용자 또는 그룹입니다	버킷	주체가 잘못되었습니다	유효합니다
리소스가 존재하지 않는 S3 버킷입니다	그룹	유효합니다	동일합니다
보안 주체는 로컬 그룹입니다	버킷	주체가 잘못되었습니다	유효합니다
정책은 개체를 넣을 수 있는 비소유자 계정(익명 계정 포함) 권한을 부여합니다	버킷	유효합니다. 객체는 생성자 계정이 소유하며 버킷 정책은 적용되지 않습니다. 생성자 계정은 개체 ACL을 사용하여 개체에 대한 액세스 권한을 부여해야 합니다.	유효합니다. 오브젝트는 버킷 소유자 계정이 소유합니다. 버킷 정책이 적용됩니다.

WORM(Write-Once-Read-Many) 보호

WORM(Write-Once-Read-Many) 버킷을 생성하여 데이터, 사용자 정의 오브젝트 메타데이터 및 S3 오브젝트 태깅을 보호할 수 있습니다. 새 객체를 생성하고 기존 컨텐츠를 덮어쓰거나 삭제하지 못하도록 WORM 버킷을 구성합니다. 여기에 설명된 방법 중 하나를 사용합니다.

덮어쓰기가 항상 거부되도록 하려면 다음을 수행할 수 있습니다.

- Grid Manager에서 * 구성 * > * 그리드 옵션 * 으로 이동하여 * 클라이언트 수정 방지 * 확인란을 선택합니다.
- 다음 규칙 및 S3 정책을 적용합니다.
  - S3 정책에 PutOverwriteObject 거부 작업을 추가합니다.

◦ DeleteObject 거부 작업을 S3 정책에 추가합니다.

◦ S3 정책에 오브젝트 허용(Put Object Allow) 작업을 추가합니다.

> S3 정책에서 DeleteObject 를 deny 로 설정해도 ""30일 후 0개 복사본""과 같은 규칙이 있을 때 ILM이 개체를 삭제하는 것을 차단하지 않습니다.

> 이러한 규칙과 정책이 모두 적용되더라도 동시 쓰기를 방지하지 않습니다(상황 A 참조). 순차적 완료된 덮어쓰기를 방지합니다(상황 B 참조).

- 상황 A *: 동시 쓰기(보호 안 됨)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 상황 B *: 순차적 완료된 덮어쓰기(방지됨)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

관련 정보

"ILM을 사용하여 개체를 관리합니다"

"특별한 처리가 필요한 정책 생성"

"StorageGRID ILM 규칙이 개체를 관리하는 방법"

"S3 그룹 정책의 예"

S3 정책 예

이 섹션의 예를 사용하여 버킷 및 그룹에 대한 StorageGRID 액세스 정책을 구축합니다.

S3 버킷 정책의 예

버킷 정책은 정책이 연결된 버킷에 대한 액세스 권한을 지정합니다. 버킷 정책은 S3 PutBucketPolicy API를 사용하여 구성됩니다.

다음 명령에 따라 AWS CLI를 사용하여 버킷 정책을 구성할 수 있습니다.

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

예: 모든 사용자가 버킷에 읽기 전용 액세스를 허용합니다

이 예제에서는 anonymous 를 비롯한 모든 사람이 버킷에 있는 오브젝트를 나열하고 버킷에 있는 모든 오브젝트에 대해 오브젝트 가져오기 작업을 수행할 수 있습니다. 다른 모든 작업은 거부됩니다. 이 정책은 계정 루트 외에는 버킷에 쓸 수 있는 권한이 없으므로 특히 유용하지 않을 수 있습니다.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

예: 한 계정의 모든 사용자가 완전히 액세스할 수 있도록 허용하고 다른 계정의 모든 사용자는 버킷에 읽기 전용으로 액세스할 수 있습니다

이 예제에서는 지정된 계정의 모든 사용자가 버킷에 완전히 액세스할 수 있지만, 지정된 다른 계정의 모든 사용자는 버킷을 나열하고 으로 시작하는 버킷의 개체에 대해 GetObject 작업만 수행할 수 있습니다 `shared/` 개체 키 접두사입니다.

StorageGRID에서 비소유자 계정(익명 계정 포함)으로 생성된 객체는 버킷 소유자 계정이 소유합니다. 버킷 정책은 이러한 오브젝트에 적용됩니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

예: 모든 사용자가 버킷에 대한 읽기 전용 액세스 및 지정된 그룹에 의한 전체 액세스 허용

이 예제에서는 anonymous 를 포함한 모든 사용자가 버킷을 나열하고 버킷의 모든 오브젝트에 대해 오브젝트 가져오기 작업을 수행할 수 있지만 그룹에 속한 사용자만 수행할 수 있습니다 `Marketing` 지정된 계정에서 전체 액세스가 허용됩니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

예: 클라이언트가 **IP** 범위에 있는 경우 모든 사용자가 버킷에 대한 읽기 및 쓰기 액세스를 허용합니다

이 예제에서는 요청이 지정된 IP 범위(54.240.143.0 ~ 54.240.143.255, 54.240.143.188 제외)에서 발생한 경우 anonymous를 포함한 모든 사람이 버킷을 나열하고 버킷의 모든 오브젝트에 대해 오브젝트 작업을 수행할 수 있습니다. 다른 모든 작업이 거부되고 IP 범위를 벗어난 모든 요청이 거부됩니다.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

예: 지정된 통합 사용자가 단독으로 버킷을 완전히 액세스할 수 있도록 허용합니다

이 예에서는 페더레이션 사용자 Alex가 에 대한 전체 액세스를 허용합니다 `examplebucket` 버킷과 그 물체. "root"를 포함한 다른 모든 사용자는 모든 작업을 명시적으로 거부합니다. 그러나 "root"는 PUT/GET/DeleteBucketPolicy에 대한 권한이 거부되지 않습니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

예: **PutOverwriteObject** 권한

이 예에서 는 입니다 `Deny` PutOverwriteObject 및 DeleteObject 에 대한 효과 개체의 데이터, 사용자 정의 메타데이터 및 S3 개체 태그 지정을 덮어쓰거나 삭제할 수 없습니다.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

관련 정보

"버킷 작업"

S3 그룹 정책의 예

그룹 정책은 정책이 연결된 그룹에 대한 액세스 권한을 지정합니다. 아니요 `Principal` 암시적 정책이므로 정책의 요소입니다. 그룹 정책은 테넌트 관리자 또는 API를 사용하여 구성됩니다.

예: 테넌트 관리자를 사용하여 그룹 정책 설정

테넌트 관리자를 사용하여 그룹을 추가 또는 편집할 때 이 그룹의 S3 액세스 권한 구성원이 가질 그룹 정책을 생성하는

방법을 다음과 같이 선택할 수 있습니다.

- * S3 액세스 없음 *: 기본 옵션. 이 그룹의 사용자는 버킷 정책을 통해 액세스가 부여되지 않는 한 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
- * 읽기 전용 액세스 *: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
- * 전체 액세스 *: 이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
- * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다.

  이 예제에서 그룹의 구성원은 지정된 버킷의 특정 폴더(키 접두사)를 나열하고 액세스할 수만 있습니다.

예: 모든 버킷에 대한 그룹 전체 액세스 허용

이 예에서 그룹의 모든 구성원은 버킷 정책에 의해 명시적으로 거부되지 않는 한 테넌트 계정이 소유한 모든 버킷에 대해 전체 액세스가 허용됩니다.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

예: 모든 버킷에 대한 그룹 읽기 전용 액세스를 허용합니다

이 예제에서 그룹의 모든 구성원은 버킷 정책에 의해 명시적으로 거부되지 않는 한 S3 리소스에 대해 읽기 전용 액세스 권한을 갖습니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

예: 그룹 구성원이 버킷의 "" 폴더에만 완전히 액세스할 수 있도록 허용합니다

이 예제에서 그룹의 구성원은 지정된 버킷의 특정 폴더(키 접두사)를 나열하고 액세스할 수만 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

관련 정보

"테넌트 계정을 사용합니다"

"PutOverwriteObject 권한 사용"

"WORM(Write-Once-Read-Many) 보호"

REST API에 대한 보안 구성

REST API에 대해 구현된 보안 조치를 검토하고 시스템 보안 방법을 이해해야 합니다.

StorageGRID가 REST API에 보안을 제공하는 방법

StorageGRID 시스템이 REST API에 대한 보안, 인증 및 권한 부여를 구현하는 방법을 이해해야 합니다.

StorageGRID는 다음과 같은 보안 조치를 사용합니다.

- 로드 밸런서 끝점에 HTTPS가 구성되어 있는 경우 로드 밸런서 서비스와의 클라이언트 통신은 HTTPS를 사용합니다.

  로드 밸런서 끝점을 구성할 때 HTTP를 선택적으로 활성화할 수 있습니다. 예를 들어, 테스트 또는 기타 비운영 목적으로 HTTP를 사용할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

- 기본적으로 StorageGRID는 게이트웨이 노드에서 스토리지 노드 및 CLB 서비스와의 클라이언트 통신에

HTTPS를 사용합니다.

이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다. 예를 들어, 테스트 또는 기타 비운영 목적으로 HTTP를 사용할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

CLB 서비스는 더 이상 사용되지 않습니다.

- StorageGRID와 클라이언트 간의 통신은 TLS를 사용하여 암호화됩니다.
- 로드 밸런서 끝점이 HTTP 또는 HTTPS 연결을 허용하도록 구성되었는지 여부에 관계없이 그리드 내의 로드 밸런서 서비스와 스토리지 노드 간의 통신이 암호화됩니다.
- 클라이언트는 REST API 작업을 수행하기 위해 StorageGRID에 HTTP 인증 헤더를 제공해야 합니다.

보안 인증서 및 클라이언트 응용 프로그램

클라이언트는 게이트웨이 노드 또는 관리 노드의 로드 밸런서 서비스, 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 직접 연결할 수 있습니다.

모든 경우에 클라이언트 응용 프로그램은 그리드 관리자가 업로드한 사용자 지정 서버 인증서 또는 StorageGRID 시스템에서 생성한 인증서를 사용하여 TLS 연결을 만들 수 있습니다.

- 클라이언트 응용 프로그램이 로드 밸런서 서비스에 연결되면 연결을 만드는 데 사용되는 특정 로드 밸런서 끝점에 대해 구성된 인증서를 사용합니다. 각 끝점마다 고유한 인증서가 있습니다. 이 인증서는 그리드 관리자가 업로드한 사용자 지정 서버 인증서이거나, 끝점 구성 시 그리드 관리자가 StorageGRID에서 생성한 인증서입니다.
- 클라이언트 응용 프로그램이 게이트웨이 노드의 스토리지 노드 또는 CLB 서비스에 직접 연결할 때 StorageGRID 시스템이 설치될 때 스토리지 노드에 대해 생성된 시스템 생성 서버 인증서(시스템 인증 기관이 서명)를 사용합니다. 또는 그리드 관리자가 그리드에 제공하는 단일 사용자 정의 서버 인증서입니다.

클라이언트가 TLS 연결을 설정하는 데 사용하는 인증서를 신뢰하도록 구성해야 합니다.

로드 밸런서 끝점 구성에 대한 정보와 TLS 연결에 대한 단일 사용자 지정 서버 인증서를 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 직접 추가하는 방법에 대한 지침은 StorageGRID 관리 지침을 참조하십시오.

요약

다음 표에서는 S3 및 Swift REST API에서 보안 문제가 구현되는 방식을 보여 줍니다.

보안 문제	**REST API** 구현
연결 보안	TLS
서버 인증	시스템 CA에서 서명한 X.509 서버 인증서 또는 관리자가 제공한 사용자 지정 서버 인증서입니다
클라이언트 인증	• S3:S3 계정(액세스 키 ID 및 비밀 액세스 키) • Swift:Swift 계정(사용자 이름 및 암호)

보안 문제	**REST API** 구현
클라이언트 인증	• S3: 버킷 소유권 및 모든 적용 가능한 액세스 제어 정책 • Swift: 관리자 역할 액세스

관련 정보

"StorageGRID 관리"

TLS 라이브러리에 대해 지원되는 해시 및 암호화 알고리즘

StorageGRID 시스템은 TLS(전송 계층 보안) 세션을 설정할 때 클라이언트 응용 프로그램에서 사용할 수 있는 제한된 암호화 그룹 세트를 지원합니다.

지원되는 TLS 버전입니다

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

SSLv3 및 TLS 1.1(또는 이전 버전)은 더 이상 지원되지 않습니다.

지원되는 암호 그룹

TLS 버전입니다	암호화 그룹의 **IANA** 이름입니다
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHACH20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHACH20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

더 이상 사용되지 않는 암호화 그룹

다음 암호화 그룹은 더 이상 사용되지 않습니다. 이러한 암호화에 대한 지원은 이후 릴리스에서 제거됩니다.

IANA 이름입니다
TLS_RSA_with_AES_128_GCM_SHA256
TLS_RSA_WITED_AES_256_GCM_SHA384

관련 정보

"클라이언트 연결 구성 방법"

작업 모니터링 및 감사

전체 그리드 또는 특정 노드에 대한 트랜잭션 추세를 확인하여 클라이언트 작업의 워크로드 및 효율성을 모니터링할 수 있습니다. 감사 메시지를 사용하여 클라이언트 작업 및 트랜잭션을 모니터링할 수 있습니다.

- "오브젝트 수집 및 검색 속도 모니터링"
- "감사 로그 액세스 및 검토"

오브젝트 수집 및 검색 속도 모니터링

오브젝트 수집 및 검색 속도와 오브젝트 수, 쿼리, 검증을 위한 메트릭을 모니터링할 수 있습니다. 클라이언트 응용 프로그램이 StorageGRID 시스템에서 개체를 읽고, 쓰고, 수정하는 데 성공한 시도 및 실패한 시도 횟수를 볼 수 있습니다.

단계

1. 지원되는 브라우저를 사용하여 Grid Manager에 로그인합니다.
2. Dashboard에서 Protocol Operations 섹션을 찾습니다.

   이 섹션에서는 StorageGRID 시스템에서 수행하는 클라이언트 작업의 수를 요약합니다. 프로토콜 속도는 최근 2분 동안의 평균값입니다.

3. 노드 * 를 선택합니다.
4. 노드 홈 페이지(배포 수준)에서 * 로드 밸런서 * 탭을 클릭합니다.

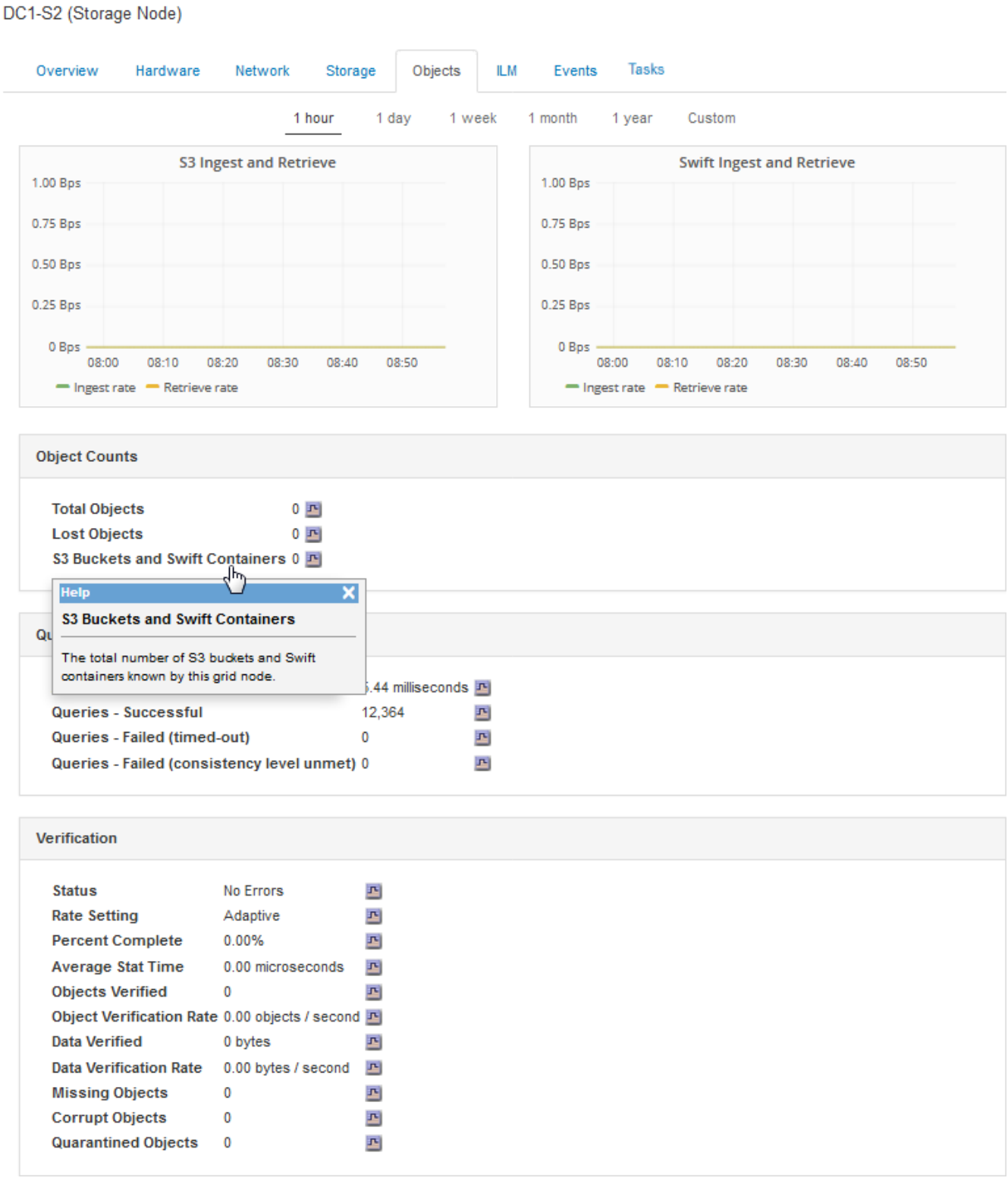
   차트에는 그리드 내의 로드 밸런서 끝점에 대한 모든 클라이언트 트래픽에 대한 추세가 표시됩니다. 시간 간격(시간, 일, 주, 월 또는 년)을 선택할 수 있습니다. 또는 사용자 지정 간격을 적용할 수 있습니다.

5. 노드 홈 페이지(배포 수준)에서 * 개체 * 탭을 클릭합니다.

   이 차트에는 전체 StorageGRID 시스템의 수집 및 검색 속도가 초당 바이트 및 총 바이트 단위로 표시됩니다. 시간 간격(시간, 일, 주, 월 또는 년)을 선택할 수 있습니다. 또는 사용자 지정 간격을 적용할 수 있습니다.

6. 특정 스토리지 노드에 대한 정보를 보려면 왼쪽의 목록에서 노드를 선택하고 * Objects * 탭을 클릭합니다.

   이 차트에는 이 스토리지 노드의 객체 수집 및 검색 속도가 나와 있습니다. 이 탭에는 개체 수, 쿼리 및 검증에 대한 메트릭도 포함되어 있습니다. 레이블을 클릭하여 이러한 메트릭의 정의를 볼 수 있습니다.



7. 더 자세한 내용을 원하는 경우:
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. site_ * > * Overview * > * Main * 을 선택합니다.

      API 작업 섹션에는 전체 그리드에 대한 요약 정보가 표시됩니다.

c. 스토리지 노드 * > * LDR * > *_CLIENT APPLICATION_ * > * Overview * > * Main * 을 선택합니다

작업 섹션에는 선택한 스토리지 노드에 대한 요약 정보가 표시됩니다.

감사 로그 액세스 및 검토

감사 메시지는 StorageGRID 서비스에서 생성되고 텍스트 로그 파일에 저장됩니다. 감사 로그의 API 관련 감사 메시지는 시스템의 상태를 평가하는 데 도움이 되는 중요한 보안, 운영 및 성능 모니터링 데이터를 제공합니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 에 가 있어야 합니다 `Passwords.txt` 파일.
- 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

활성 감사 로그 파일의 이름은 입니다 `audit.log`, 및 은 관리 노드에 저장됩니다.

하루에 한 번 활성 audit.log 파일이 저장되고 새 파일이 저장됩니다 `audit.log` 파일이 시작되었습니다. 저장된 파일의 이름은 저장 시기를 형식으로 나타냅니다 *`yyyy-mm-dd.txt`*.

하루 후에는 저장된 파일이 압축되고 이름이 파일 형식으로 변경됩니다 `*yyyy-mm-dd.txt.gz*`원래 날짜를 유지합니다.

이 예제에서는 활성 을 보여 줍니다 `audit.log` 파일, 이전 날짜의 파일입니다 (`2018-04-15.txt`), 및 이전 날짜의 압축 파일 (`2018-04-14.txt.gz`)를 클릭합니다.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다.
      `ssh admin@primary_Admin_Node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
2. 감사 로그 파일이 포함된 디렉토리로 이동합니다.

   ```
   cd /var/local/audit/export
   ```

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

감사 로그에서 **S3** 작업을 추적했습니다

StorageGRID 감사 로그에서 여러 버킷 작업 및 오브젝트 작업을 추적합니다.

감사 로그에서 버킷 작업을 추적했습니다

- 버킷 삭제
- 버킷 태그 지정을 삭제합니다
- 여러 개체를 삭제합니다
- 버킷 가져오기(객체 나열)
- 버킷 객체 버전을 가져옵니다
- 버킷 태그 지정을 가져옵니다
- 헤드 버킷
- 버킷 을 놓습니다
- 버킷 규정 준수
- Bucket 태그 달기
- 버킷 버전 관리

감사 로그에서 추적된 객체 작업입니다

- 멀티파트 업로드를 완료합니다
- 파트 업로드(ILM 규칙이 Strict 또는 Balanced 수집 동작을 사용하는 경우)
- Upload Part-Copy (ILM 규칙이 Strict 또는 Balanced 수집 동작을 사용하는 경우)
- 개체 삭제
- 객체 가져오기
- 헤드 개체
- 사후 개체 복원
- 개체 를 넣습니다
- 개체 - 복사 를 선택합니다

관련 정보

"버킷 작업"

"객체에 대한 작업"

활성, 유휴 및 동시 **HTTP** 연결의 이점

HTTP 연결을 구성하는 방법은 StorageGRID 시스템의 성능에 영향을 줄 수 있습니다. 구성은 HTTP 연결이 활성 상태인지 유휴 상태인지 또는 여러 개의 동시 연결이 있는지 여부에 따라 달라집니다.

다음과 같은 유형의 HTTP 연결에 대한 성능 이점을 확인할 수 있습니다.

- 유휴 HTTP 연결
- 활성 HTTP 연결

- 동시 HTTP 연결

관련 정보

- "유휴 HTTP 연결을 열어 두면 얻을 수 있는 이점"
- "활성 HTTP 연결의 이점"
- "동시 HTTP 연결의 이점"
- "읽기 및 쓰기 작업을 위한 HTTP 연결 풀 분리"

유휴 **HTTP** 연결을 열어 두면 얻을 수 있는 이점

클라이언트 응용 프로그램이 열려 있는 연결을 통해 후속 트랜잭션을 수행할 수 있도록 클라이언트 응용 프로그램이 유휴 상태인 경우에도 HTTP 연결을 열어 두어야 합니다. 시스템 측정 및 통합 경험을 바탕으로 유휴 HTTP 연결을 최대 10분 동안 열어 두어야 합니다. StorageGRID는 열려 있고 10분 이상 유휴 상태로 유지되는 HTTP 연결을 자동으로 닫을 수 있습니다.

개방 및 유휴 HTTP 연결은 다음과 같은 이점을 제공합니다.

- StorageGRID 시스템이 HTTP 트랜잭션을 수행해야 한다고 결정하는 시간부터 StorageGRID 시스템이 트랜잭션을 수행할 수 있는 시간까지 지연 시간을 줄였습니다

  지연 시간 감소는 특히 TCP/IP 및 TLS 연결을 설정하는 데 필요한 시간의 주요 장점입니다.

- 이전에 수행된 전송을 사용하여 TCP/IP 저속 시작 알고리즘을 프라이밍하여 데이터 전송 속도를 높였습니다
- 클라이언트 응용 프로그램과 StorageGRID 시스템 간의 연결을 중단하는 여러 가지 장애 조건에 대한 즉각적인 알림

유휴 연결을 유지하는 기간을 결정하는 것은 기존 연결과 관련된 느린 시작의 이점과 내부 시스템 리소스에 대한 연결의 이상적인 할당을 절충하는 것입니다.

활성 **HTTP** 연결의 이점

스토리지 노드 또는 게이트웨이 노드의 CLB 서비스(더 이상 사용되지 않음)에 직접 연결하는 경우 HTTP 연결이 지속적으로 트랜잭션을 수행하더라도 활성 HTTP 연결 기간을 최대 10분으로 제한해야 합니다.

연결을 열어 두어야 하는 최대 기간을 결정하는 것은 연결 지속성의 이점과 내부 시스템 리소스에 대한 연결을 이상적으로 할당하는 것입니다.

클라이언트가 스토리지 노드 또는 CLB 서비스에 접속할 경우 활성 HTTP 연결을 제한하면 다음과 같은 이점이 있습니다.

- StorageGRID 시스템 전체에서 최적의 로드 밸런싱을 지원합니다.

  CLB 서비스를 사용할 때는 오래 지속되는 TCP/IP 연결을 방지하여 StorageGRID 시스템 전체의 로드 밸런싱을 최적화해야 합니다. HTTP 연결을 다시 설정하고 재조정할 수 있도록 클라이언트 응용 프로그램을 구성하여 각 HTTP 연결 기간을 추적하고 설정된 시간 후에 HTTP 연결을 닫아야 합니다.

CLB 서비스는 클라이언트 응용 프로그램이 HTTP 연결을 설정할 때 StorageGRID 시스템 전체의 로드 균형을 조정합니다. 시간이 지남에 따라 로드 밸런싱 요구 사항이 변경됨에 따라 HTTP 연결이 더 이상 최적화되지 않을 수 있습니다. 시스템은 클라이언트 애플리케이션이 각 트랜잭션에 대해 별도의 HTTP 연결을 설정할 때 최상의 로드 밸런싱을 수행하지만, 이 경우 영구 연결과 관련된 훨씬 더 가치 있는 이득을 얻을 수 없습니다.

CLB 서비스는 더 이상 사용되지 않습니다.

- 클라이언트 응용 프로그램이 사용 가능한 공간이 있는 LDR 서비스로 HTTP 트랜잭션을 보낼 수 있도록 합니다.
- 유지보수 절차를 시작할 수 있습니다.

  일부 유지 관리 절차는 진행 중인 모든 HTTP 연결이 완료된 후에만 시작됩니다.

부하 분산 서비스에 대한 클라이언트 연결의 경우 일부 유지 관리 절차를 즉시 시작할 수 있도록 개방 연결 기간을 제한하는 것이 유용할 수 있습니다. 클라이언트 연결 기간이 제한되지 않으면 활성 연결이 자동으로 종료되는 데 몇 분이 걸릴 수 있습니다.

동시 **HTTP** 연결의 이점

병렬 처리를 허용하도록 StorageGRID 시스템에 대한 여러 TCP/IP 연결을 열린 상태로 유지하여 성능을 향상시켜야 합니다. 최적의 병렬 연결 수는 다양한 요인에 따라 달라집니다.

동시 HTTP 연결은 다음과 같은 이점을 제공합니다.

- 지연 시간 단축

  다른 트랜잭션이 완료될 때까지 기다리지 않고 즉시 트랜잭션을 시작할 수 있습니다.

- 처리량 향상

  StorageGRID 시스템은 병렬 트랜잭션을 수행하고 총 트랜잭션 처리량을 늘릴 수 있습니다.

클라이언트 응용 프로그램은 여러 HTTP 연결을 설정해야 합니다. 클라이언트 응용 프로그램은 트랜잭션을 수행해야 하는 경우 트랜잭션을 현재 처리하지 않는 설정된 연결을 선택하여 즉시 사용할 수 있습니다.

각 StorageGRID 시스템의 토폴로지에는 성능이 저하되기 전에 동시 트랜잭션 및 연결에 대해 서로 다른 최대 처리량이 있습니다. 최대 처리량은 컴퓨팅 리소스, 네트워크 리소스, 스토리지 리소스, WAN 링크 등의 요인에 따라 달라집니다. StorageGRID 시스템에서 지원하는 서버 및 서비스 수와 애플리케이션 수도 고려해야 합니다.

StorageGRID 시스템은 종종 여러 클라이언트 애플리케이션을 지원합니다. 클라이언트 응용 프로그램에서 사용하는 최대 동시 연결 수를 결정할 때 이 점에 유의해야 합니다. 클라이언트 응용 프로그램이 StorageGRID 시스템에 대한 연결을 설정하는 여러 소프트웨어 엔터티로 구성된 경우 엔터티에 대한 모든 연결을 추가해야 합니다. 다음과 같은 경우 최대 동시 연결 수를 조정해야 할 수 있습니다.

- StorageGRID 시스템의 토폴로지는 시스템에서 지원할 수 있는 최대 동시 트랜잭션 및 연결 수에 영향을 줍니다.
- 대역폭이 제한된 네트워크에서 StorageGRID 시스템과 상호 작용하는 클라이언트 응용 프로그램은 개별 트랜잭션이 적절한 시간 내에 완료되도록 동시성 정도를 줄여야 할 수 있습니다.
- 많은 클라이언트 응용 프로그램이 StorageGRID 시스템을 공유하는 경우 시스템의 제한을 초과하지 않도록 동시성 정도를 줄여야 할 수 있습니다.

읽기 및 쓰기 작업을 위한 **HTTP** 연결 풀 분리

읽기 및 쓰기 작업에 별도의 HTTP 연결 풀을 사용하고 각 풀에 사용할 풀 수를 제어할 수 있습니다. 별도의 HTTP 연결 풀을 통해 트랜잭션을 보다 효율적으로 제어하고 로드 밸런싱을 수행할 수 있습니다.

클라이언트 애플리케이션은 검색 가능(읽기) 또는 저장 가능(쓰기) 부하를 생성할 수 있습니다. 읽기 및 쓰기 트랜잭션을 위한 별도의 HTTP 연결 풀을 사용하여 읽기 또는 쓰기 트랜잭션에 사용할 각 풀의 양을 조정할 수 있습니다.