



Amazon S3 REST API 지원 StorageGRID

NetApp
March 12, 2025

목차

Amazon S3 REST API 지원	1
S3 REST API 구현 세부 정보	1
날짜 처리	1
공통 요청 헤더	1
공통 응답 헤더	1
요청을 인증합니다	2
HTTP 인증 헤더를 사용합니다	2
쿼리 매개 변수를 사용합니다	2
서비스에 대한 작업	2
버킷 작업	2
객체에 대한 작업	10
객체에 대한 작업	10
S3 Select를 사용합니다	13
서버측 암호화를 사용합니다	16
CopyObject 를 선택합니다	18
GetObject 를 참조하십시오	22
HeadObject 를 선택합니다	24
PutObject 를 선택합니다	27
RestoreObject 를 선택합니다	32
SelectObjectContent 를 선택합니다	33
멀티파트 업로드 작업	38
멀티파트 업로드 작업	38
CompleteMultipartUpload를 클릭합니다	39
CreateMultptUpload 를 클릭합니다	41
ListMultipartUploads 를 참조하십시오	44
업로드 파트	44
업로드파트 복사	45
오류 응답	46
지원되는 S3 API 오류 코드입니다	46
StorageGRID 사용자 지정 오류 코드	48

Amazon S3 REST API 지원

S3 REST API 구현 세부 정보

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.

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). 요청에 헤더를 포함하면 `x-amz-date` 날짜 요청 헤더에 지정된 모든 값이 재정의됩니다. AWS Signature 버전 4를 사용할 `x-amz-date` 경우 날짜 헤더가 지원되지 않으므로 서명된 요청에 헤더가 있어야 합니다.

공통 요청 헤더

StorageGRID 시스템은 한 가지 예외를 제외하고 에서 정의한 일반 요청 헤더를 ["Amazon Simple Storage Service API 참조: 일반 요청 헤더"](#) 지원합니다.

요청 헤더	구축
권한 부여	AWS Signature 버전 2에 대한 전체 지원 다음 경우를 제외하고 AWS Signature 버전 4 지원: <ul style="list-style-type: none">에서 실제 페이로드 체크섬 값을 <code>x-amz-content-sha256</code> 제공하면 헤더에 값이 제공된 것처럼 값이 유효성 검사 없이 수락됩니다. UNSIGNED-PAYLOAD 스트리밍을 의미하는 헤더 값 <code>aws-chunked</code>(예: <code>streaming-AWS4-HMAC-SHA256</code> 페이로드)을 제공하면 <code>x-amz-content-sha256</code> 체크 데이터에 대해 체크 서명이 확인되지 않습니다.
X-amz-security-token	구현되지 않았습니다. `XNotImplemented`를 반환합니다.

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

요청을 인증합니다

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 HTTP 헤더와 쿼리 매개 변수 사용이라는 두 가지 인증 방법을 `Authorization` 지원합니다.

HTTP 인증 헤더를 사용합니다

HTTP `Authorization` 헤더는 버킷 정책에서 허용하는 익명 요청을 제외하고 모든 S3 API 작업에서 사용됩니다. `'Authorization'` 헤더에는 요청을 인증하는 데 필요한 모든 서명 정보가 들어 있습니다.

쿼리 매개 변수를 사용합니다

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 없으며, 이를 통해 타사에 리소스에 대한 제한된 액세스를 제공할 수 있습니다.

서비스에 대한 작업

StorageGRID 시스템은 서비스에 대해 다음 작업을 지원합니다.

작동	구축
ListBucket (이전 명칭: Get Service)	모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.
스토리지 사용량을 가져옵니다	StorageGRID " 스토리지 사용량을 가져옵니다 " 요청에서는 계정에 의해 사용 중인 총 저장소 양과 계정에 연결된 각 버킷에 대해 알려줍니다. 이 작업은 <code>/</code> 의 경로와 사용자 지정 쿼리 매개 변수(<code>?x-ntap-sg-usage</code>)가 추가된 서비스에 대한 작업입니다.
옵션 <code>/</code>	클라이언트 애플리케이션은 스토리지 노드의 사용 가능 여부를 확인하기 위해 S3 인증 자격 증명을 제공하지 않고 스토리지 노드의 S3 포트에 요청을 전송할 수 있습니다 <code>OPTIONS /</code> . 이 요청을 사용하여 모니터링을 수행하거나, 외부 로드 밸런서가 스토리지 노드가 다운된 시점을 식별하도록 할 수 있습니다.

버킷 작업

StorageGRID 시스템은 각 S3 테넌트 계정에 대해 최대 5,000개의 버킷을 지원합니다.

각 그리드에는 최대 100,000개의 버킷을 포함할 수 있습니다.

5,000개의 버킷을 지원하려면 그리드의 각 스토리지 노드에 최소 64GB의 RAM이 있어야 합니다.

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

자세한 내용은 다음을 참조하십시오.

- ["Amazon Simple Storage Service 사용자 가이드: 버킷 할당량, 제한 및 제한 사항"](#)
- ["S3 끝점 도메인 이름을 구성합니다"](#)

ListObjects(Get Bucket) 및 ListObjectVersions(Get Bucket 개체 버전) 작업은 StorageGRID를 ["일관성 값"](#) 지원합니다.

개별 버킷에 대해 마지막 액세스 시간에 대한 업데이트가 설정되었는지 여부를 확인할 수 있습니다. 을 ["버킷 최종 액세스 시간 가져오기"](#)참조하십시오.

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

작동	구축
CreateBucket	<p>새 버킷을 생성합니다. 버킷을 만들면 버킷 소유자가 됩니다.</p> <ul style="list-style-type: none"> • 버킷 이름은 다음 규칙을 준수해야 합니다. <ul style="list-style-type: none"> ◦ 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 지역에 생성되지만 us-east-1 요청 본문의 요청 요소를 사용하여 다른 영역을 지정할 수 LocationConstraint 있습니다. 요소를 사용할 때는 LocationConstraint 그리드 관리자 또는 그리드 관리 API를 사용하여 정의된 영역의 정확한 이름을 지정해야 합니다. 사용할 지역 이름을 모르는 경우 시스템 관리자에게 문의하십시오. <p>참고: CreateBucket 요청이 StorageGRID에 정의되지 않은 영역을 사용하는 경우 오류가 발생합니다.</p> <ul style="list-style-type: none"> • 요청 헤더를 포함하여 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 x-amz-bucket-object-lock-enabled 있습니다. 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오. <p>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.</p>
삭제 버킷	버킷을 삭제합니다.
DeleteBucketCors	버킷에 대한 CORS 구성을 삭제합니다.
DeleteBucketEncryption	버킷에서 기본 암호화를 삭제합니다. 암호화된 기존 개체는 암호화된 상태로 유지되지만 버킷에 추가된 새 개체는 암호화되지 않습니다.
DeleteBucketLifecycle	버킷에서 문서 수정 상태 설정을 삭제합니다. 을 "S3 라이프사이클 구성을 생성합니다" 참조하십시오.
DeleteBucketPolicy를 참조하십시오	버킷에 연결된 정책을 삭제합니다.

작동	구축
DeleteBuckReplication 을 참조하십시오	버킷에 연결된 복제 구성을 삭제합니다.
삭제 BucketTagging	하위 리소스를 사용하여 tagging 버킷에서 모든 태그를 제거합니다. 주의: 이 버킷에 대해 기본값이 아닌 ILM 정책 태그가 설정된 경우 이 버킷에 NTAP-SG-ILM-BUCKET-TAG 할당된 값이 있는 버킷 태그가 있습니다. 버킷 태그가 있는 경우 DeleteBucketTagging 요청을 NTAP-SG-ILM-BUCKET-TAG 실행하지 마십시오. 대신 태그 및 할당된 값만 사용하여 PutBucketTagging 요청을 NTAP-SG-ILM-BUCKET-TAG 실행하여 버킷에서 다른 모든 태그를 제거합니다. 버킷 태그를 수정하거나 제거하지 NTAP-SG-ILM-BUCKET-TAG 마십시오.
GetBucketAcl	양수 응답과 ID, DisplayName 및 버킷 소유자의 사용 권한을 반환합니다. 이는 소유자가 버킷에 대한 모든 액세스 권한을 가지고 있음을 나타냅니다.
GetBucketCors 를 참조하십시오	버킷의 구성을 반환합니다 cors.
GetBucketEncryption을 참조하십시오	버킷의 기본 암호화 구성을 반환합니다.
GetBuckLifecycleConfiguration 을 참조하십시오 (이전 명칭 Get Bucket 수명주기)	버킷의 수명주기 구성을 반환합니다. 을 "S3 라이프사이클 구성을 생성합니다" 참조하십시오.
GetBucketLocation 을 참조하십시오	CreateBucket 요청에서 요소를 사용하여 설정한 영역을 반환합니다 LocationConstraint. 버킷의 영역이 인 경우 us-east-1 영역에 대해 빈 문자열이 반환됩니다.
GetBuckNotificationConfiguration 을 참조하십시오 (이전 명칭 Get Bucket 알림)	버킷에 연결된 알림 구성을 반환합니다.
GetBucketPolicy를 참조하십시오	버킷에 연결된 정책을 반환합니다.
GetBucketReplication 을 참조하십시오	버킷에 연결된 복제 구성을 반환합니다.

작동	구축
GetBucketTagging	<p>하위 리소스를 사용하여 tagging 버킷의 모든 태그를 반환합니다.</p> <p>주의: 이 버킷에 대해 기본값이 아닌 ILM 정책 태그가 설정된 경우 이 버킷에 NTAP-SG-ILM-BUCKET-TAG 할당된 값이 있는 버킷 태그가 있습니다. 이 태그를 수정하거나 제거하지 마십시오.</p>
GetBucketVersioning 을 참조하십시오	<p>이 구현에서는 하위 리소스를 사용하여 versioning 버킷의 버전 관리 상태를 반환합니다.</p> <ul style="list-style-type: none"> • <i>blank</i>: 버전 관리가 활성화되지 않았습니다(버킷이 "버전 없음"). • 사용: 버전 관리가 활성화됩니다 • 일시 중단됨: 버전 관리가 이전에 활성화되었으며 일시 중단되었습니다
GetObjectLockConfiguration 을 참조하십시오	<p>구성된 경우 버킷 기본 보존 모드와 기본 보존 기간을 반환합니다.</p> <p>을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.</p>
머리버킷	<p>버킷이 존재하는지, 버킷에 액세스할 수 있는 권한이 있는지 확인합니다.</p> <p>이 작업은 다음을 반환합니다.</p> <ul style="list-style-type: none"> • x-ntap-sg-bucket-id: UUID 형식의 버킷의 UUID입니다. • x-ntap-sg-trace-id: 연결된 요청의 고유한 추적 ID입니다.
ListObjects 및 ListObjectsV2 를 참조하십시오 (이전 명칭 Get Bucket)	<p>버킷에 있는 오브젝트의 일부 또는 전체(최대 1,000개)를 반환합니다. 객체에 대한 스토리지 클래스는 스토리지가 스토리지 클래스 옵션으로 수집된 경우에도 두 값 중 하나를 가질 수 있습니다. REDUCED_REDUNDANCY</p> <ul style="list-style-type: none"> • `STANDARD` 객체가 스토리지 노드로 구성된 스토리지 풀에 저장되었음을 나타냅니다. • GLACIER- 클라우드 스토리지 풀에 지정된 외부 버킷으로 오브젝트가 이동되었음을 나타냅니다. <p>버킷에 접두사가 같은 삭제된 키가 많은 경우 키가 포함되지 않은 키가 응답에 포함될 수 <code>CommonPrefixes</code> 있습니다.</p>
ListObjectVersions 를 선택합니다 (이전에 명명된 Get Bucket Object 버전)	<p>버킷에서 읽기 권한을 가진 경우 이 작업을 하위 리소스와 함께 <code>versions</code> 사용하면 버킷에 있는 모든 오브젝트 버전의 메타데이터가 나열됩니다.</p>

작동	구축
BucketCors의	<p>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 사용하여 그래픽을 저장한다고 가정해 images 보겠습니다. 버킷에 대한 CORS 구성을 설정하면 images 해당 버킷의 이미지가 웹사이트에 표시되도록 할 수 http://www.example.com 있습니다.</p>
PutBucketEncryption을 참조하십시오	<p>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. 서버측 암호화 구성 규칙을 지정할 때 매개 변수를 로 AES256 설정하고 SSEAlgorithm 매개 변수를 사용하지 마십시오 KMSMasterKeyID.</p> <p>객체 업로드 요청이 이미 암호화를 지정한 경우(즉, 요청에 요청 헤더가 포함된 경우) 버킷 기본 암호화 구성은 x-amz-server-side-encryption-* 무시됩니다.</p>
PutBucketLifecycleConfiguration을 참조하십시오 (이전에 명명된 Put Bucket 수명 주기)	<p>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.</p> <ul style="list-style-type: none"> • 만료(일, 날짜, ExpiredObjectDeleteMarker) • 비currentVersionExpiration(NewerNoncurrentVersions, NoncurrentDays) • 필터(접두사, 태그) • 상태 • ID입니다 <p>StorageGRID는 다음 작업을 지원하지 않습니다.</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload를 중단합니다 • 전환 <p>을 "S3 라이프사이클 구성을 생성합니다"참조하십시오. 버킷 수명 주기의 만료 작업이 ILM 배치 지침과 상호 작용하는 방식을 이해하려면 을 참조하십시오."ILM이 개체 수명 전반에 걸쳐 작동하는 방식"</p> <ul style="list-style-type: none"> • 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
<p>PutBucketNotificationConfiguration을 참조하십시오</p> <p>(이전에 명명된 Put Bucket 알림)</p>	<p>요청 본문에 포함된 알림 구성 XML을 사용하여 버킷에 대한 알림을 구성합니다. 다음과 같은 구현 세부 사항에 유의해야 합니다.</p> <ul style="list-style-type: none"> • StorageGRID는 Amazon SNS(Simple Notification Service) 또는 Kafka 토픽을 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. <p>알림 설정을 성공적으로 하려면 끝점이 있어야 합니다. 끝점이 없으면 400 Bad Request 코드와 함께 오류가 InvalidArgument 반환됩니다.</p> <ul style="list-style-type: none"> • 다음 이벤트 유형에 대한 알림을 구성할 수 없습니다. 이러한 이벤트 유형은 * 지원되지 않습니다 *. <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed • StorageGRID에서 보낸 이벤트 알림은 다음 목록에 표시된 것처럼 일부 키를 포함하지 않고 다른 키에 대해 특정 값을 사용한다는 점을 제외하고 표준 JSON 형식을 사용합니다. <ul style="list-style-type: none"> ◦ * eventSource * 를 선택합니다 <pre>sgws:s3</pre> ◦ * awsRegion * <pre>포함되지 않음</pre> ◦ x-amz-id-2 * <pre>포함되지 않음</pre> ◦ * 표시 * <pre>urn:sgws:s3:::bucket_name</pre>
<p>BucketPolicy를 참조하십시오</p>	<p>버킷에 연결된 정책을 설정합니다. 을 "버킷 및 그룹 액세스 정책을 사용합니다" 참조하십시오.</p>

작동	구축
PutBucketReplication을 참조하십시오	<p>"StorageGRID CloudMirror 복제" 요청 본문에 제공된 복제 구성 XML을 사용하여 버킷을 구성합니다. CloudMirror 복제의 경우 다음과 같은 구축 세부 정보를 알고 있어야 합니다.</p> <ul style="list-style-type: none"> StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 요소 사용을 지원하지 않으며 <code>Filter</code> 객체 버전을 삭제하기 위한 V1 규칙을 따릅니다. 자세한 내용은 을 참조하십시오 "Amazon Simple Storage Service 사용 설명서: 복제 구성". 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. 을 "CloudMirror 복제를 구성합니다" 참조하십시오. <p>복제 구성이 성공하려면 엔드포인트가 있어야 합니다. 끝점이 없으면 요청이 A로 실패합니다 400 Bad Request. 오류 메시지는 다음과 같습니다. Unable to save the replication policy. The specified endpoint URN does not exist: URN.</p> <ul style="list-style-type: none"> 구성 XML에서 을 지정할 Role 필요는 없습니다. 이 값은 StorageGRID에서 사용되지 않으며 제출될 경우 무시됩니다. 구성 XML에서 스토리지 클래스를 생략하면 StorageGRID에서는 STANDARD 기본적으로 스토리지 클래스를 사용합니다. 소스 버킷에서 객체를 삭제하거나 소스 버킷 자체를 삭제하는 경우 지역 간 복제 동작은 다음과 같습니다. <ul style="list-style-type: none"> 복제되기 전에 오브젝트 또는 버킷을 삭제하면 객체/버킷이 복제되지 않으므로 사용자에게 통지되지 않습니다. 복제된 후 오브젝트 또는 버킷을 삭제하면 StorageGRID는 지역 간 복제 V1에 대한 표준 Amazon S3 삭제 동작을 따릅니다.

작동	구축
BucketTagging	<p>에서는 하위 리소스를 사용하여 tagging 버킷의 태그 집합을 추가하거나 업데이트합니다. 버킷 태그를 추가할 때 다음과 같은 제한 사항을 숙지하십시오.</p> <ul style="list-style-type: none"> • 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. <p>주의: 이 버킷에 대해 기본값이 아닌 ILM 정책 태그가 설정된 경우 이 버킷에 NTAP-SG-ILM-BUCKET-TAG 할당된 값이 있는 버킷 태그가 있습니다. `NTAP-SG-ILM-BUCKET-TAG` 버킷 태그가 모든 PutBucketTagging 요청에 할당된 값과 함께 포함되어 있는지 확인합니다. 이 태그를 수정하거나 제거하지 마십시오.</p> <p>참고: 이 작업은 버킷에 이미 있는 현재 태그를 덮어씁니다. 기존 태그를 세트에서 생략하면 해당 태그가 버킷에 대해 제거됩니다.</p>
PutBucketVersioning을 참조하십시오	<p>하위 리소스를 사용하여 versioning 기존 버킷의 버전 관리 상태를 설정합니다. 다음 값 중 하나를 사용하여 버전 관리 상태를 설정할 수 있습니다.</p> <ul style="list-style-type: none"> • 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 객체는 버전 ID를 `null` 받습니다.
PutObjectLockConfiguration을 참조하십시오	<p>버킷 기본 보존 모드 및 기본 보존 기간을 구성하거나 제거합니다.</p> <p>기본 보존 기간이 수정되면 기존 개체 버전의 보존 기한은 그대로 유지되며 새 기본 보존 기간을 사용하여 다시 계산되지 않습니다.</p> <p>자세한 내용은 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다" 참조하십시오.</p>

객체에 대한 작업

객체에 대한 작업

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

다음 조건은 모든 개체 작업에 적용됩니다.

- StorageGRID "일관성 값"은 다음과 같은 경우를 제외하고 개체의 모든 작업에서 지원됩니다.
 - GetObjectAcl

- OPTIONS /
- PutObjectLegalHold를 선택합니다
- PutObjectRetention
- SelectObjectContent 를 선택합니다
- 동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 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
DeleteObject 를 클릭합니다	<p>MFA(다중 요소 인증) 및 응답 헤더는 x-amz-mfa 지원되지 않습니다.</p> <p>DeleteObject 요청을 처리할 때 StorageGRID는 저장된 모든 위치에서 개체의 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.</p> <p>버전 관리</p> <p>특정 버전을 제거하려면 요청자가 버킷 소유자여야 하고 하위 리소스를 사용해야 versionId 합니다. 이 하위 리소스를 사용하면 버전이 영구적으로 삭제됩니다. 가 삭제 마커에 해당하는 경우 versionId 응답 헤더는 x-amz-delete-marker 로 설정된 상태로 `true` 반환됩니다.</p> <ul style="list-style-type: none"> • 버전 관리가 활성화된 버킷에서 하위 리소스 없이 오브젝트를 삭제하면 versionId 삭제 마커가 생성됩니다. 응답 헤더를 x-amz-delete-marker 사용하여 삭제 마커에 대한 를 versionId 반환하고 x-amz-version-id 응답 헤더를 로 반환한다. true • 버전 관리가 일시 중지된 버킷에서 하위 리소스 없이 개체를 삭제하면 versionId 기존 'null' 버전 또는 'null' 삭제 마커가 영구적으로 삭제되고 새 'null' 삭제 마커가 생성됩니다. x-amz-delete-marker`응답 헤더가 로 설정된 `true 상태로 반환됩니다. • 참고 *: 경우에 따라 객체에 대해 여러 개의 삭제 마커가 존재할 수 있습니다. <p>거버넌스 모드에서 개체 버전을 삭제하는 방법은 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다" 참조하십시오.</p>

작동	구축
DeleteObjects 를 클릭합니다 (이전에 이름이 여러 개체 삭제)	MFA(다중 요소 인증) 및 응답 헤더는 x-amz-mfa 지원되지 않습니다. 동일한 요청 메시지에서 여러 객체를 삭제할 수 있습니다. 거버넌스 모드에서 개체 버전을 삭제하는 방법은 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다" 참조하십시오.
DeleteObjectTagging 을 선택합니다	에서는 하위 리소스를 사용하여 tagging 개체에서 모든 태그를 제거합니다. 버전 관리 쿼리 매개 변수가 요청에 지정되지 않은 경우 versionId 작업은 버전 버킷의 가장 최신 버전의 객체에서 모든 태그를 삭제합니다. 개체의 현재 버전이 삭제 표식이면 응답 헤더가 로 설정된 true 상태로 "MethodNotAllowed" 상태가 x-amz-delete-marker 반환됩니다.
GetObject 를 참조하십시오	"GetObject 를 참조하십시오"
GetObjectAcl	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.
GetObjectLegalHold 를 참조하십시오	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
GetObjectRetention을 참조하십시오	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
GetObjectTagging	에서는 하위 리소스를 사용하여 tagging 개체의 모든 태그를 반환합니다. 버전 관리 쿼리 매개 변수가 요청에 지정되지 않은 경우 versionId 작업은 버전이 지정된 버킷에 있는 가장 최신 버전의 객체에서 모든 태그를 반환합니다. 개체의 현재 버전이 삭제 표식이면 응답 헤더가 로 설정된 true 상태로 "MethodNotAllowed" 상태가 x-amz-delete-marker 반환됩니다.
HeadObject 를 선택합니다	"HeadObject 를 선택합니다"
RestoreObject 를 선택합니다	"RestoreObject 를 선택합니다"
PutObject 를 선택합니다	"PutObject 를 선택합니다"
CopyObject 를 선택합니다 (이전에 명명된 Put Object - Copy)	"CopyObject 를 선택합니다"

작동	구축
PutObjectLegalHold를 선택합니다	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
PutObjectRetention	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
PutObjectTagging	<p>에서는 하위 리소스를 사용하여 tagging 기존 개체에 태그 집합을 추가합니다.</p> <p>개체 태그 제한</p> <p>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.</p> <p>태그 업데이트 및 수집 동작</p> <p>PutObjectTagging을 사용하여 개체의 태그를 업데이트하는 경우 StorageGRID는 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.</p> <p>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.</p> <p>충돌 해결</p> <p>동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.</p> <p>버전 관리</p> <p>쿼리 매개 변수가 요청에 지정되지 않은 경우 versionId 작업은 버전이 지정된 버킷에서 가장 최신 버전의 객체에 태그를 추가합니다. 개체의 현재 버전이 삭제 표시이면 응답 헤더가 로 설정된 true 상태로 "MethodNotAllowed" 상태가 x-amz-delete-marker 반환됩니다.</p>
SelectObjectContent 를 선택합니다	"SelectObjectContent 를 선택합니다"

S3 Select를 사용합니다

StorageGRID는 에 대해 다음과 같은 Amazon S3 Select 절, 데이터 형식 및 연산자를 "SelectObjectContent 명령"지원합니다.



목록에 없는 항목은 지원되지 않습니다.

구문은 을 참조하십시오 ["SelectObjectContent 를 선택합니다"](#). S3 Select에 대한 자세한 내용은 를 ["S3 Select용 AWS 문서"](#) 참조하십시오.

S3 Select가 활성화된 테넌트 계정만 SelectObjectContent 쿼리를 실행할 수 있습니다. 를 ["S3 Select 사용에 대한 고려 사항 및 요구 사항"](#) 참조하십시오.

절을 참조하십시오

- 목록을 선택합니다
- FROM 절
- WHERE 절
- Limit 절

데이터 유형

- 불입니다
- 정수
- 문자열
- 부동
- 십진수, 숫자
- 타임 스탬프입니다

연산자

논리 연산자

- 및
- 아닙니다
- 또는

비교 연산자

- 를 누릅니다
- 를 누릅니다
- lt;=.(&L
- GT;=.(&G
- =
- =
- 를 누릅니다
- !=

- 사이
- 인치

패턴 일치 연산자

- 좋아요
- _
- %

단일 작업자

- NULL입니다
- NULL이 아닙니다

수학 연산자

- 를 누릅니다
- -
- *
- /
- %

StorageGRID는 Amazon S3 Select 운영자 우선권을 따릅니다.

집계 함수

- 평균()
- 개수(*)
- 최대()
- 최소()
- 합계()

조건부 함수

- 케이스
- 합체
- 노LIF

변환 함수

- 캐스트(지원되는 데이터 형식용)

날짜 함수

- date_add

- Date_DIFF(날짜/시간)
- 압축 풀기
- to_string(대상 문자열)
- 를 _TIMESTAMP로 설정합니다
- UTCNOW

문자열 함수

- char_length, character_length
- 낮음
- 부분 문자열
- 잘라내기
- 위쪽

서버측 암호화를 사용합니다

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.

SSE를 사용합니다

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

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

SSE 요청 헤더는 다음 오브젝트 작업에서 지원됩니다.

- "PutObject 를 선택합니다"

- ["CopyObject 를 선택합니다"](#)
- ["CreateMultptUpload 를 클릭합니다"](#)

SSE-C를 사용합니다

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 AES256 이어야 합니다.
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.

- ["GetObject 를 참조하십시오"](#)
- ["HeadObject 를 선택합니다"](#)
- ["PutObject 를 선택합니다"](#)
- ["CopyObject 를 선택합니다"](#)
- ["CreateMultptUpload 를 클릭합니다"](#)
- ["업로드 파트"](#)
- ["업로드파트 복사"](#)

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

SSE-C를 사용하기 전에 다음 사항을 고려하십시오.

- [https](#)를 사용해야 합니다.



StorageGRID는 SSE-C를 사용할 때 [http](#)를 통해 이루어진 모든 요청을 거부합니다. 보안을 위해 [http](#)를 사용하여 실수로 보낸 모든 키가 손상되는 것을 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.

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

관련 정보

["Amazon S3 사용자 가이드: SSE-C\(고객 제공 키\)와 함께 서버측 암호화 사용"](#)

CopyObject 를 선택합니다

S3 CopyObject 요청을 사용하여 이미 S3에 저장된 개체의 복사본을 만들 수 있습니다. CopyObject 작업은 GetObject 를 수행한 다음 PutObject 를 수행하는 작업과 같습니다.

충돌 해결

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

개체 크기

단일 PutObject 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 오브젝트가 있는 경우 대신 ["멀티파트 업로드"](#) 사용하십시오.

단일 PutObject 작업의 maximum_supported_size는 5TiB(5,497,558,138,880바이트)입니다.



StorageGRID 11.6 이하에서 업그레이드한 경우 5GiB를 초과하는 객체를 업로드하려고 하면 S3 PUT 개체 크기가 너무 큼 경고가 트리거됩니다. StorageGRID 11.7 또는 11.8을 새로 설치한 경우 경고가 트리거되지 않습니다. 하지만 StorageGRID의 향후 릴리즈에서는 AWS S3 표준에 맞춰 5GiB보다 큰 오브젝트 업로드를 지원하지 않습니다.

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.
- 키 이름 또는 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우 StorageGRID는 헤더를 반환하지 `x-amz-missing-meta` 않습니다.

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-, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다
- x-amz-metadata-directive: 기본값은 로 COPY, 개체 및 관련 메타데이터를 복사할 수 있습니다.

개체를 복사할 때 기존 메타데이터를 덮어쓰도록 지정하거나 개체 메타데이터를 업데이트하도록 지정할 수 REPLACE 있습니다.

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

개체를 복사할 때 기존 태그를 덮어쓰도록 지정하거나 태그를 업데이트하도록 지정할 수 REPLACE 있습니다.

- S3 오브젝트 잠금 요청 헤더:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

이러한 헤더 없이 요청이 이루어지면 버킷 기본 보존 설정을 사용하여 오브젝트 버전 모드와 보존 기간을 계산합니다. 을 ["S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"](#)참조하십시오.

- 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

을 참조하십시오 [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-checksum-algorithm

개체를 복사할 때 소스 개체에 체크섬이 있으면 StorageGRID에서 해당 체크섬 값을 새 개체에 복사하지 않습니다. 이 동작은 개체 요청에서 을 사용하려고 하는지 여부에 관계없이 x-amz-checksum-algorithm 적용됩니다.

- x-amz-website-redirect-location

스토리지 클래스 옵션

`x-amz-storage-class` 요청 헤더가 지원되며 일치하는 ILM 규칙이 Dual Commit 또는 Balanced를 사용할 경우 StorageGRID에서 생성하는 객체 복제본 수에 영향을 xref:{relative_path}../ilm/data-protection-options-for-ingest.html["수집 옵션"] 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 상태에서 오브젝트를 버킷에 수집하면 REDUCED_REDUNDANCY 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 REDUCED_REDUNDANCY 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

CopyObject에서 x-amz-copy-source 사용

헤더에 지정된 소스 버킷 및 키가 대상 버킷 및 키와 다른 경우 x-amz-copy-source 소스 오브젝트 데이터의 복사본이 대상에 기록됩니다.

소스와 대상이 일치하고 헤더가 로 지정된 REPLACE 경우 x-amz-metadata-directive 객체의 메타데이터는 요청에 제공된 메타데이터 값으로 업데이트됩니다. 이 경우 StorageGRID는 오브젝트를 다시 수집하지 않습니다. 여기에는 두 가지 중요한 결과가 있습니다.

- 기존 개체를 현재 위치에서 암호화하거나 기존 개체의 암호화를 변경하는 데 CopyObject 를 사용할 수 없습니다. 헤더나 x-amz-server-side-encryption-customer-algorithm 헤더를 제공하면 x-amz-server-side-encryption StorageGRID는 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

사용자가 "서버측 암호화를 사용합니다" 제공하는 요청 헤더는 소스 개체가 암호화되어 있는지 여부와 대상 개체를 암호화할 계획인지에 따라 달라집니다.

- 소스 객체가 SSE-C(고객 제공 키)를 사용하여 암호화되는 경우 CopyObject 요청에 다음 세 개의 헤더를 포함해야 객체를 해독한 후 복사할 수 있습니다.
 - x-amz-copy-source-server-side-encryption-customer-algorithm: AES256 지정합니다.
 - x-amz-copy-source-server-side-encryption-customer-key: 원본 개체를 만들 때 제공한 암호화 키를 지정합니다.
 - x-amz-copy-source-server-side-encryption-customer-key-MD5: 원본 개체를 만들 때 제공한 MD5 다이제스트를 지정합니다.
- 제공 및 관리하는 고유 키를 사용하여 대상 개체(복사본)를 암호화하려면 다음 세 개의 머리를 포함합니다.
 - x-amz-server-side-encryption-customer-algorithm: AES256 지정합니다.
 - x-amz-server-side-encryption-customer-key: 대상 객체에 대한 새 암호화 키를 지정합니다.
 - x-amz-server-side-encryption-customer-key-MD5: 새 암호화 키의 MD5 다이제스트를 지정합니다.



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 에 대한 고려 사항을 "서버 측 암호화 사용" 검토하십시오.

- SSE(StorageGRID)에서 관리하는 고유 키를 사용하여 대상 개체(복사본)를 암호화하려는 경우 CopyObject 요청에 다음 헤더를 포함합니다.
 - x-amz-server-side-encryption



server-side-encryption` 개체 값을 업데이트할 수 없습니다. 대신 다음을 사용하여 새 값으로 `x-amz-metadata-directive` 복사본을 server-side-encryption 만듭니다 REPLACE.

버전 관리

소스 버킷의 버전이 관리되는 경우 헤더를 사용하여 개체의 최신 버전을 복사할 수 x-amz-copy-source 있습니다. 개체의 특정 버전을 복사하려면 하위 리소스를 사용하여 복사할 버전을 명시적으로 지정해야 versionId 합니다. 대상 버킷의 버전이 지정된 경우 생성된 버전이 x-amz-version-id 응답 헤더에 반환됩니다. 대상 버킷에 대한 버전 관리가 일시 중단된 경우 x-amz-version-id "null" 값이 반환됩니다.

GetObject 를 참조하십시오

S3 GetObject 요청을 사용하여 S3 버킷에서 객체를 검색할 수 있습니다.

GetObject 및 multipart 개체

요청 매개변수를 사용하여 멀티파트나 분할된 오브젝트의 특정 부분을 검색할 수 `partNumber` 있습니다. ``x-amz-mp-parts-count`` 응답 요소는 개체의 파트 수를 나타냅니다.

분할/다중 파트 오브젝트 및 비분할/비다중 파트 오브젝트 모두에 대해 1로 설정할 수 `partNumber` 있지만 `x-amz-mp-parts-count` 응답 요소는 분할된 오브젝트 또는 다중 파트 오브젝트에 대해서만 반환됩니다.

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 요청 가져오기 키 이름 또는 값에 인쇄할 수 없는 문자가 포함된 경우 헤더를 반환하지 `x-amz-missing-meta` 않습니다.

지원되는 요청 헤더

다음 요청 헤더가 지원됩니다.

- `x-amz-checksum-mode`: 지정합니다 ENABLED

``Range`` 헤더는 GetObject 에 대해 지원되지 ``x-amz-checksum-mode`` 않습니다. 활성화된 상태로 요청에 ``x-amz-checksum-mode`` 포함하면 ``Range`` StorageGRID는 응답에 체크섬 값을 반환하지 않습니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 `XNotImplemented` 반환됩니다.

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

버전 관리

하위 리소스가 지정되지 않은 경우 `versionId` 이 작업은 버전이 지정된 버킷에서 가장 최신 버전의 개체를 가져옵니다. 객체의 현재 버전이 삭제 마커인 경우 응답 헤더가 로 설정된 `true` 상태에서 "찾을 수 없음" 상태가 `x-amz-delete-marker` 반환됩니다.

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`: AES256 지정합니다.
- `x-amz-server-side-encryption-customer-key`: 개체의 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 개체의 암호화 키의 MD5 다이제스트를 지정합니다.



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"[서버측 암호화를 사용합니다](#)".

클라우드 스토리지 풀 객체에 대한 **GetObject**의 동작입니다

개체가 에 저장된 경우 "[클라우드 스토리지 풀](#)"GetObject 요청의 동작은 개체의 상태에 따라 달라집니다. 자세한 내용은 ["HeadObject 를 선택합니다"](#)참조하십시오.



오브젝트가 클라우드 스토리지 풀에 저장되고 하나 이상의 오브젝트 복제본이 그리드에 있는 경우 GetObject 요청은 클라우드 스토리지 풀에서 검색하기 전에 그리드에서 데이터 검색을 시도합니다.

개체의 상태입니다	GetObject 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 요청을 사용하여 " RestoreObject 를 선택합니다 "객체를 검색 가능한 상태로 복원합니다.
복구할 수 없는 상태에서 복원 중인 개체입니다	403 Forbidden, InvalidObjectState RestoreObject 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. 개체의 일부 부분이 이미 검색할 수 없는 상태로 전환되었거나 개체의 일부 부분이 아직 복원되지 않은 경우 GetObject 요청이 잘못 반환될 수 200 OK 있습니다.

다음과 같은 경우:

- GetObject 요청에서 일부 데이터를 반환하지만 전송 도중에 중지됩니다.
- 이후의 GetObject 요청이 반환될 수 403 Forbidden 있습니다.

GetObject 및 교차 그리드 복제

를 사용 중이며 "교차 그리드 복제"버킷에 대해 활성화된 경우 "그리드 통합"S3 클라이언트는 GetObject 요청을 실행하여 개체의 복제 상태를 확인할 수 있습니다. 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 x-ntap-sg-cgr-replication-status 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	<ul style="list-style-type: none">• * 완료됨 *: 복제가 성공했습니다.• * 보류 중 *: 객체가 아직 복제되지 않았습니다.• * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	<ul style="list-style-type: none">• replica *: 객체가 소스 그리드에서 복제되었습니다.



StorageGRID는 헤더를 지원하지 x-amz-replication-status 않습니다.

HeadObject 를 선택합니다

S3 HeadObject 요청을 사용하여 개체 자체를 반환하지 않고 개체에서 메타데이터를 검색할 수 있습니다. 객체가 클라우드 스토리지 풀에 저장된 경우 HeadObject 를 사용하여 객체의 전환 상태를 확인할 수 있습니다.

HeadObject 및 multipart 개체

요청 매개 변수를 사용하여 멀티파트 또는 분할된 개체의 특정 부분에 대한 메타데이터를 검색할 수 partNumber 있습니다. `x-amz-mp-parts-count` 응답 요소는 개체의 파트 수를 나타냅니다.

분할/다중 파트 오브젝트 및 비분할/비다중 파트 오브젝트 모두에 대해 1로 설정할 수 partNumber 있지만 x-amz-mp-parts-count 응답 요소는 분할된 오브젝트 또는 다중 파트 오브젝트에 대해서만 반환됩니다.

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 헤드 요청은 키 이름이나 값에 인쇄할 수 없는 문자가 포함된 경우 헤더를 반환하지 x-amz-missing-meta 않습니다.

지원되는 요청 헤더

다음 요청 헤더가 지원됩니다.

- x-amz-checksum-mode

`partNumber` 매개 변수 및 `Range` 머리글은 HeadObject 에 대해 지원되지 `x-amz-checksum-mode` 않습니다. 활성화된 상태로 요청에 포함하면 `x-amz-checksum-mode` StorageGRID는 응답에 체크섬 값을 반환하지 않습니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 `xNotImplemented` 반환됩니다.

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

버전 관리

하위 리소스가 지정되지 않은 경우 `versionId` 이 작업은 버전이 지정된 버킷에서 가장 최신 버전의 개체를 가져옵니다. 객체의 현재 버전이 삭제 마커인 경우 응답 헤더가 로 설정된 `true` 상태에서 "찾을 수 없음" 상태가 `x-amz-delete-marker` 반환됩니다.

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`: AES256 지정합니다.
- `x-amz-server-side-encryption-customer-key`: 개체의 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 개체의 암호화 키의 MD5 다이제스트를 지정합니다.



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"**서버측 암호화를 사용합니다**".

클라우드 스토리지 풀 객체에 대한 **HeadObject** 응답입니다

개체가 에 저장된 경우 "**클라우드 스토리지 풀**"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	HeadObject 에 대한 응답입니다
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	200 OK (특수 응답 헤더가 반환되지 않음)

개체의 상태입니다	HeadObject 에 대한 응답입니다
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>오브젝트가 검색 불가능한 상태로 전환될 때까지의 값은 expiry-date 나중에 먼 시간으로 설정됩니다. 정확한 전환 시간은 StorageGRID 시스템에 의해 제어되지 않습니다.</p>
개체가 검색할 수 없는 상태로 전환되었지만 하나 이상의 복사본이 그리드에 있습니다	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>의 값은 expiry-date 나중에 먼 시간으로 설정됩니다.</p> <ul style="list-style-type: none"> 참고 *: 그리드의 복제본을 사용할 수 없는 경우(예: 스토리지 노드가 다운된 경우), 객체를 성공적으로 검색하기 전에 클라우드 스토리지 풀에서 복제본을 복원하도록 요청을 해야 "RestoreObject 를 선택합니다"합니다.
개체가 검색할 수 없는 상태로 전환되었으며 그리드에 복사본이 없습니다	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
복구할 수 없는 상태에서 복원 중인 개체입니다	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

개체의 상태입니다	HeadObject 에 대한 응답입니다
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	<pre>200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" 는 expiry-date 클라우드 스토리지 풀의 객체가 검색할 수 없는 상태로 반환되는 시점을 나타냅니다.</pre>

Cloud Storage Pool에서 다중 또는 분할 오브젝트 지원

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. 개체의 일부 부분이 이미 검색할 수 없는 상태로 전환되었거나 개체의 일부 부분이 아직 복원되지 않은 경우 HeadObject 요청이 잘못 반환될 수 `x-amz-restore: ongoing-request="false"` 있습니다.

HeadObject 및 교차 그리드 복제

를 사용 중이며 "**교차 그리드 복제**" 버킷에 대해 활성화된 경우 "**그리드 통합**" S3 클라이언트는 HeadObject 요청을 실행하여 객체의 복제 상태를 확인할 수 있습니다. 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	<ul style="list-style-type: none"> * 완료됨 *: 복제가 성공했습니다. * 보류 중 *: 객체가 아직 복제되지 않았습니다. * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	<ul style="list-style-type: none"> * replica *: 객체가 소스 그리드에서 복제되었습니다.



StorageGRID는 헤더를 지원하지 `x-amz-replication-status` 않습니다.

PutObject 를 선택합니다

S3 PutObject 요청을 사용하여 객체를 버킷에 추가할 수 있습니다.

충돌 해결

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

개체 크기

단일 PutObject 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 오브젝트가 있는 경우 대신 ["멀티파트 업로드"](#) 사용하십시오.

단일 PutObject 작업의 maximum_supported_size는 5TiB(5,497,558,138,880바이트)입니다.



StorageGRID 11.6 이하에서 업그레이드한 경우 5GiB를 초과하는 객체를 업로드하려고 하면 S3 PUT 개체 크기가 너무 큼 경고가 트리거됩니다. StorageGRID 11.7 또는 11.8을 새로 설치한 경우 경고가 트리거되지 않습니다. 하지만 StorageGRID의 향후 릴리즈에서는 AWS S3 표준에 맞춰 5GiB보다 큰 오브젝트 업로드를 지원하지 않습니다.

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 PutObject, CopyObject, GetObject 및 HeadObject 요청이 성공합니다.
- 키 이름 또는 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우 StorageGRID는 헤더를 반환하지 x-amz-missing-meta 않습니다.

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

Content-EncodingStorageGRID에 대해 를 aws-chunked 지정하면 다음 항목이 검증되지 않습니다.

- StorageGRID는 청크 데이터에 대해 를 확인하지 chunk-signature 않습니다.
- StorageGRID는 사용자가 개체에 대해 제공한 값을 확인하지 x-amz-decoded-content-length 않습니다.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

페이로드 서명도 사용되는 경우 청크 전송 인코딩이 aws-chunked 지원됩니다.

- x-amz-checksum-sha256
- x-amz-meta-, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다.

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

```
x-amz-meta-name: value
```

사용자 정의 생성 시간 * 옵션을 ILM 규칙의 참조 시간으로 사용하려면 객체를 생성할 때 기록하는 메타데이터의 이름으로 를 사용해야 creation-time 합니다. 예를 들면 다음과 같습니다.

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

의 값은 creation-time 1970년 1월 1일 이후 초로 계산됩니다.



ILM 규칙은 참조 시간에 * 사용자 정의 생성 시간 * 과 Balanced 또는 Strict 수집 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

이러한 헤더 없이 요청이 이루어지면 버킷 기본 보존 설정을 사용하여 오브젝트 버전 모드와 보존 기간을 계산합니다. 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.

- 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

을 참조하십시오 [서버측 암호화에 대한 요청 헤더](#).

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- x-amz-acl
- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-website-redirect-location

``x-amz-website-redirect-location`` 헤더가 `를 `XNotImplemented` 반환합니다.`

스토리지 클래스 옵션

``x-amz-storage-class`` 요청 헤더가 지원됩니다. 에 제출된 ``x-amz-storage-class`` 값은 StorageGRID 시스템 (ILM에 의해 결정됨)에 저장되는 오브젝트의 영구 사본의 수가 아니라 수집 중에 StorageGRID가 오브젝트 데이터를 보호하는 방법에 영향을 줍니다.

수집된 객체와 일치하는 ILM 규칙이 Strict 수집 옵션을 사용하는 경우 x-amz-storage-class 헤더는 영향을 미치지 않습니다.

다음 값을 사용할 수 x-amz-storage-class 있습니다.

- 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 StorageGRID가 규칙에 지정된 모든 복사본을 즉시 만들 수 없는 경우 StorageGRID는 다른 스토리지 노드에 두 개의 임시 복사본을 만듭니다.

StorageGRID가 ILM 규칙(동기식 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있다면 x-amz-storage-class 헤더는 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. 이 REDUCED_REDUNDANCY 옵션은 오브젝트와 일치하는 ILM 규칙이 복제된 단일 복사본을 생성할 때 가장 적합합니다. 이 경우 REDUCED_REDUNDANCY 사용하면 모든 수집 작업에서 불필요한 추가 오브젝트 복사본을 생성하여 삭제할 필요가 없습니다.

다른 상황에서는 이 옵션을 사용하지 REDUCED_REDUNDANCY 않는 것이 좋습니다. REDUCED_REDUNDANCY 수집 중 오브젝트 데이터가 손실될 위험이 증가함 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.



복제된 복사본이 항상 하나만 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.

REDUCED_REDUNDANCY 지정하면 오브젝트를 처음 수집할 때 생성되는 복사본의 개수만 영향을 줍니다. 활성 ILM 정책에 따라 오브젝트를 평가할 때 생성되는 오브젝트 복사본 수에 영향을 미치지 않으며 StorageGRID 시스템에서 더 낮은 수준의 이중화로 데이터가 저장되지 않습니다.



S3 오브젝트 잠금이 설정된 상태에서 오브젝트를 버킷에 수집하면 REDUCED_REDUNDANCY 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 REDUCED_REDUNDANCY 옵션은 오류를 반환합니다. 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

머리글이 PutObject 요청에 포함되어 있지 않으면 x-amz-server-side-encryption PutObject 응답에서 그리드 전체의 머리글이 "저장된 개체 암호화 설정입니다"생략됩니다.

- * SSE-C *: 사용자가 제공 및 관리하는 고유 키로 객체를 암호화하려면 이 헤더 세 개를 모두 사용합니다.

- x-amz-server-side-encryption-customer-algorithm: AES256 지정합니다.
- x-amz-server-side-encryption-customer-key: 새 개체에 대한 암호화 키를 지정합니다.
- x-amz-server-side-encryption-customer-key-MD5: 새 개체의 암호화 키의 MD5 다이제스트를 지정합니다.



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 에 대한 고려 사항을 "서버 측 암호화 사용"검토하십시오.



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

버전 관리

버킷에 대해 버전 관리를 사용하도록 설정하면 저장되는 오브젝트 버전에 대해 고유한 `versionId` 버전이 자동으로 생성됩니다. `versionId` 응답 헤더를 사용하여 응답에서도 `x-amz-version-id` 반환됩니다.

버전 관리가 일시 중단되면 개체 버전이 null로 저장되고 null 버전이 이미 있는 경우 해당 버전을 `versionId` 덮어씁니다.

승인 헤더의 서명 계산

헤더를 사용하여 요청을 인증하는 경우 `Authorization StorageGRID`는 다음과 같은 점에서 AWS와 다릅니다.

- `StorageGRID`에서는 머리글이 에 포함될 `CanonicalHeaders` 필요가 `host` 없습니다.
- `StorageGRID`는 `Content-Type` 에 포함되지 `CanonicalHeaders` 않아도 됩니다.
- `StorageGRID`에서는 머리글이 에 포함될 `CanonicalHeaders` 필요가 `x-amz-*` 없습니다.



일반적으로 이러한 헤더를 항상 포함시켜 유효성을 확인하지만 이러한 헤더를 `CanonicalHeaders` 제외하면 `StorageGRID`에서 오류를 반환하지 않습니다.

자세한 내용은 을 ["승인 헤더에 대한 서명 계산:단일 청크\(AWS 서명 버전 4\)로 페이로드 전송"](#)참조하십시오.

관련 정보

- ["ILM을 사용하여 개체를 관리합니다"](#)
- ["Amazon Simple Storage Service API 참조: PutObject"](#)

RestoreObject 를 선택합니다

S3 `RestoreObject` 요청을 사용하여 클라우드 스토리지 풀에 저장된 개체를 복원할 수 있습니다.

지원되는 요청 유형입니다

`StorageGRID`에서는 객체를 복원하기 위한 `RestoreObject` 요청만 지원합니다. 복원 유형을 지원하지 `SELECT` 않습니다. 요청 반환 을 선택합니다 `XNotImplemented`.

버전 관리

선택적으로 `versionId` 버전 지정된 버킷에서 특정 버전의 개체를 복원하도록 지정합니다. 을 지정하지 `versionId` 않으면 개체의 최신 버전이 복원됩니다

클라우드 스토리지 풀 객체에서 **RestoreObject**의 동작입니다

개체가 에 저장된 경우 ["클라우드 스토리지 풀"](#)`RestoreObject` 요청에는 개체의 상태에 따라 다음과 같은 동작이 발생합니다. 자세한 내용은 을 ["HeadObject 를 선택합니다"](#)참조하십시오.



객체가 클라우드 스토리지 풀에 저장되어 있고 하나 이상의 객체 복제본도 그리드에 있는 경우 `RestoreObject` 요청을 실행하여 객체를 복구할 필요가 없습니다. 대신 `GetObject` 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

개체의 상태입니다	RestoreObject 의 동작입니다
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 변경되지 않았습니다. • 참고 *: 개체가 검색 불가능한 상태로 전환되기 전에 개체를 변경할 수 expiry-date 없습니다.
개체가 검색할 수 없는 상태로 전환되었습니다	202 Accepted 요청 본문에 지정된 일 수 동안 객체의 검색 가능한 복제본을 클라우드 스토리지 풀에 복구합니다. 이 기간이 끝나면 객체는 복구할 수 없는 상태로 돌아갑니다. 필요한 경우, request 요소를 사용하여 Tier 복원 작업이 완료되는 데 걸리는 시간을 (Expedited Standard` 결정합니다, 또는 `Bulk). 지정하지 않으면 Tier Standard 계층이 사용됩니다. • 중요 *: 개체가 S3 Glacier Deep Archive로 전환되었거나 클라우드 스토리지 풀이 Azure Blob 스토리지를 사용하는 경우 계층을 사용하여 복원할 수 없습니다 Expedited. 다음 오류가 403 Forbidden 반환됩니다 InvalidTier Retrieval option is not supported by this storage class.
복구할 수 없는 상태에서 복원 중인 개체입니다	409 Conflict, RestoreAlreadyInProgress
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	200 OK • 참고: * 오브젝트가 검색 가능한 상태로 복원된 경우 에 대한 새 값으로 RestoreObject 요청을 다시 실행하여 오브젝트를 Days 변경할 수 expiry-date 있습니다. 복원 날짜는 요청 시간을 기준으로 업데이트됩니다.

SelectObjectContent 를 선택합니다

S3 SelectObjectContent 요청을 사용하여 간단한 SQL 문을 기반으로 S3 개체의 내용을 필터링할 수 있습니다.

자세한 내용은 을 ["Amazon Simple Storage Service API 참조: SelectObjectContent"](#)참조하십시오.

시작하기 전에

- 테넌트 계정에 S3 Select 권한이 있습니다.
- `s3:GetObject` 쿼리할 개체에 대한 사용 권한이 있습니다.
- 쿼리할 객체는 다음 형식 중 하나여야 합니다.

- CSV *. GZIP 또는 BZIP2 보관 파일로 압축하거나 그대로 사용할 수 있습니다.
- * 파케 *. Parquet 객체에 대한 추가 요구 사항:
 - S3 Select는 GZIP 또는 Snappy를 사용한 컬럼 압축만 지원합니다. S3 Select는 Parquet 오브젝트에 대한 전체 오브젝트 압축을 지원하지 않습니다.
 - S3 Select는 Parquet 출력을 지원하지 않습니다. 출력 형식을 CSV 또는 JSON으로 지정해야 합니다.
 - 압축되지 않은 최대 행 그룹 크기는 512MB입니다.
 - 개체의 스키마에 지정된 데이터 형식을 사용해야 합니다.
 - 간격, JSON, 목록, 시간 또는 UUID 논리적 유형은 사용할 수 없습니다.
- SQL 식의 최대 길이는 256KB입니다.
- 입력 또는 결과에 있는 모든 레코드의 최대 길이는 1MiB입니다.

CSV 요청 구문 예

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

쪽모이 세공 요청 구문 예

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

SQL 쿼리의 예

이 쿼리는 시/도 이름, 2010년 인구, 2015년 예상 인구, 미국 인구 조사 데이터의 변경 비율을 가져옵니다. 상태가 아닌 파일의 레코드는 무시됩니다.

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

쿼리할 파일의 처음 몇 줄은 SUB-EST2020_ALL.csv 다음과 같습니다.

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

AWS-CLI 사용 예(CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\"}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

출력 파일의 처음 몇 줄은 changes.csv 다음과 같습니다.

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

AWS-CLI 사용 예(Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

출력 파일의 처음 몇 줄인 changes.csv는 다음과 같습니다.

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

멀티파트 업로드 작업

멀티파트 업로드 작업

이 섹션에서는 StorageGRID가 멀티파트 업로드 작업을 지원하는 방법에 대해 설명합니다.

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

- 해당 버킷에 대한 ListMultipartUploads 쿼리의 결과가 불완전한 결과를 반환할 수 있으므로 단일 버킷에 대한 동시 다중 파트 업로드가 1,000개를 초과해서는 안 됩니다.
- 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 Balanced 또는 Strict를 사용하는 경우, ILM은 수집 시 멀티파트 개체의 각 부분과 다중 파트 업로드가 완료될 때 개체 전체에 대해 평가됩니다. "수집 옵션" 이 사항이 개체 및 파트 배치에 미치는 영향에 대해 알고 있어야 합니다.
 - S3 다중 파트 업로드가 진행되는 동안 ILM이 변경되면 다중 파트 업로드가 완료될 때 개체의 일부 부분이 현재 ILM 요구사항을 충족하지 못할 수 있습니다. 올바르게 배치되지 않은 모든 부품은 ILM 재평가를 위해 대기열에 추가되고 나중에 올바른 위치로 이동됩니다.

- 파트에 대한 ILM을 평가할 때 StorageGRID은 개체의 크기가 아닌 파트 크기를 필터링합니다. 즉, 개체의 일부를 개체에 대한 ILM 요구 사항을 전체가 충족하지 않는 위치에 저장할 수 있습니다. 예를 들어, 모든 작은 오브젝트가 DC2에 저장되지만 10GB 이상의 오브젝트는 모두 DC1에 저장되도록 규칙이 지정된 경우 10부분 다중 부분 업로드의 각 1GB 부분은 인제스트 시 DC2에 저장됩니다. 그러나 개체 전체에 대해 ILM을 평가하면 개체의 모든 부분이 DC1로 이동됩니다.

- 모든 멀티 파트 업로드 작업은 StorageGRID를 "일관성 값"지원합니다.
- 멀티파트 업로드를 사용하여 개체를 수집하는 경우 이 "객체 분할 임계값(1GiB)"적용되지 않습니다.
- 필요에 따라 멀티파트 업로드와 함께 을 사용할 수 "서버 측 암호화"있습니다. SSE(StorageGRID 관리 키가 있는 서버측 암호화)를 사용하려면 CreateMultipartUpload 요청에만 요청 헤더를 포함합니다 x-amz-server-side-encryption. SSE-C(고객 제공 키를 사용한 서버측 암호화)를 사용하려면 CreateMultipartUpload 요청과 이후의 각 UploadPart 요청에서 동일한 3개의 암호화 키 요청 헤더를 지정합니다.

작동	구축
AbortMultipartUpload 를 클릭합니다	모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.
CompleteMultipartUpload를 클릭합니다	을 참조하십시오 "CompleteMultipartUpload를 클릭합니다"
CreateMulptUpload 를 클릭합니다 (이전에 명명된 다중 파트 업로드 시작)	을 참조하십시오 "CreateMulptUpload 를 클릭합니다"
ListMultipartUploads 를 참조하십시오	을 참조하십시오 "ListMultipartUploads 를 참조하십시오"
목록 파트	모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.
업로드 파트	을 참조하십시오 "업로드 파트"
업로드파트 복사	을 참조하십시오 "업로드파트 복사"

CompleteMultipartUpload를 클릭합니다

CompleteMultipartUpload 작업은 이전에 업로드한 부품을 조립하여 객체의 다중 부분 업로드를 완료합니다.



StorageGRID는 CompleteMultipartUpload를 사용하여 요청 매개 변수에 대해 비연속 값을 오름차순으로 partNumber 지원합니다. 매개 변수는 어떤 값으로든 시작할 수 있습니다.

충돌 해결

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

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- x-amz-checksum-sha256
- x-amz-storage-class

``x-amz-storage-class`` 일치하는 ILM 규칙이 을 지정한 경우 머릿글에 StorageGRID에서 생성하는 개체 복사본 수에 영향을 `xref:{relative_path}../ilm/data-protection-options-for-ingest.html` ["이중 커밋 또는 Balanced 인제스트 옵션"] 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 상태에서 오브젝트를 버킷에 수집하면 REDUCED_REDUNDANCY 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 REDUCED_REDUNDANCY 옵션은 오류를 반환합니다. 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.



ETag` 반환되는 값은 데이터의 MD5 합계가 아니라 다중 개체 값의 Amazon S3 API 구현을 `ETag` 따릅니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

버전 관리

이 작업은 여러 부분 업로드를 완료합니다. 버킷에 대해 버전 관리가 활성화된 경우 다중 파트 업로드가 완료된 후 개체 버전이 생성됩니다.

버킷에 대해 버전 관리를 사용하도록 설정하면 저장되는 오브젝트 버전에 대해 고유한 `versionId` 버전이 자동으로 생성됩니다. `versionId` 응답 헤더를 사용하여 응답에서도 `x-amz-version-id` 반환됩니다.`

버전 관리가 일시 중단되면 개체 버전이 null로 저장되고 null 버전이 이미 있는 경우 해당 버전을 `versionId` 덮어씁니다.



버킷에 대해 버전 관리가 활성화된 경우, 같은 개체 키에서 동시 다중 파트 업로드가 완료된 경우에도 다중 파트 업로드를 완료하면 항상 새 버전이 생성됩니다. 버킷에 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.

복제, 알림 또는 메타데이터 알림에 실패했습니다

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

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

을 "[플랫폼 서비스 문제 해결](#)" 참조하십시오.

CreateMultipartUpload 를 클릭합니다

CreateMultipartUpload(이전에 이름이 Multipart Upload 시작) 작업은 개체에 대한 다중 부분 업로드를 시작하고 업로드 ID를 반환합니다.

``x-amz-storage-class`` 요청 헤더가 지원됩니다. 에 제출된 ``x-amz-storage-class`` 값은 StorageGRID 시스템(ILM에 의해 결정됨)에 저장되는 오브젝트의 영구 사본의 수가 아니라 수집 중에 StorageGRID가 오브젝트 데이터를 보호하는 방법에 영향을 줍니다.

수집된 객체와 일치하는 ILM 규칙이 Strict 를 사용하는 경우 "수집 옵션" ``x-amz-storage-class`` 헤더는 영향을 미치지 않습니다.

다음 값을 사용할 수 `x-amz-storage-class` 있습니다.

- STANDARD (기본값)
 - * Dual Commit *: ILM 규칙이 Dual Commit Ingest 옵션을 지정하는 경우 오브젝트가 수집되는 즉시 해당 오브젝트의 두 번째 복사본이 생성되어 다른 스토리지 노드(Dual Commit)로 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.

StorageGRID가 ILM 규칙(동기식 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있다면 `x-amz-storage-class` 헤더는 효과가 없습니다.

- REDUCED_REDUNDANCY
 - * Dual Commit *: ILM 규칙이 Dual Commit 옵션을 지정하는 경우 StorageGRID는 개체가 수집될 때(단일 커밋) 하나의 중간 복사본을 생성합니다.
 - * 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. 이 REDUCED_REDUNDANCY 옵션은 오브젝트와 일치하는 ILM 규칙이 복제된 단일 복사본을 생성할 때 가장 적합합니다. 이 경우를 REDUCED_REDUNDANCY 사용하면 모든 수집 작업에서 불필요한 추가 오브젝트 복사본을 생성하여 삭제할 필요가 없습니다.

다른 상황에서는 이 옵션을 사용하지 REDUCED_REDUNDANCY 않는 것이 좋습니다. REDUCED_REDUNDANCY 수집 중 오브젝트 데이터가 손실될 위험이 증가함 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.



복제된 복사본이 항상 하나만 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.

`REDUCED_REDUNDANCY` 지정하면 오브젝트를 처음 수집할 때 생성되는 복사본의 개수만 영향을 줍니다. 활성 ILM 정책에 따라 오브젝트를 평가할 때 생성되는 오브젝트 복사본 수에 영향을 미치지 않으며 StorageGRID 시스템에서 더 낮은 수준의 이중화로 데이터가 저장되지는 않습니다.



S3 오브젝트 잠금이 설정된 상태에서 오브젝트를 버킷에 수집하면 REDUCED_REDUNDANCY 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 REDUCED_REDUNDANCY 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- Content-Type
- x-amz-checksum-algorithm

현재는 의 SHA256 값만 x-amz-checksum-algorithm 지원됩니다.

- x-amz-meta-, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다

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

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

사용자 정의 생성 시간 * 옵션을 ILM 규칙의 참조 시간으로 사용하려면 객체를 생성할 때 기록하는 메타데이터의 이름으로 를 사용해야 creation-time 합니다. 예를 들면 다음과 같습니다.

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

의 값은 creation-time 1970년 1월 1일 이후 초로 계산됩니다.



'creation-time' 기존 Compliance가 활성화된 버킷에 오브젝트를 추가하는 경우 사용자 정의 메타데이터로 추가할 수 없습니다. 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

이러한 헤더 없이 요청이 이루어지면 버킷 기본 보존 설정을 사용하여 개체 버전 보존 기간을 계산합니다.

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

• 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

서버측 암호화에 대한 요청 헤더



StorageGRID에서 UTF-8 문자를 처리하는 방법에 대한 자세한 내용은 을 참조하십시오"**PutObject** 를 선택합니다".

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 개체를 암호화하려면 CreateMultipartUpload 요청에서 다음 헤더를 사용합니다. UploadPart 요청에는 이 헤더를 지정하지 마십시오.
 - x-amz-server-side-encryption
- * SSE-C *: 제공 및 관리하는 고유 키로 개체를 암호화하려면 CreateMultipartUpload 요청(및 이후의 각 UploadPart 요청)에 이 헤더 세 개를 모두 사용하십시오.
 - x-amz-server-side-encryption-customer-algorithm: AES256 지정합니다.
 - x-amz-server-side-encryption-customer-key: 새 개체에 대한 암호화 키를 지정합니다.
 - x-amz-server-side-encryption-customer-key-MD5: 새 개체의 암호화 키의 MD5 다이제스트를 지정합니다.



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 에 대한 고려 사항을 "**서버 측 암호화 사용**" 검토하십시오.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

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

``x-amz-website-redirect-location`헤더가 를 `XNotImplemented`반환합니다.`

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

ListMultipartUploads 를 참조하십시오

ListMultipartUploads 작업은 버킷에 대해 진행 중인 다중 파트 업로드를 나열합니다.

지원되는 요청 매개 변수는 다음과 같습니다.

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

업로드 파트

UploadPart 작업은 객체에 대한 다중 부분 업로드의 파트를 업로드합니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

서버측 암호화에 대한 요청 헤더

CreateMultipartUpload 요청에 대해 SSE-C 암호화를 지정한 경우 각 UploadPart 요청에 다음 요청 머리글도 포함해야 합니다.

- `x-amz-server-side-encryption-customer-algorithm`: AES256 지정합니다.
- `x-amz-server-side-encryption-customer-key`: CreateMultipartUpload 요청에서 제공한 것과 동일한 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: CreateMultipartUpload 요청에 제공한 것과 동일한 MD5 다이제스트를 지정합니다.



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"**서버측 암호화를 사용합니다**".

CreateMultipartUpload 요청 중에 SHA-256 체크섬을 지정한 경우 각 UploadPart 요청에 다음 요청 헤더도 포함해야 합니다.

- `x-amz-checksum-sha256`: 이 부품에 대한 SHA-256 체크섬을 지정합니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

업로드파트 복사

UploadPartCopy 작업은 기존 개체의 데이터를 데이터 소스로 복사하여 개체의 일부를 업로드합니다.

UploadPartCopy 작업은 모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.

이 요청은 StorageGRID 시스템 내에 지정된 오브젝트 데이터를 읽고 `x-amz-copy-source-range` 씩니다.

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

CreateMultipartUpload 요청에 대해 SSE-C 암호화를 지정한 경우 각 UploadPartCopy 요청에 다음 요청 머리글도 포함해야 합니다.

- x-amz-server-side-encryption-customer-algorithm: AES256 지정합니다.
- x-amz-server-side-encryption-customer-key: CreateMultipartUpload 요청에서 제공한 것과 동일한 암호화 키를 지정합니다.
- x-amz-server-side-encryption-customer-key-MD5: CreateMultipartUpload 요청에 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

소스 객체가 SSE-C(고객 제공 키)를 사용하여 암호화되는 경우 UploadPartCopy 요청에 다음 세 개의 헤더를 포함해야 객체를 해독한 후 복사할 수 있습니다.

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



제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"**서버측 암호화를 사용합니다**".

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

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
BucketAlreadyExists를 참조하십시오	409 충돌
BucketNotEmpty	409 충돌

이름	HTTP 상태입니다
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
InvalidBucketState입니다	409 충돌
InvalidDigest 를 선택합니다	400 잘못된 요청
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

이름	HTTP 상태입니다
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
NoSuchBucketPolicy를 참조하십시오	404를 찾을 수 없습니다
ObjectLockConfigurationNotFoundError 가 발생합니다	404를 찾을 수 없습니다
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
XBucketLifecycleNotAllowed를 참조하십시오	버킷 수명 주기 구성은 레거시 준수 버킷에서 허용되지 않습니다	400 잘못된 요청
XBucketPolicyParseException 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

이름	설명	HTTP 상태입니다
XMaxBuckketPolicyLengthExceeded 를 참조하십시오	정책이 허용되는 최대 버킷 정책 길이를 초과합니다.	400 잘못된 요청
XMissingInternalRequestHeader를 참조하십시오	내부 요청의 헤더가 누락되었습니다.	400 잘못된 요청
XNoSuchBucketCompliance	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

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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