



## **S3 버킷 관리** StorageGRID 11.5

NetApp  
April 11, 2024

# 목차

S3 버킷 관리 .....	1
S3 오브젝트 잠금 사용 .....	1
S3 버킷 생성 .....	5
S3 버킷 세부 정보 보기 .....	8
정합성 보장 수준을 변경하는 중입니다 .....	10
마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다 .....	12
CORS(Cross-Origin Resource Sharing) 구성 .....	14
S3 버킷을 삭제하는 중입니다 .....	16

# S3 버킷 관리

적절한 권한이 있는 S3 테넌트를 사용하는 경우 S3 버킷을 생성, 보기 및 삭제하고, 정합성 보장 수준 설정을 업데이트하고, CORS(Cross-Origin Resource Sharing)를 구성하고, 마지막 액세스 시간 업데이트 설정을 활성화 및 비활성화하고, S3 플랫폼 서비스를 관리할 수 있습니다.

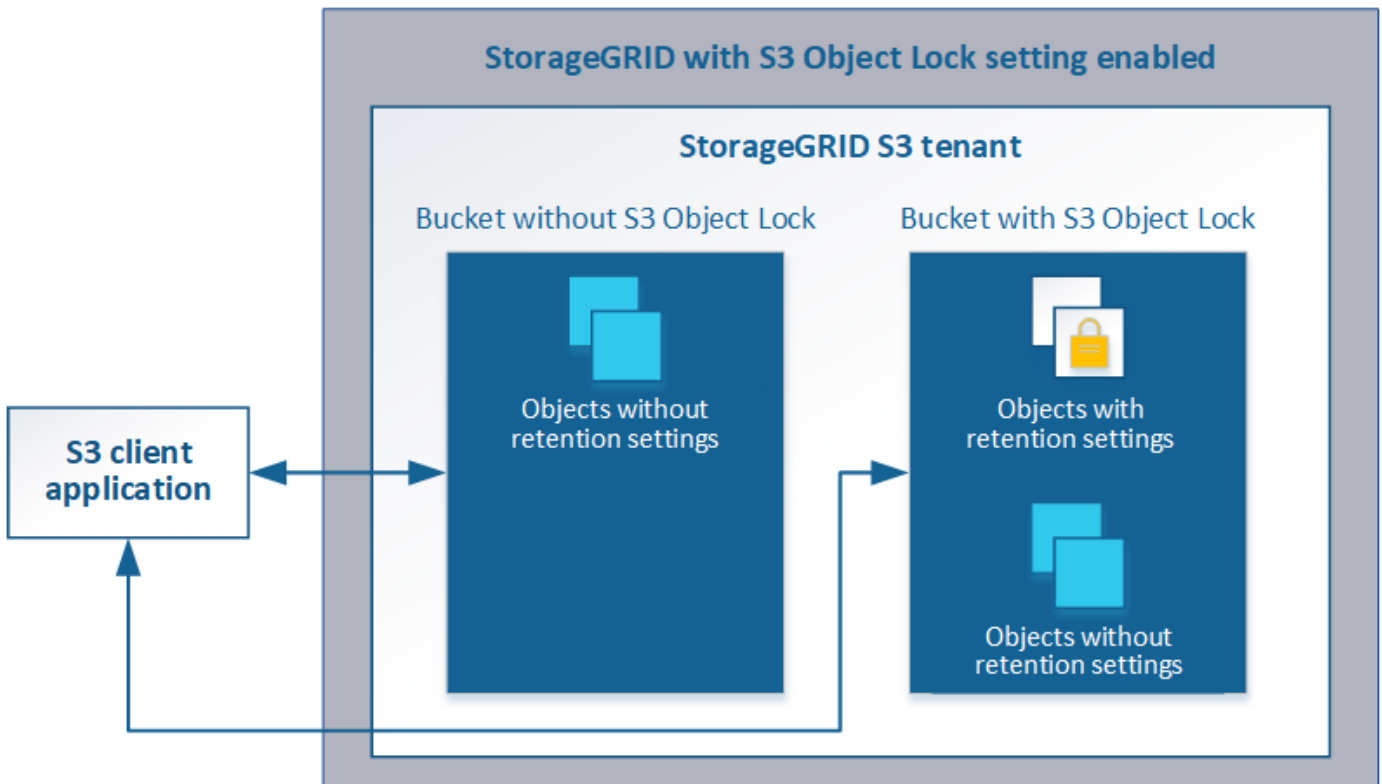
## S3 오브젝트 잠금 사용

오브젝트가 보존 규정 요구사항을 충족해야 하는 경우 StorageGRID의 S3 오브젝트 잠금 기능을 사용할 수 있습니다.

### S3 오브젝트 잠금이란 무엇입니까?

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3(Amazon Simple Storage Service)의 S3 오브젝트 잠금과 동등한 오브젝트 보호 솔루션입니다.

그림에서 볼 수 있듯이 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 사용하면 S3 테넌트 계정이 S3 오브젝트 잠금을 사용하거나 사용하지 않고 버킷을 생성할 수 있습니다. 버킷에 S3 오브젝트 잠금이 설정된 경우 S3 클라이언트 애플리케이션이 해당 버킷의 모든 오브젝트 버전에 대한 보존 설정을 선택적으로 지정할 수 있습니다. 오브젝트 버전에 S3 오브젝트 잠금으로 보호할 보존 설정이 지정되어 있어야 합니다.



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 S3 오브젝트 잠금이 활성화된 경우 오브젝트를 생성하거나 업데이트할 때 S3 클라이언트 애플리케이션에서

다음 오브젝트 레벨 보존 설정 중 하나 또는 모두를 선택적으로 지정할 수 있습니다.

- \* Retain-until-date \*: 개체 버전의 Retain-until-date가 미래인 경우 개체를 검색할 수 있지만 수정하거나 삭제할 수 없습니다. 필요에 따라 오브젝트의 보존 기간(Retain-until-date)을 늘릴 수 있지만 이 날짜는 줄일 수 없습니다.
- \* 법적 증거 자료 보관 \*: 개체 버전에 법적 증거 자료 보관 기능을 적용하면 해당 개체가 즉시 잠깁니다. 예를 들어 조사 또는 법적 분쟁과 관련된 객체에 법적 보류를 지정해야 할 수 있습니다. 법적 보류는 만료 날짜가 없지만 명시적으로 제거될 때까지 유지됩니다. 법적 보류는 보존 기한 과 무관합니다.

이러한 설정에 대한 자세한 내용은 의 ""S3 오브젝트 잠금 사용""을 참조하십시오 ["S3 REST API에서 지원되는 작업 및 제한 사항"](#).

## 레거시 준수 버킷 관리

S3 오브젝트 잠금 기능은 이전 StorageGRID 버전에서 사용할 수 있었던 규정 준수 기능을 대체합니다. 이전 버전의 StorageGRID를 사용하여 준수 버킷을 생성한 경우 이러한 버킷의 설정을 계속 관리할 수 있지만, 더 이상 새로운 준수 버킷을 생성할 수 없습니다. 자세한 내용은 NetApp 기술 자료 문서를 참조하십시오.

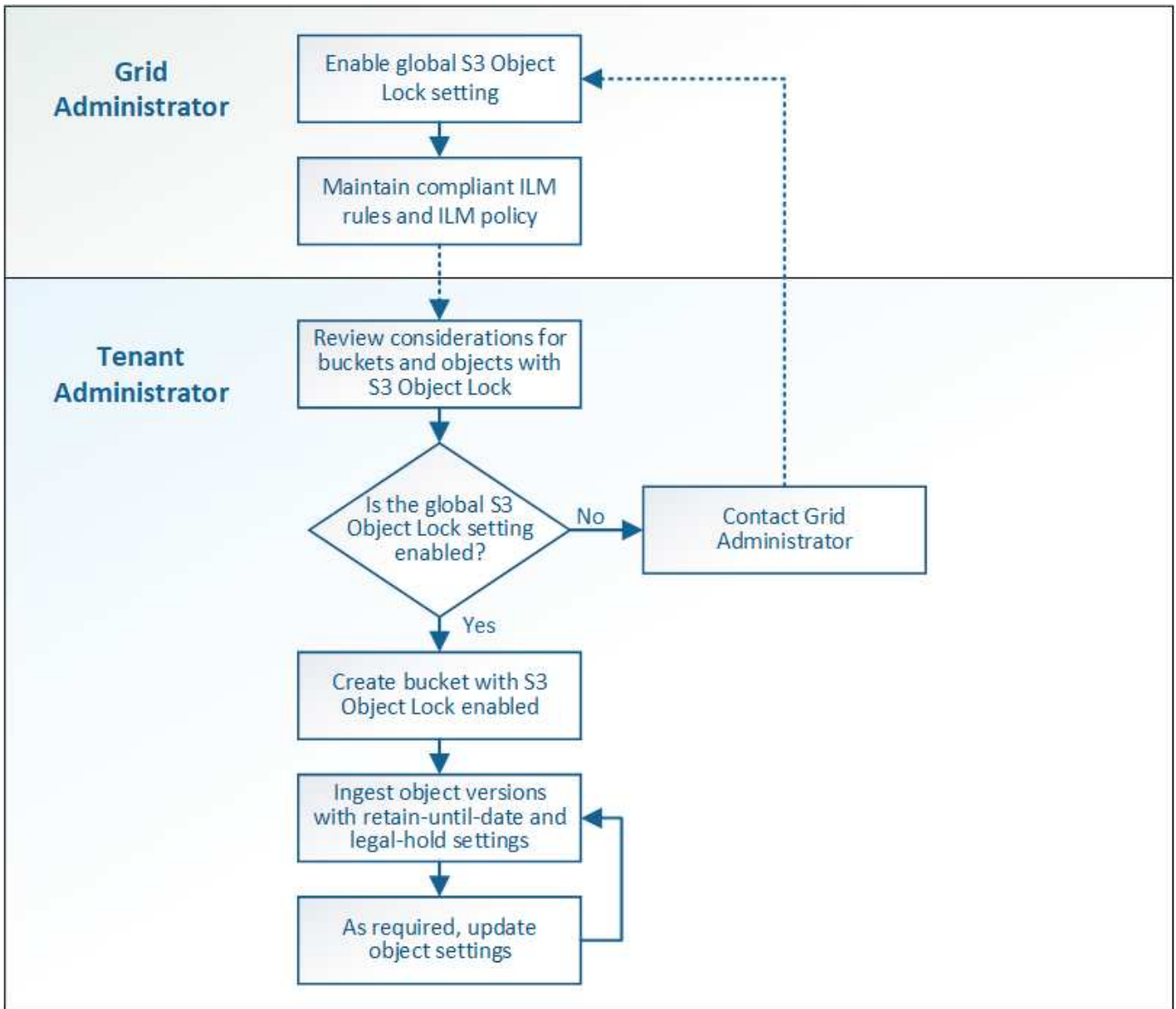
["NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"](#)

## S3 오브젝트 잠금 워크플로

워크플로우 다이어그램은 StorageGRID에서 S3 오브젝트 잠금 기능을 사용하기 위한 상위 단계를 보여줍니다.

S3 오브젝트 잠금이 설정된 버킷을 생성하려면 그리드 관리자가 전체 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 활성화해야 합니다. 또한 그리드 관리자는 정보 수명 주기 관리(ILM) 정책이 "준수"해야 하며, S3 오브젝트 잠금이 활성화된 버킷의 요구 사항을 충족해야 합니다. 자세한 내용은 그리드 관리자에게 문의하거나 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

글로벌 S3 오브젝트 잠금 설정을 활성화한 후 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 있습니다. 그런 다음 S3 클라이언트 애플리케이션을 사용하여 필요에 따라 각 오브젝트 버전에 대한 보존 설정을 지정할 수 있습니다.



관련 정보

"ILM을 사용하여 개체를 관리합니다"

### S3 오브젝트 잠금에 대한 요구사항

버킷에 대해 S3 오브젝트 잠금을 설정하기 전에 S3 오브젝트 잠금 버킷 및 오브젝트에 대한 요구사항과 S3 오브젝트 잠금이 활성화된 버킷에 포함된 오브젝트의 수명 주기를 검토하십시오.

### S3 오브젝트 잠금이 설정된 버킷의 요구 사항

- StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 S3 오브젝트 잠금이 활성화된 버킷을 생성할 수 있습니다.

테넌트 관리자의 이 예에서는 S3 오브젝트 잠금이 설정된 버킷을 보여 줍니다.

# Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock	Region ▾	Object Count	Space Used	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- S3 오브젝트 잠금을 사용하려는 경우 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에 대해 S3 오브젝트 잠금을 활성화할 수 없습니다.
- S3 오브젝트 잠금에서 버킷 버전 관리가 필요합니다. 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 StorageGRID는 해당 버킷의 버전 관리를 자동으로 활성화합니다.
- S3 오브젝트 잠금이 설정된 버킷을 생성한 후에는 해당 버킷에 대한 S3 오브젝트 잠금을 비활성화하거나 버전 관리를 일시 중단할 수 없습니다.
- S3 오브젝트 잠금이 활성화된 StorageGRID 버킷에는 기본 보존 기간이 없습니다. 대신 S3 클라이언트 애플리케이션에서 해당 버킷에 추가되는 각 오브젝트 버전에 대해 보존 날짜 및 법적 보류 설정을 지정할 수도 있습니다.
- S3 오브젝트 라이프사이클 버킷에 대해 버킷 라이프사이클 구성이 지원됩니다.
- S3 오브젝트 잠금이 설정된 버킷에는 CloudMirror 복제가 지원되지 않습니다.

## S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

- S3 클라이언트 애플리케이션은 S3 오브젝트 잠금으로 보호해야 하는 각 오브젝트에 대해 보존 설정을 지정해야 합니다.
- 개체 버전에 대한 보존 기간을 늘릴 수 있지만 이 값을 줄일 수는 없습니다.
- 법적 조치 또는 규제 조사가 보류 중인 경우 개체 버전에 법적 증거 자료를 두어 관련 정보를 보존할 수 있습니다. 개체 버전이 법적 증거 자료 보관 중인 경우, 해당 개체가 보존 기한에 도달한 경우에도 StorageGRID에서 해당 개체를 삭제할 수 없습니다. 법적 증거 자료 보관 기간이 해제됨과 동시에, 보존 기한이 만료된 경우 개체 버전을 삭제할 수 있습니다.
- S3 오브젝트 잠금에는 버전 관리되는 버킷을 사용해야 합니다. 보존 설정은 개별 개체 버전에 적용됩니다. 개체 버전에는 보존 기한 및 법적 보류 설정이 둘 다 있을 수 있으며, 둘 중 하나만 설정할 수도 있고 둘 다 가질 수도 없습니다. 개체에 대한 보존 기한 또는 법적 보류 설정을 지정하면 요청에 지정된 버전만 보호됩니다. 이전 버전의 개체는 잠겨 있는 상태에서 새 버전의 개체를 만들 수 있습니다.

## S3 오브젝트 잠금이 설정된 버킷의 오브젝트 라이프사이클

S3 오브젝트 잠금이 설정된 버킷에 저장된 각 오브젝트는 다음 3단계를 거칩니다.

### 1. \* 오브젝트 수집 \*

- S3 오브젝트 잠금이 설정된 버킷에 오브젝트 버전을 추가할 경우 S3 클라이언트 애플리케이션이 오브젝트에

대한 보존 설정을 선택적으로 지정할 수 있습니다(보존 기한, 법적 보류 또는 둘 다). 그런 다음 StorageGRID에서는 해당 개체의 메타데이터를 생성하며 고유한 UUID(Object Identifier)와 수집 날짜 및 시간이 포함됩니다.

- 보존 설정이 포함된 오브젝트 버전을 수집하면 해당 데이터와 S3 사용자 정의 메타데이터를 수정할 수 없습니다.
- StorageGRID는 오브젝트 메타데이터를 오브젝트 데이터와 독립적으로 저장합니다. 이 기능은 각 사이트에서 모든 오브젝트 메타데이터의 복사본을 3개 유지 관리합니다.

## 2. \* 개체 보존 \*

- 개체의 여러 복사본이 StorageGRID에 저장됩니다. 정확한 복제본 수와 유형 및 스토리지 위치는 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다.

## 3. \* 개체 삭제 \*

- 보존 기한에 도달하면 개체를 삭제할 수 있습니다.
- 법적 증거 자료 보관 중인 개체는 삭제할 수 없습니다.

# S3 버킷 생성

테넌트 관리자를 사용하여 오브젝트 데이터용 S3 버킷을 생성할 수 있습니다. 버킷을 생성할 때 버킷의 이름과 영역을 지정해야 합니다. StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 버킷에 대해 S3 오브젝트 잠금을 선택적으로 활성화할 수 있습니다.

## 필요한 것

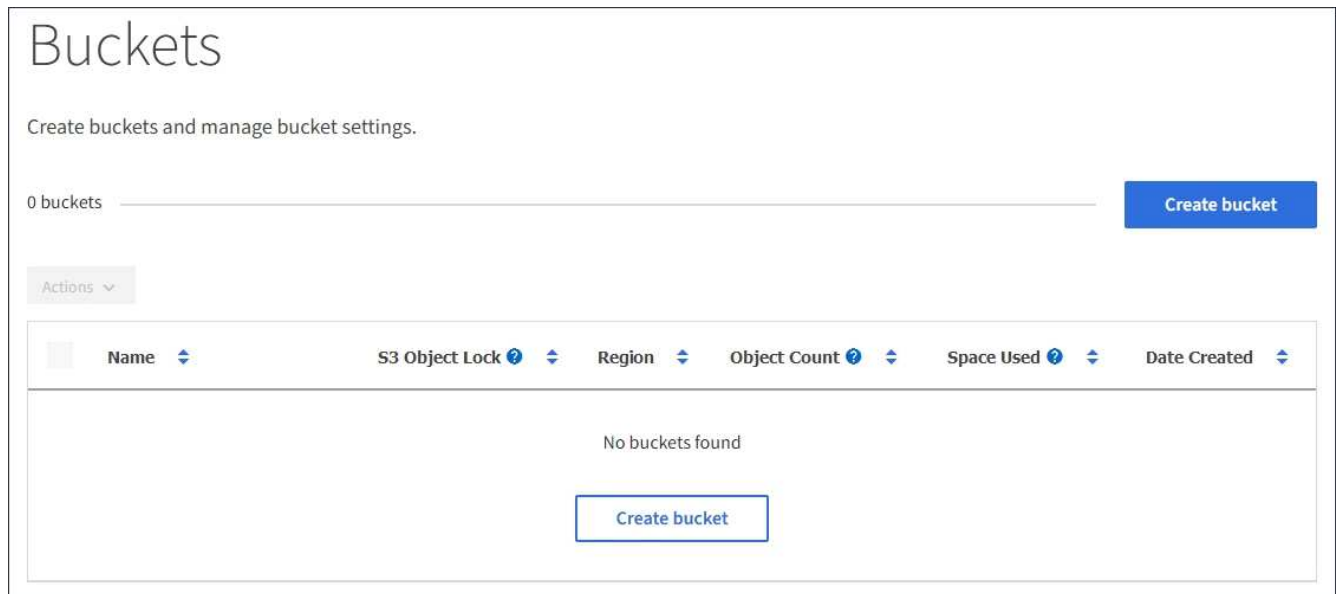
- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- S3 오브젝트 잠금을 사용하여 버킷을 생성하려는 경우 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화되어 있어야 하며 S3 오브젝트 잠금 버킷 및 오브젝트에 대한 요구사항을 검토해야 합니다.

## "S3 오브젝트 잠금 사용"

## 단계

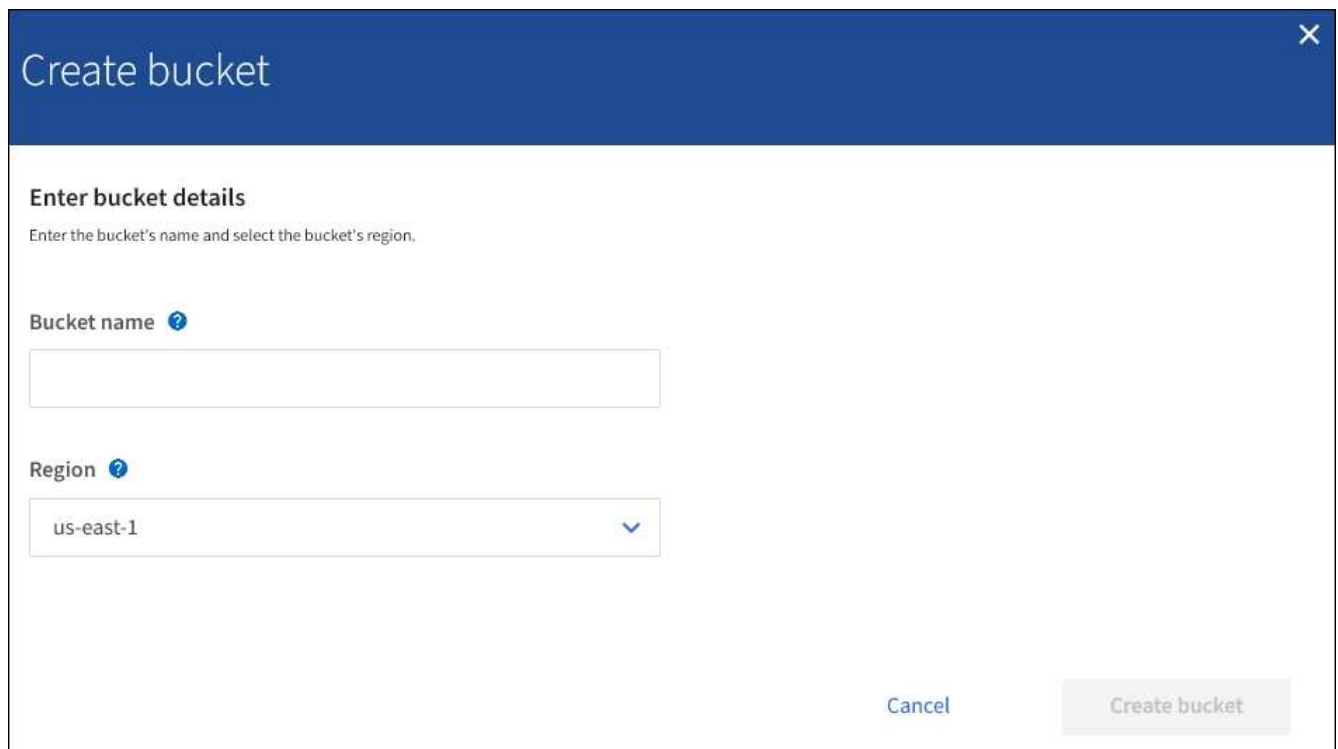
1. 스토리지(S3) \* > \* 버킷 \* 을 선택합니다.

Bucket 페이지가 나타나고 이미 생성된 모든 버킷이 나열됩니다.



2. Create bucket \* 을 선택합니다.

Create Bucket 마법사가 나타납니다.



전역 S3 오브젝트 잠금 설정이 활성화된 경우 버킷 생성에는 버킷의 S3 오브젝트 잠금을 관리하는 두 번째 단계가 포함됩니다.

3. 버킷의 고유한 이름을 입력하십시오.



버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

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.



자세한 내용은 AWS(Amazon Web Services) 문서를 참조하십시오.

#### 4. 이 버킷의 영역을 선택합니다.

StorageGRID 관리자가 사용 가능한 영역을 관리합니다. 버킷 영역은 오브젝트에 적용되는 데이터 보호 정책에 영향을 미칠 수 있습니다. 기본적으로 모든 버킷은 `us-east-1` 지역:



버킷을 생성한 후에는 지역을 변경할 수 없습니다.

#### 5. Create bucket \* 또는 \* Continue \* 를 선택합니다.

- 전역 S3 오브젝트 잠금 설정이 활성화되어 있지 않으면 \* 버킷 생성 \* 을 선택합니다. 버킷이 생성되어 버킷 페이지의 테이블에 추가됩니다.
- 전역 S3 오브젝트 잠금 설정이 활성화된 경우 \* 계속 \* 을 선택합니다. 2단계, S3 오브젝트 잠금 관리 가 나타납니다.

×

## Create bucket

✓ Enter details
2
Manage S3 Object Lock  
Optional

### Manage S3 Object Lock (This step is optional)

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot add or disable S3 Object Lock after a bucket is created.

If S3 Object Lock is enabled, bucket versioning is required and will be enabled automatically.

Enable S3 Object Lock

Previous
Create bucket

6. 필요에 따라 이 버킷에 대해 S3 오브젝트 잠금을 설정하려면 이 확인란을 선택합니다.

S3 클라이언트 애플리케이션이 버킷에 추가된 오브젝트에 대한 보관 종료 날짜 및 법적 보류 설정을 지정하려면 먼저 버킷에 대해 S3 오브젝트 잠금을 활성화해야 합니다.



버킷을 생성한 후에는 S3 오브젝트 잠금을 설정하거나 해제할 수 없습니다.



버킷에 대해 S3 오브젝트 잠금을 설정하면 버킷 버전 관리가 자동으로 활성화됩니다.

7. Create bucket \* 을 선택합니다.

버킷이 생성되어 버킷 페이지의 테이블에 추가됩니다.

관련 정보

["ILM을 사용하여 개체를 관리합니다"](#)

["테넌트 관리 API 이해"](#)

["S3을 사용합니다"](#)

## S3 버킷 세부 정보 보기

테넌트 계정에서 버킷 및 버킷 설정 목록을 볼 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.

단계

1. 스토리지(S3) \* > \* 버킷 \* 을 선택합니다.

Bucket 페이지가 나타나고 테넌트 계정에 대한 모든 버킷이 나열됩니다.

Buckets

Create buckets and manage bucket settings.

2 buckets Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock	Region ▾	Object Count	Space Used	Date Created ▾
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous **1** Next →

## 2. 각 버킷에 대한 정보를 검토합니다.

필요에 따라 모든 열을 기준으로 정보를 정렬하거나 목록 앞뒤에 페이지를 표시할 수 있습니다.

- 이름: 변경할 수 없는 버킷의 고유 이름입니다.
- S3 오브젝트 잠금: 이 버킷에 대해 S3 오브젝트 잠금이 설정되었는지 여부.

전역 S3 오브젝트 잠금 설정이 비활성화된 경우 이 열은 표시되지 않습니다. 또한 이 열에는 레거시 준수 버킷에 대한 정보도 표시됩니다.

- 지역: 변경할 수 없는 버킷의 영역입니다.
- 개체 수: 이 버킷의 오브젝트 수입입니다.
- 사용된 공간: 이 버킷에 있는 모든 오브젝트의 논리적 크기입니다. 논리적 크기에는 복제 또는 삭제 코딩 복사본 또는 오브젝트 메타데이터에 필요한 실제 공간이 포함되지 않습니다.
- 만든 날짜: 버킷을 만든 날짜 및 시간입니다.



표시된 개체 수와 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다.

## 3. 버킷의 설정을 보고 관리하려면 버킷 이름을 선택합니다.

버킷 세부 정보 페이지가 나타납니다.

이 페이지에서는 버킷 옵션, 버킷 액세스 및 플랫폼 서비스에 대한 설정을 보고 편집할 수 있습니다.

각 설정 또는 플랫폼 서비스 구성 지침을 참조하십시오.

Buckets > bucket-02

### Overview

Name:	<b>bucket-02</b>
Region:	<b>us-east-1</b>
S3 Object Lock:	<b>Disabled</b>
Date created:	<b>2020-11-04 14:51:59 MST</b>

**Bucket options** | Bucket access | Platform services

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

관련 정보

"정합성 보장 수준을 변경하는 중입니다"

"마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다"

"CORS(Cross-Origin Resource Sharing) 구성"

"CloudMirror 복제 구성"

"이벤트 알림을 구성하는 중입니다"

"검색 통합 서비스 구성"

## 정합성 보장 수준을 변경하는 중입니다

S3 테넌트를 사용하는 경우 테넌트 관리자 또는 테넌트 관리 API를 사용하여 S3 버킷의 오브젝트에 대해 수행된 작업의 정합성 제어를 변경할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

이 작업에 대해

정합성 보장 레벨은 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트에서 이러한 오브젝트의 일관성 간에 균형을 전환합니다. 일반적으로 버킷에 대해 \* Read-After-new-write \* 정합성 수준을 사용해야 합니다. 새 쓰기 후 읽기 \* 정합성 보장 레벨이 클라이언트 애플리케이션의 요구 사항을 충족하지 않는 경우 버킷 정합성 수준을 설정하거나 을 사용하여 정합성 보장 레벨을 변경할 수 있습니다 Consistency-Control 머리글. 를 클릭합니다 Consistency-Control 헤더는 버킷 정합성 레벨을 오버라이드합니다.



버킷의 정합성 수준을 변경하면 변경 후 수집된 객체만 수정된 레벨에 맞게 보장됩니다.

단계

1. 스토리지(S3) \* > \* 버킷 \* 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.

버킷 세부 정보 페이지가 나타납니다.

3. 버킷 옵션 \* > \* 정합성 보장 레벨 \* 을 선택합니다.

Bucket options
Bucket access
Platform services

Consistency level
Read-after-new-write (default)
⤴

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the Consistency-Control header for an individual API request, which overrides the bucket setting.

- All  
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global  
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site  
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)**  
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

- Available  
Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

4. 이 버킷의 오브젝트에 대해 수행된 작업의 정합성 수준을 선택합니다.

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

정합성 보장 레벨	설명
강력한 사이트	사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
Read-After-new-write (기본값)	새 객체에 대한 읽기-쓰기 후 정합성 보장 및 객체 업데이트에 대한 최종 정합성 보장 기능을 제공합니다. 예서는 고가용성을 제공하고 데이터 보호 보장을 제공합니다. Amazon S3 일관성 보장 과 일치합니다.  <ul style="list-style-type: none"> <li>참고: * 응용 프로그램이 존재하지 않는 키에 대해 헤드 작업을 시도하는 경우, Amazon S3 정합성 보장 기능이 필요하지 않는 한 정합성 보장 수준을 * 사용 가능 * 으로 설정합니다. 그렇지 않으면 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다.</li> </ul>
사용 가능(헤드 작업의 최종 일관성)	는 * Read-After-new-write * 정합성 수준과 동일하게 작동하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 * Read-After-new-write * 보다 헤드 작업에 더 높은 가용성을 제공합니다. 헤드 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

5. 변경 내용 저장 \* 을 선택합니다.

관련 정보

["테넌트 관리 권한"](#)

## 마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다

그리드 관리자가 StorageGRID 시스템에 대한 ILM(정보 수명 주기 관리) 규칙을 만들 때 오브젝트의 마지막 액세스 시간을 사용하여 해당 오브젝트를 다른 스토리지 위치로 이동할지 여부를 결정하도록 선택적으로 지정할 수 있습니다. S3 테넌트를 사용하는 경우 S3 버킷의 오브젝트에 대한 마지막 액세스 시간 업데이트를 활성화하여 이러한 규칙을 활용할 수 있습니다.

이 지침은 배치 지침에서 \* Last Access Time \* 옵션을 사용하는 ILM 규칙을 하나 이상 포함하는 StorageGRID 시스템에만 적용됩니다. StorageGRID 시스템에 이러한 규칙이 포함되어 있지 않으면 이 지침을 무시할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- 마지막 액세스 시간 \* 은 ILM 규칙에 대한 \* 참조 시간 \* 배치 명령에 사용할 수 있는 옵션 중 하나입니다. 규칙의 참조 시간을 마지막 액세스 시간으로 설정하면 그리드 관리자는 해당 개체를 마지막으로 검색한 시기(읽기 또는 보기)에 따라 특정 저장소 위치에 개체가 배치되도록 지정할 수 있습니다.

예를 들어, 최근에 본 오브젝트를 더 빠른 스토리지에 유지하기 위해 그리드 관리자는 다음을 지정하는 ILM 규칙을 생성할 수 있습니다.

- 지난 달 동안 검색된 객체는 로컬 스토리지 노드에 남아 있어야 합니다.
- 지난 달에 검색되지 않은 객체는 오프 사이트 위치로 이동해야 합니다.



정보 수명 주기 관리를 사용하여 개체를 관리하는 방법에 대한 지침을 참조하십시오.

기본적으로 마지막 액세스 시간에 대한 업데이트는 사용되지 않습니다. StorageGRID 시스템에 \* Last Access Time \* 옵션을 사용하는 ILM 규칙이 포함되어 있고 이 옵션이 이 버킷의 오브젝트에 적용되도록 하려면 해당 규칙에 지정된 S3 버킷에 대한 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다.



개체가 검색될 때 마지막 액세스 시간을 업데이트하면 특히 작은 개체의 StorageGRID 성능이 저하될 수 있습니다.

StorageGRID는 객체가 검색될 때마다 다음 추가 단계를 수행해야 하므로 마지막 액세스 시간 업데이트 시 성능 영향이 발생합니다.

- 객체를 새 타임스탬프로 업데이트합니다
- ILM 대기열에 개체를 추가하여 현재 ILM 규칙 및 정책에 대해 다시 평가할 수 있습니다

이 표에는 마지막 액세스 시간이 비활성화되거나 활성화될 때 버킷의 모든 오브젝트에 적용되는 동작이 요약되어 있습니다.

요청 유형입니다	마지막 액세스 시간이 비활성화된 경우의 동작(기본값)		마지막 액세스 시간이 설정된 경우의 동작	
	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?
개체, 해당 액세스 제어 목록 또는 해당 메타데이터를 검색하는 요청입니다	아니요	아니요	예	예
개체의 메타데이터를 업데이트하도록 요청합니다	예	예	예	예
한 버킷에서 다른 버킷으로 오브젝트 복사 요청	<ul style="list-style-type: none"> <li>• 아니요, 소스 복제본입니다</li> <li>• 예, 대상 복사본에 대해입니다</li> </ul>	<ul style="list-style-type: none"> <li>• 아니요, 소스 복제본입니다</li> <li>• 예, 대상 복사본에 대해입니다</li> </ul>	<ul style="list-style-type: none"> <li>• 예, 소스 복제본에 대해 가능합니다</li> <li>• 예, 대상 복사본에 대해입니다</li> </ul>	<ul style="list-style-type: none"> <li>• 예, 소스 복제본에 대해 가능합니다</li> <li>• 예, 대상 복사본에 대해입니다</li> </ul>
여러 부분 업로드를 완료하도록 요청합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다

단계

1. 스토리지(S3) \* > \* 버킷 \* 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.

버킷 세부 정보 페이지가 나타납니다.

3. Bucket options \* > \* Last access time updates \* 를 선택합니다.
4. 마지막 액세스 시간 업데이트를 활성화하거나 비활성화하려면 해당 라디오 버튼을 선택합니다.

The screenshot shows the 'Bucket options' tab in the AWS S3 console. The 'Consistency level' is set to 'Read-after-new-write'. The 'Last access time updates' section is expanded, showing 'Disabled' as the current setting. A yellow warning box states: 'Updating the last access time when an object is retrieved can reduce performance, especially for small objects.' Two radio buttons are visible: 'Enable last access time updates when retrieving an object' (unselected) and 'Disable last access time updates when retrieving an object' (selected). A 'Save changes' button is at the bottom right.

5. 변경 내용 저장 \* 을 선택합니다.

관련 정보

["테넌트 관리 권한"](#)

["ILM을 사용하여 개체를 관리합니다"](#)

## CORS(Cross-Origin Resource Sharing) 구성

다른 도메인의 웹 애플리케이션에서 해당 버킷의 버킷 및 오브젝트에 액세스할 수 있도록 하려면 S3 버킷에 대해 CORS(Cross-Origin Resource Sharing)를 구성할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

이 작업에 대해



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 CORS를 구성합니다 Images 버킷을 사용하면 버킷의 이미지를 웹 사이트에 표시할 수 있습니다 <http://www.example.com>.

## 단계

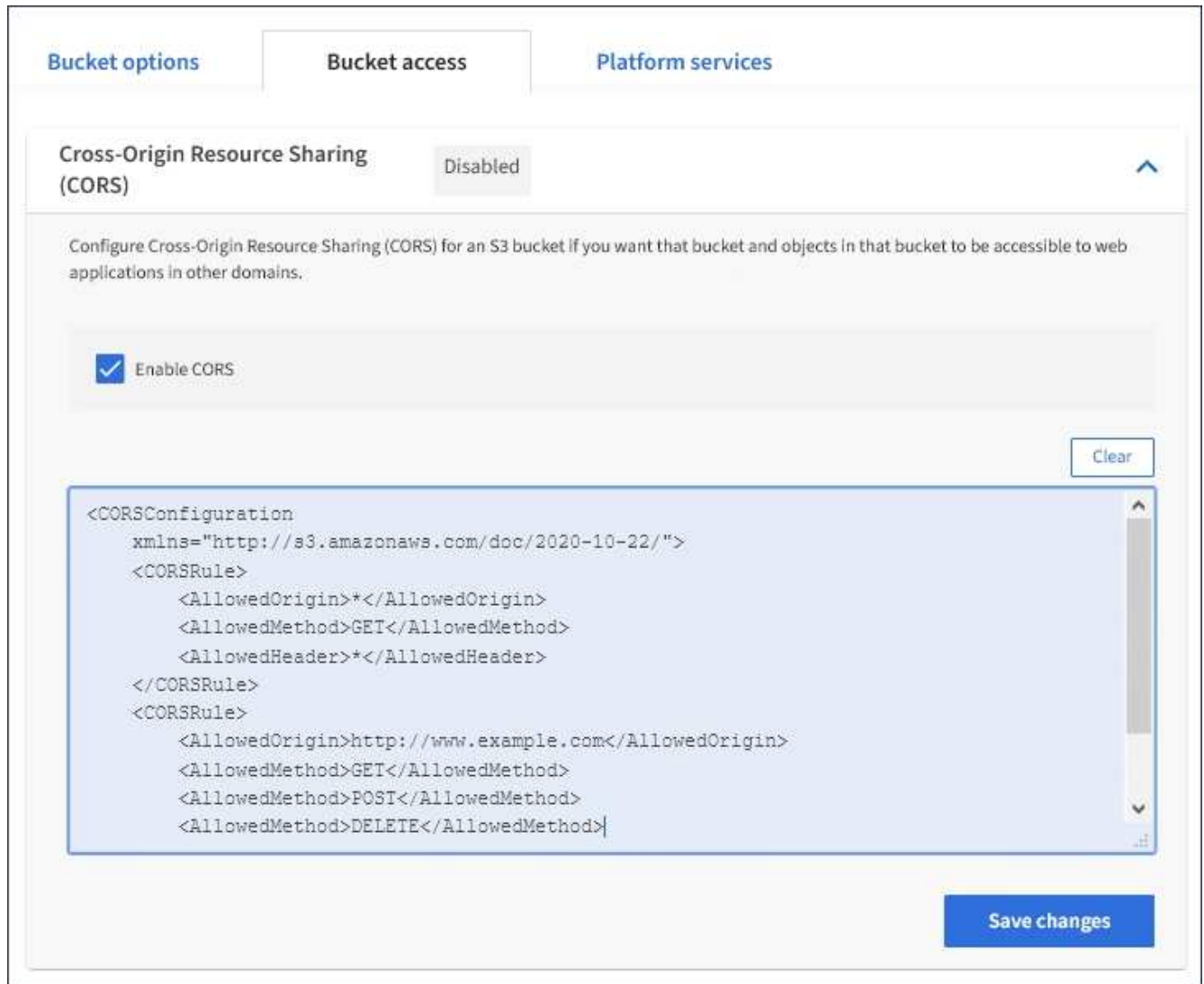
1. 텍스트 편집기를 사용하여 CORS를 활성화하는 데 필요한 XML을 만듭니다.

이 예에서는 S3 버킷에 대해 CORS를 활성화하는 데 사용되는 XML을 보여 줍니다. 이 XML을 사용하면 모든 도메인에서 버킷에 GET 요청을 보낼 수 있지만 만 허용됩니다 <http://www.example.com> POST를 전송하고 요청을 삭제하는 도메인입니다. 모든 요청 헤더가 허용됩니다.

```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

CORS 구성 XML에 대한 자세한 내용은 을 참조하십시오 ["AWS\(Amazon Web Services\) 문서: Amazon Simple Storage Service 개발자 가이드 를 참조하십시오"](#).

2. 테넌트 관리자에서 \* 스토리지(S3) \* > \* 버킷 \* 을 선택합니다.
3. 목록에서 버킷 이름을 선택합니다.  
  
버킷 세부 정보 페이지가 나타납니다.
4. Bucket access \* > \* Cross-Origin Resource Sharing (CORS) \* 를 선택합니다.
5. CORS \* 활성화 확인란을 선택합니다.
6. 텍스트 상자에 CORS 구성 XML을 붙여 넣고 \* 변경 내용 저장 \* 을 선택합니다.



7. 버킷의 CORS 설정을 수정하려면 텍스트 상자에서 CORS 구성 XML을 업데이트하거나 다시 시작하려면 \* Clear \* 를 선택하십시오. 그런 다음 \* 변경 사항 저장 \* 을 선택합니다.
8. 버킷에 대한 CORS를 비활성화하려면 \* CORS \* 활성화 확인란의 선택을 취소한 다음 \* 변경 사항 저장 \* 을 선택합니다.

## S3 버킷을 삭제하는 중입니다

테넌트 관리자를 사용하여 비어 있는 S3 버킷을 삭제할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

이 작업에 대해

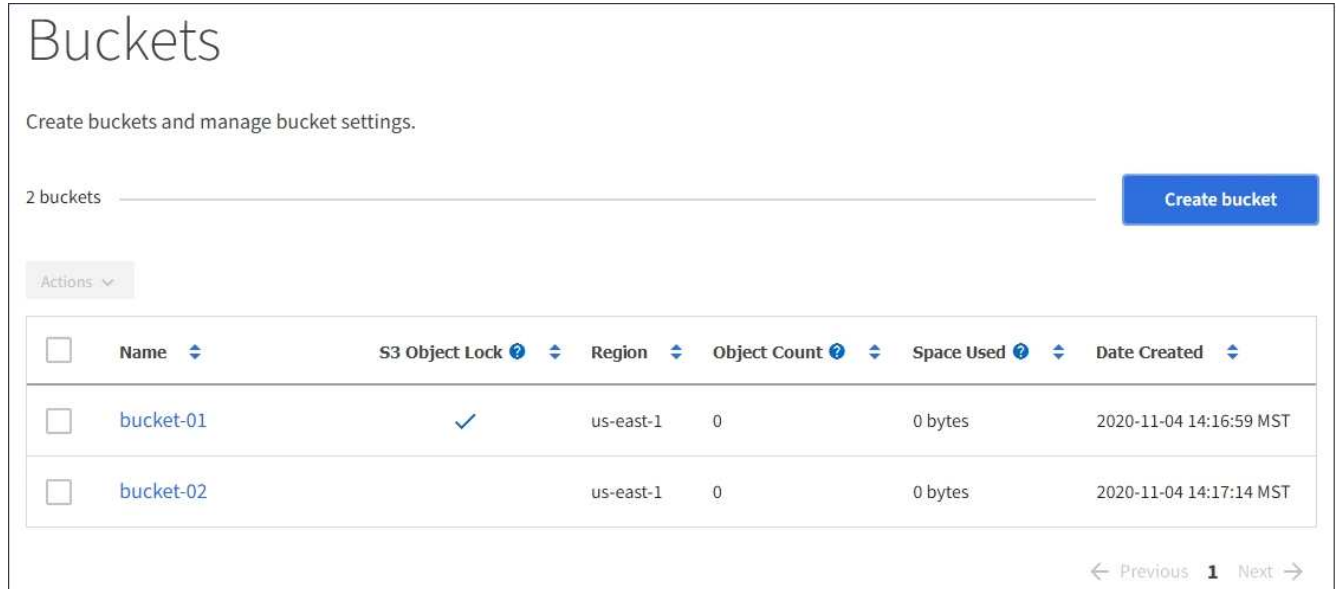
다음 지침은 Tenant Manager를 사용하여 S3 버킷을 삭제하는 방법을 설명합니다. 테넌트 관리 API 또는 S3 REST API를 사용하여 S3 버킷을 삭제할 수도 있습니다.

오브젝트 또는 비최신 오브젝트 버전이 포함된 S3 버킷을 삭제할 수 없습니다. S3 버전 오브젝트를 삭제하는 방법에 대한 자세한 내용은 정보 수명 주기 관리를 사용하여 오브젝트를 관리하는 지침을 참조하십시오.

단계

1. 스토리지(S3) \* > \* 버킷 \* 을 선택합니다.

Bucket 페이지가 나타나고 기존의 모든 S3 버킷을 표시합니다.




The screenshot shows the AWS S3 Buckets console. At the top, it says "Buckets" and "Create buckets and manage bucket settings." Below this, it indicates "2 buckets" and has a "Create bucket" button. There is an "Actions" dropdown menu. The main content is a table with the following columns: Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The table contains two rows: "bucket-01" and "bucket-02". Both buckets are in the "us-east-1" region, have 0 objects, and 0 bytes of space used. The creation dates are "2020-11-04 14:16:59 MST" and "2020-11-04 14:17:14 MST" respectively. At the bottom right, there are navigation arrows and a page number "1".

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

2. 삭제할 빈 버킷의 확인란을 선택합니다.

작업 메뉴가 활성화됩니다.

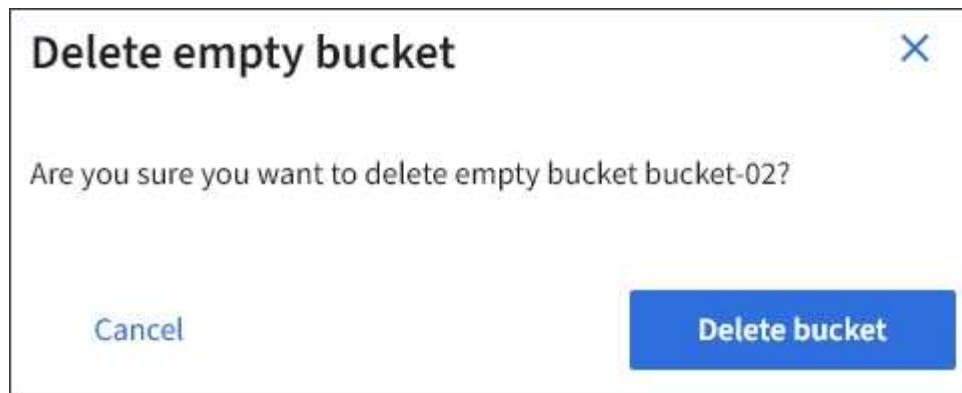
3. 작업 메뉴에서 \* 빈 버킷 삭제 \* 를 선택합니다.



The screenshot shows the AWS S3 Buckets console with the "Actions" dropdown menu open. The menu is positioned over the "bucket-02" row. The menu item "Delete empty bucket" is highlighted. The table content is the same as in the previous screenshot, but the checkbox for "bucket-02" is now checked.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

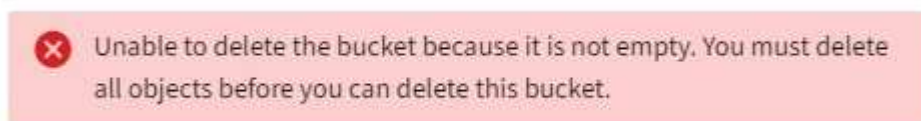
확인 메시지가 나타납니다.



4. 버킷을 삭제하려면 \* 버킷 삭제 \* 를 선택합니다.

StorageGRID가 버킷이 비어 있음을 확인한 다음 버킷을 삭제합니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

버킷이 비어 있지 않으면 오류 메시지가 나타납니다. 버킷을 삭제하려면 먼저 모든 오브젝트를 삭제해야 합니다.



관련 정보

["ILM을 사용하여 개체를 관리합니다"](#)

## 저작권 정보

Copyright © 2024 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.