



심층 분석: Amazon S3 및 AWS CLI

학습 내용

강의의 핵심

배울 내용은 다음과 같습니다.

- Amazon S3를 정의합니다.
- 서로 다른 객체 스토리지 클래스를 구분합니다.
- Amazon S3의 특징을 파악합니다.
- Amazon S3 데이터 모델 개념을 설명합니다.
- Amazon S3의 이점을 요약합니다.
- Amazon S3 버전 관리와 S3 Intelligent-Tiering의 차이점을 개괄적으로 설명합니다.
- AWS CLI를 사용하여 Amazon Simple Storage Service(Amazon S3) 객체를 저장, 검색, 아카이브하는 방법을 파악합니다.

주제:


- Amazon S3
- AWS Command Line Interface(AWS CLI)

주요 용어:

- Amazon S3 Intelligent-Tiering
- Amazon S3 버전 관리
- Amazon S3 객체 잠금
- Amazon S3 스탠더드
- Amazon S3 스탠더드 - 저빈도 액세스(S3 스탠더드 - IA)
- Amazon S3 단일 영역 - 저빈도 액세스(S3 단일 영역 - IA)
- 버킷
- 객체
- 키
- 버전 관리 비활성화됨
- GET 요청
- API



Amazon S3 검토



Amazon S3는 인터넷을 통해 언제 어디서든 원하는 양의 데이터(객체)를 저장하고 검색하는 데 사용할 수 있습니다.

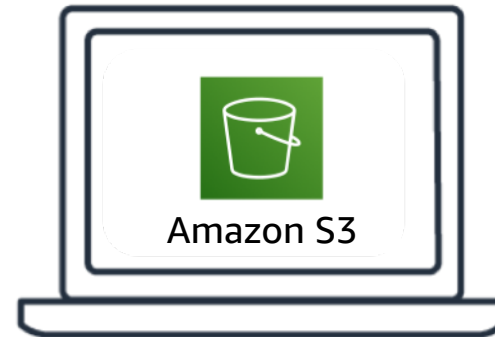
객체 스토리지 클래스



Amazon S3의 특징

Amazon S3의 특징은 다음과 같습니다.

- 어디서든 액세스할 수 있음(AWS 내부 및 외부 모두에서)
- 중복 스토리지로 인해 내구성이 우수함(11 9s의 내구성을 보장하도록 설계)
- 가용성이 높음(4 9s의 가용성을 보장하도록 설계)
- 데이터 저장량에 제한이 없음
- 객체당 최대 5TB



Amazon S3의 개념

버킷 및 객체

버킷

버킷은 Amazon S3에 저장된 객체의 컨테이너입니다. 어떤 객체든 버킷에 포함됩니다.

예를 들어, `photos/puppy.jpg`라는 객체가 미국 서부(오레곤) 리전의 `awsexamplebucket1` 버킷에 저장되었다면 주소는 다음 URL과 같이 표현될 수 있습니다.

`https://awsexamplebucket1.s3.us-west-2.amazonaws.com/photos/puppy.jpg`.

객체

객체는 Amazon S3에 저장되는 기본 엔터티입니다. 객체는 객체 데이터와 메타데이터로 구성됩니다. 데이터 부분은 Amazon S3에서 볼 수 없습니다. 메타데이터는 객체를 설명하는 이름 값 페어의 집합입니다. 객체는 키(이름)와 버전 ID로 버킷 내에서 고유하게 식별됩니다.



키 및 리전

키

키는 버킷 내 객체의 고유한 식별자입니다. 버킷 내 각 객체는 정확히 하나의 키를 갖습니다. 버킷, 키, 버전 ID의 조합이 각 객체를 고유하게 식별합니다. 따라서 Amazon S3를 **버킷 + 키 + 버전**과 객체 그 자체에 있는 정보 사이의 기본적인 데이터 맵이라고 생각하면 됩니다.

다음 URL을 예로 들어보겠습니다.

<https://DOC-EXAMPLE-BUCKET.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl>

- DOC-EXAMPLE-BUCKET은 버킷의 이름입니다.
- 2006-03-01/AmazonS3.wsdl은 객체의 키입니다.

리전

리전은 Amazon S3가 사용자가 생성한 버킷을 저장하는 지리적인 AWS 리전입니다. 한 리전에 저장된 객체는 명시적으로 다른 리전으로 전송하지 않는 한 해당 리전을 벗어나지 않습니다.

예를 들어, 유럽(아일랜드) 리전에 저장된 객체는 유럽 밖으로 이동하지 않습니다.



Amazon S3의 이점

Amazon S3의 이점은 다음과 같습니다.

버킷 만들기 - 데이터를 저장하는 버킷을 만들고 해당 버킷의 이름을 지정합니다. 버킷은 데이터 스토리지를 위한 Amazon S3의 기본 컨테이너입니다.

데이터 저장 - 버킷에 데이터를 사실상 무제한으로 저장합니다. 각 객체에 최대 5TB의 데이터를 포함할 수 있습니다. 고유한 개발자 할당 키를 사용하여 각 객체를 저장 및 검색합니다.

데이터 다운로드 - 데이터를 직접 다운로드하거나 다른 사람이 다운로드할 수 있게 합니다. 언제든지 데이터를 직접 다운로드하거나 다른 사람이 다운로드하도록 허용할 수 있습니다.

권한 - 데이터를 S3 버킷을 상대로 업로드 또는 다운로드하려는 사용자에게 액세스 권한을 부여하거나 거부합니다. 세 가지 유형의 사용자에게 업로드 및 다운로드 권한을 부여할 수 있습니다. 사용 권한 메커니즘을 사용하면 데이터가 무단으로 액세스되지 않도록 보호하는 데 도움이 될 수 있습니다.

표준 인터페이스 - 모든 인터넷 개발 도구 키트에서 사용할 수 있도록 설계된 표준 기반 REST 및 SOAP 인터페이스를 사용합니다.



버전 관리 및 S3 Intelligent-Tiering

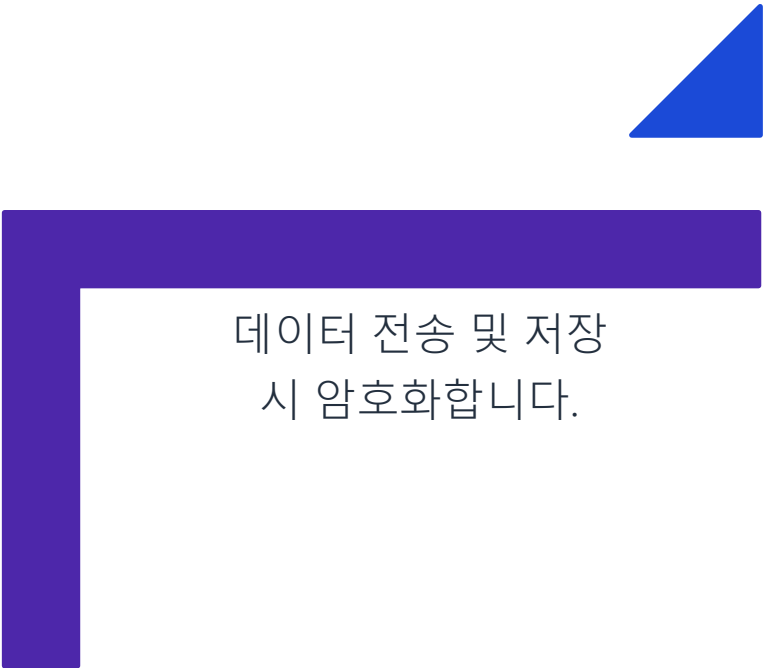
Amazon S3 버전 관리

Amazon S3 버전 관리는 실수로 덮어쓰거나 삭제하는 것을 방지합니다.

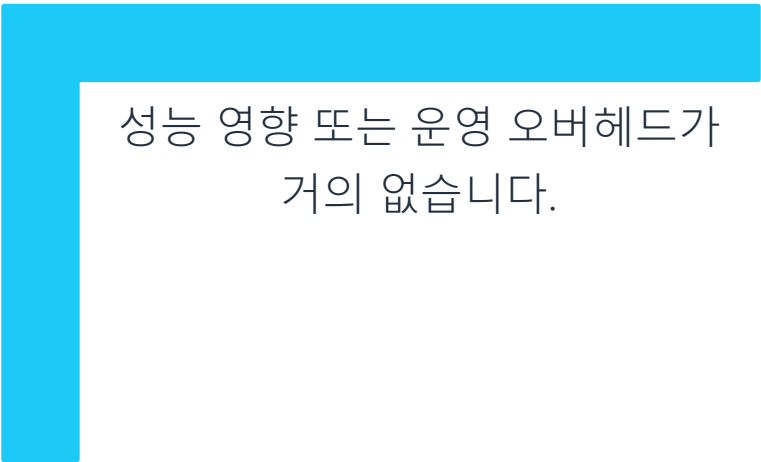
작업	버전 관리 활성화됨	버전 관리 비활성화됨 또는 버전 관리가 일시 중지됨
동일한 키를 사용하여 객체 업로드	<ul style="list-style-type: none">다른 버전 ID로 새 객체를 생성합니다.둘 다 버전 ID로 검색 가능합니다.	<ul style="list-style-type: none">원본 객체를 덮어씁니다.이전 객체를 검색할 수 없게 됩니다.
삭제	<ul style="list-style-type: none">삭제 마커를 추가합니다.그러나 여전히 버전 ID로 객체를 검색할 수 있습니다.	<ul style="list-style-type: none">객체를 삭제합니다.객체를 더 이상 검색할 수 없게 됩니다.

S3 Intelligent-Tiering

S3 Intelligent-Tiering은 데이터를 가장 비용 효율적인 액세스 계층으로 자동으로 이동시킵니다.



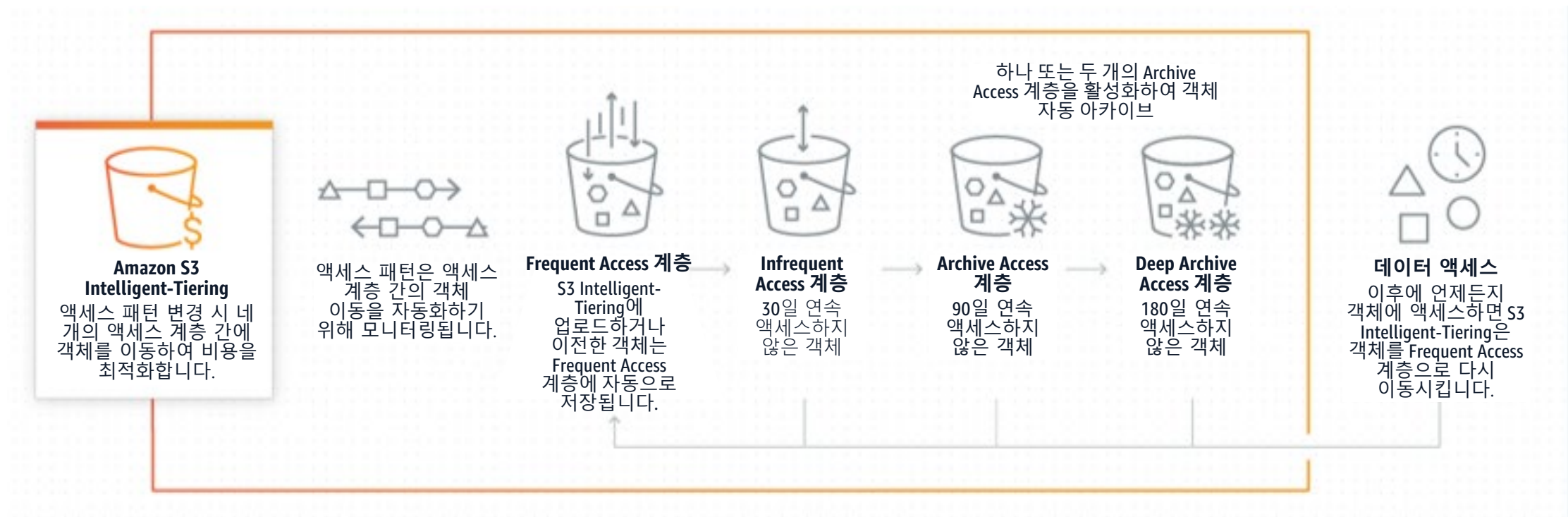
데이터 전송 및 저장
시 암호화합니다.



성능 영향 또는 운영 오버헤드가
거의 없습니다.

작동 원리

S3 Intelligent-Tiering





엑세스 및 객체

Amazon S3 퍼블릭 액세스 차단

퍼블릭 액세스 차단(버킷 설정)

퍼블릭 액세스는 액세스 제어 목록(ACL), 버킷 정책, 액세스 포인트 정책 또는 그 외 모든 것을 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체에 대해 퍼블릭 액세스를 차단하려면 '모든 퍼블릭 액세스 차단'을 켜십시오. 이 설정은 이 버킷과 해당 액세스 포인트에만 적용됩니다. AWS에서는 '모든 퍼블릭 액세스 차단'을 켜는 것이 좋지만 이러한 설정을 적용하기 전에 애플리케이션이 퍼블릭 액세스 없이도 제대로 작동하는지 확인하십시오. 버킷이나 내부의 객체에 어느 정도 퍼블릭 액세스가 필요한 경우, 특정 스토리지 용례에 맞게 아래의 개별 설정을 사용자 지정할 수 있습니다. [자세히 알아보기](#)

편집

모든 퍼블릭 액세스 차단

☑ 켜짐

새로운 액세스 제어 목록(ACL)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

☑ 켜짐

모든 액세스 제어 목록(ACL)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

☑ 켜짐

새로운 퍼블릭 버킷 또는 액세스 포인트 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

☑ 켜짐

모든 퍼블릭 버킷 또는 액세스 포인트 정책을 통해 버킷 및 객체에 대한 퍼블릭 액세스 및 교차 계정 액세스 차단

☑ 켜짐

Amazon S3 퍼블릭 액세스 설정

새 퍼블릭 ACL 및 퍼블릭 객체 업로드 차단

퍼블릭 ACL을 통해 부여된 퍼블릭 액세스 권한 제거

새 퍼블릭 버킷 정책 차단

퍼블릭 정책이 있는 버킷에 대한 퍼블릭 액세스 및 교차 계정 액세스 차단

Amazon S3 객체 잠금

- 한 번 쓰고 여러 번 읽기(WORM) 모델을 사용하여 객체 저장
- 버킷이 생성되는 시점에 활성화

객체 보존을 관리하는
두 가지 방법:

- 보존
- 법적 보존

2가지 보존 모드:

- 규정 준수
- 거버넌스

Amazon S3에 대한 이벤트 알림

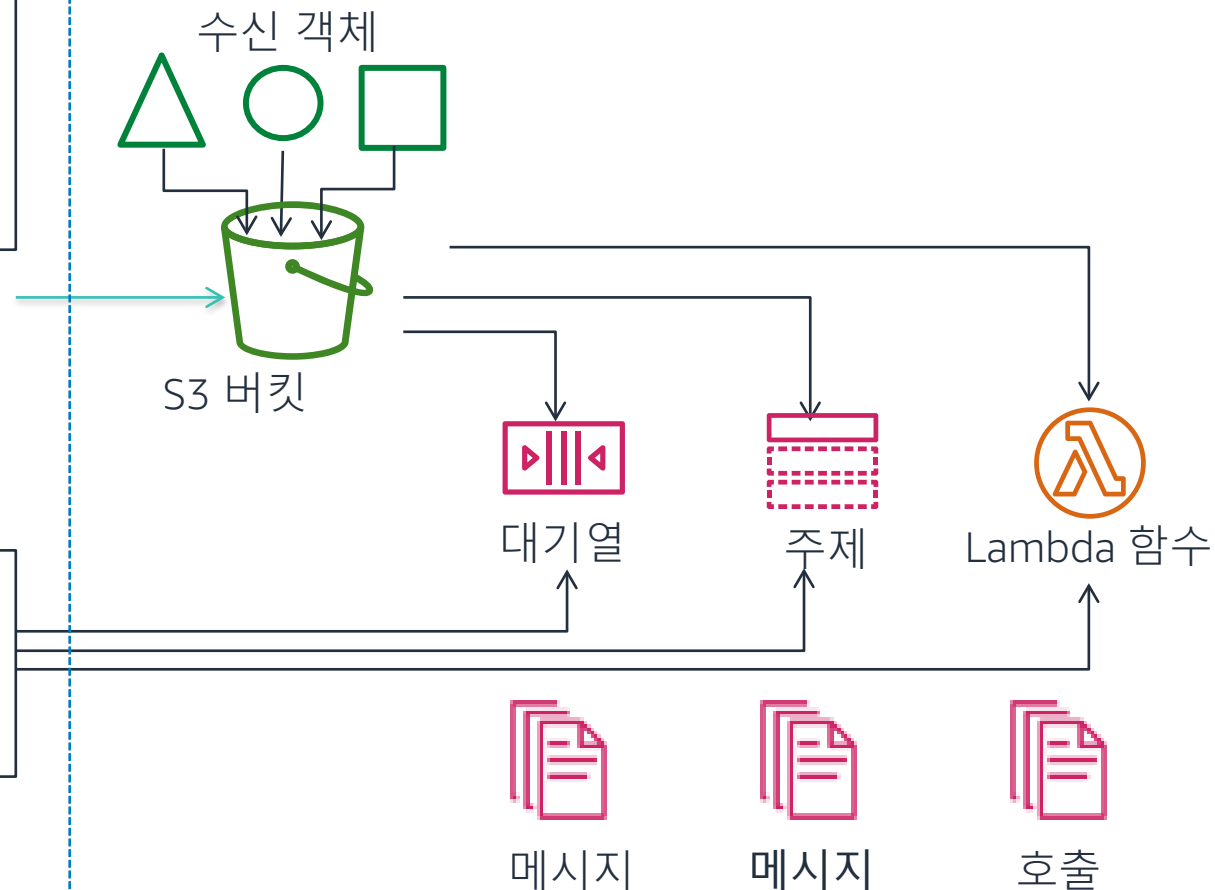
다음과 같이 객체가 변경될 경우 알림이 발행되도록 버킷 구성

- 추가됨
- 삭제됨
- 덮어써짐

알림은 다음으로 직접 발행될 수 있음

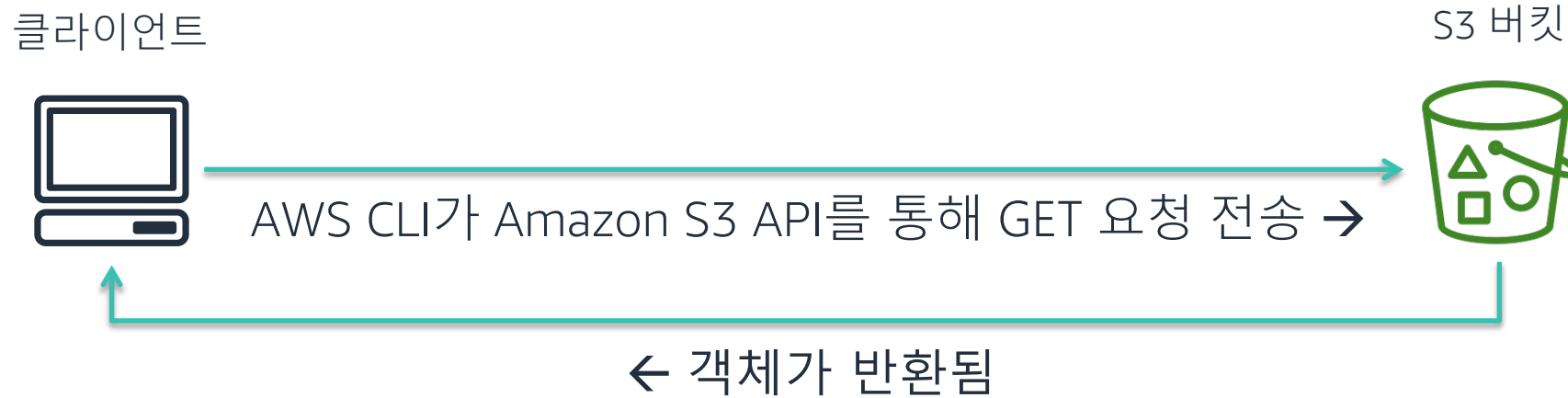
- Amazon Simple Queue Service(Amazon SQS) 대기열
- Amazon Simple Notification Service(Amazon SNS) 주제
- AWS Lambda 함수

리전



Amazon S3 및 AWS CLI

Amazon S3에 있는 객체에 액세스



Amazon S3에 대한 AWS CLI 명령

- 새 버킷 생성:

```
aws s3 mb s3://mybucket
```

- AWS 계정의 모든 버킷 나열:

```
aws s3 ls
```

- Amazon S3에 로컬 파일 복사:

```
aws s3 cp file.txt  
s3://mybucket/myprefix/file.txt
```

- 지정된 버킷 및 접두부(prefix) 아래의 객체를 현재 로컬 디렉터리에 동기화:

```
aws s3 sync s3://mybucket/myprefix/
```

- 버킷에서 객체 제거:

```
aws s3 rm  
s3://mybucket/myprefix/file.txt
```

특정 스토리지 클래스로 객체 생성

copy 명령과 `--storage-class` 파라미터를 사용하여 스토리지 클래스 지정

```
aws s3 cp file.txt s3://mybucket/myprefix/file.txt  
--storage-class INTELLIGENT_TIERING
```

s3api 명령

s3api 명령:

- Amazon S3 API에 대한 직접 액세스 제공
- `aws s3` 로 인해 노출되지 않는 작업 활성화

aws s3api

`create-multipart-upload`

`put-object-acl`

`put-bucket-policy`

`list-object-versions`

Amazon S3의 추가 기능

Amazon S3의 추가 기능

기능	목적 또는 이점	사용 방법
객체 수명 주기 관리	<ul style="list-style-type: none">수명 주기 내내 객체가 비용 효율적으로 저장되도록 객체 관리	<ul style="list-style-type: none">다음 시기를 정의하는 규칙으로 수명 주기 구성 생성<ul style="list-style-type: none">객체가 다른 스토리지 클래스로 전환해야 하는 시기객체가 삭제되어야 하는 시기
미리 서명된 객체 URL	<ul style="list-style-type: none">AWS 보안 인증 정보 또는 권한이 없는 사용자와 프라이빗 객체 공유	<ul style="list-style-type: none">프로그래밍 방식으로 미리 서명된 객체 URL 생성객체에 액세스할 수 있도록 미리 서명된 객체 URL을 수신자에게 제공
교차 오리진 리소스 공유(CORS)	<ul style="list-style-type: none">CORS를 지원하기 위해 정적 웹 사이트를 호스트하는 S3 버킷 허용한 버킷에 여러 오리진 지원	<ul style="list-style-type: none">다음을 지정하는 규칙으로 버킷에 CORS 구성 생성<ul style="list-style-type: none">사용 권한이 있는 오리진HTTP 작업

핵심 사항



- Amazon S3는 리전별로 프로비저닝된 객체 스토리지 서비스입니다.
- 내구성과고가용성이 필요하다면 Amazon S3를 사용하십시오.
- 버킷은 객체를 저장하고 버킷에 있는 객체의 고유 식별자로 키를 사용합니다.
- Amazon S3는 여러 스토리지 클래스와 버전 관리, 객체 잠금, 이벤트 알림 기능을 제공합니다.