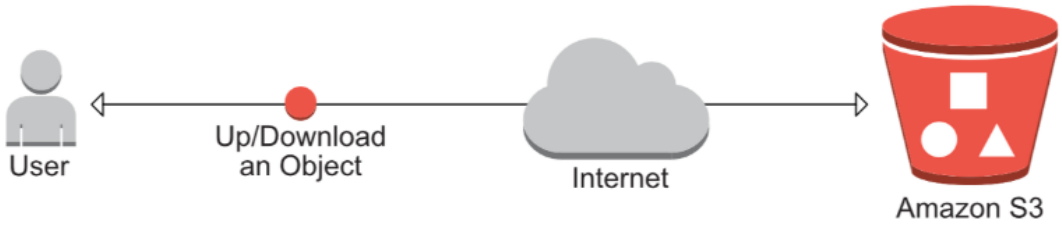
[AWS] 3. AWS 스토리지

- **References**
  - AWS 공인 솔루션스 아키텍트 스터디 가이드 - 어소시에이트 3/e - 3장
  - https://inpa.tistory.com/entry/AWS-📚-S3-버킷-생성-사용법-실전-구축?category=947443

- **AWS Simple Stroage Service (S3) 개요**
  - EC2 의 인스턴스 OS 볼륨이 블록 스토리지인 반면, S3는 객체 스토리지 라는 차이점
  - 객체 스토리지에는 어떤 형태의 데이터라도 저장 가능하다
  - S3는 파일을 버킷에 저장한다
  - 파일 저장 시 2KB의 메타데이터도 함께 저장, 메타데이터는 데이터 퍼미션, 버킷 내 파일 시스템에서의 위치 등의 정보를 키형식으로 제공한다.

- **AWS S3 서비스**

- 온라인 오브젝트 스토리지 서비스 (Object Storage)
- 데이터를 온라인으로 오브젝트 형태로 저장하는 서비스
- 데이터 조작에 HTTP/HTTPS 를 통한 API가 사용 된다.
- 비용도 저렴하고, 저장 가능한 데이터 양이 무한에 가깝다.
- S3는 파일을 버킷에 저장
- 다른 서비스와 마찬가지로 가용 버킷 수를 증가하고자 할때 AWS측에 요청 할 수 있다.
- S3 자체가 수천 대 이상의 성능 좋은 웹서버로 구성되어 있어, EC2 + EBS 구축 했을 때 처럼 Auto Scaling 과 Load Balancing 에 신경 쓰지 않아도 된다.



- 사용 용도 예시
  - 클라우드 저장소 (On-Premise 환경의 재난 복구 전용 데이터 백업)
  - 서비스 대용량 파일 저장소 (이미지, 동영상, 빅데이터 등)
  - 서비스 사용 로그 저장 및 분석
  - 정적 웹사이트 호스팅

    → 동적 웹페이지는 EC2, 정적 웹페이지는 S3에서 이용하여 성능을 높이고 비용을 절감
  - EBS 스냅샷의 저장 영역
  - AWS 아데나를 이용한 빅 데이터 업로드 및 분석, 데이터소스로 활용
  - AWS Glacier와 연동으로 비용 절감 및 규정 준수 가능
  - Auto Scaling 을 활용한 EC2 인스턴스의 로그 저장

- **객체 스토리지의 특징 (Amazon EBS (블록스토리지) 와 비교)**

	Amazon EBS	Amazon S3
스토리지	파일 시스템이 있는 블록 스토리지	객체 스토리지
성능	매우 빠름	빠름
중복성	가용 영역의 여러서버에 걸쳐 있음	리전 내 여러시설에 걸쳐 있음
보안	EBS 암호화 - 데이터 볼륨 및 스냅샷	암호화
인터넷 액세스 가능 여부	불가능	가능
일반적 사용 사례	디스크 드라이브	온라인 스토리지 (프로그램을 설치해서 저장하는 기능은 없음)
비용	-	EC2 + EBS 구축 보다 저렴

- **객체와 버킷**
  - **객체(Object)**는 데이터와 메타데이터를 구성하는 저장 단위
  - S3에 저장되는 모든 데이터는 객체 라고 부른다.
  - 객체는 하나 당 1Byte 에서 최대 5TB (??????) 저장이 가능하며 객체 수는 제한이 없다.
  - **버킷(Bucket)**은 객체를 저장하고 관리하는 영역
  - 버킷 및 그 속에 저장 된 콘텐츠는 단일 AWS 리전에만 존재 하여야 한다.
  - 버킷의 이름은 전세계 S3 시스템을 기준으로 유일한 것이어야 한다
  - 버킷 명은 명명 규칙이 존재하며, S3에서 유일해야 한다 (전세계 중복 X)
  - 버킷에 특정 파일을 저장하면 URL이 생성
    - http://{USER}.s3.amazonaws.com/{파일명}
    - 버킷 주소는 https://{bucketname}.s3.amazonaws.com 형태로 이루어진다
  - 계정 당 최대 100개의 버킷을 생성 할 수 있으며, 버킷 단위 접근 제한 설정이 가능하다.
  - S3가 생성한 버킷의 리전 구성이 필요하고, 리전간 객체 공유는 불가능하다.
  - 버킷을 어느 리전에 지정하느냐에 따라 지연 시간, 비용 결정
  - 버킷은 생성시 default 로 private 한 상태이며, 소유권 이전이 불가능하다.

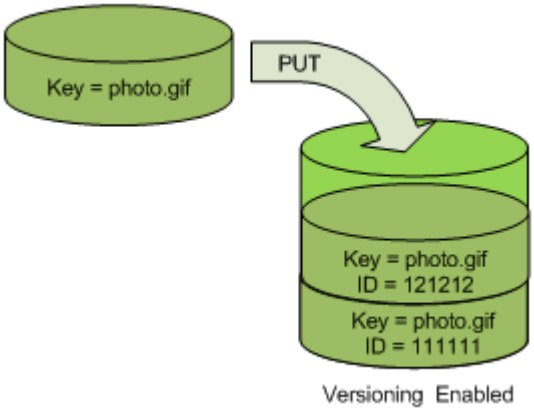
- MFA (이중 인증) 을 활용해 파일 삭제 방지 가능

- **객체(Object)의 구성**
  - Key, Value, Version ID, Metadata, CORS 등 다양한 구성요소가 존재

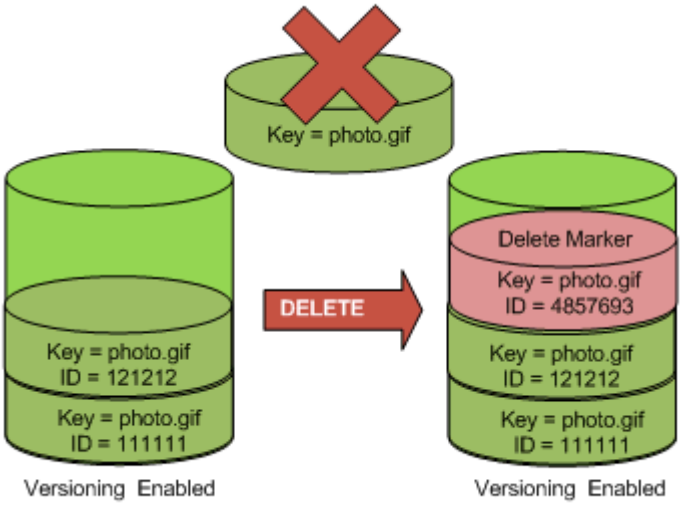
Key	파일 이름, 버킷 내 객체의 고유 식별자, 버킷내 모든 객체는 하나의 키를 갖는다, 버킷 & 키 & 버전 ID 의 조합은 각 객체를 고유하게 식별
Value	파일의 데이터, S3는 Key-Value 형태로 저장, Key 의 접두어 및 슬래시를 이용하여 폴더 개념으로 사용가능하다
Version ID	파일의 버전 아이디, 같은 파일이지만 다른 버전으로 올릴 수 있도록 돕는 인식표 개념
Metadata	파일의 정보를 담은 데이터, 최종수정일, 파일 타입, 소유자, 사이즈 등, 객체가 업로드 된 후에는 수정 불가능, 복사해서 수정하여야 한다. 객체의 metadata는 Response Header에 반환된다.
ACL	파일의 권한을 담은 데이터(접근, 수정)
Torrents	토렌트 공유를 위한 데이터
CORS (Cross Origin Resource Sharing)	한 버킷의 파일을 지역을 무시하고 다른 버킷에서 접근 가능하게 해주는 기능

- **접두사 및 구분문자**
  - 체계적으로 저장 객체를 관리하기 위해 버킷에 접두사 또는 구분문자를 추가해서 사용
  - 접두사는 스토리지 구조 레벨을 표기하기 위한 텍스트 문자열, 구분문자 ”/” 다음에 특정 단어를 추가해 파일들을 그룹화 한다.

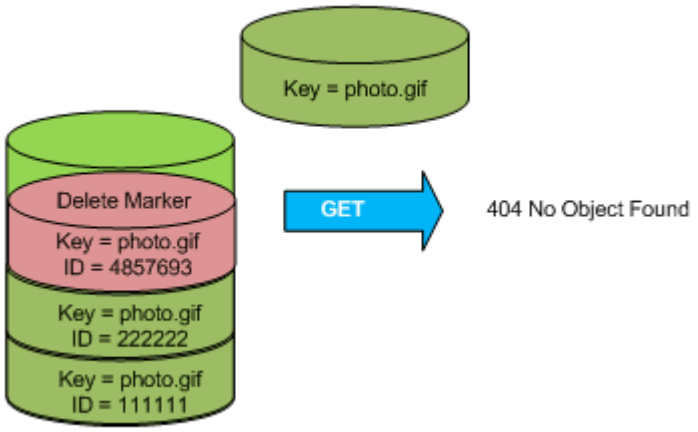
- **S3 버저닝 (Versioning)**
  - 버전관리 및 생애주기 관리 기법
  - 변경 내용 추적에 용이하지만 비용을 조심해야 한다.
  - AWS 매니저에서 버킷을 만들때 Default로 비활성화, 직접 활성화 해야한다.
  - 활성화 이후에는 비활성화 상태로 돌아갈 수 없으며, 버전관리 일시중지는 가능하다.

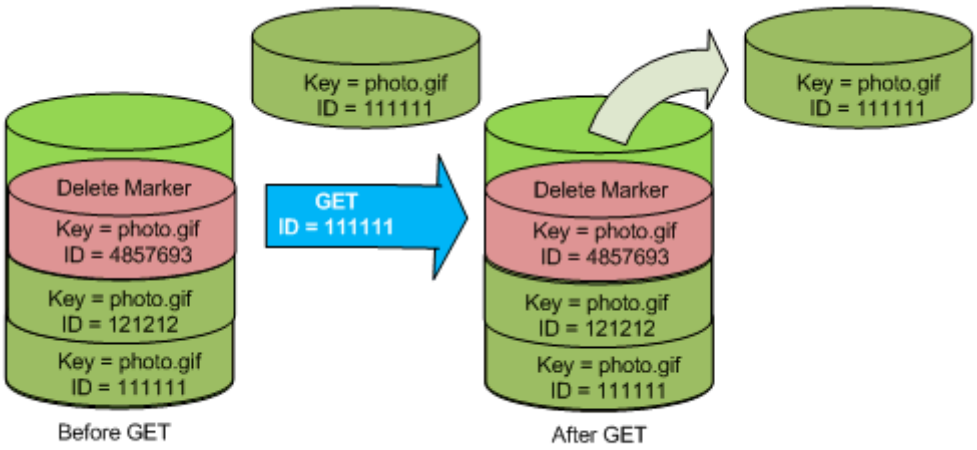


- PUT 할 때 파일을 덮어쓰지 않는다. (맨 위의 데이터를 최신 데이터로 인식)



- DELETE 할 때 삭제 마커(Delete Marker)가 삽입 되어 삭제 마커를 최상단에 두어 삭제 된 것 같은 효과를 준다. (객체의 영구적으로 삭제 하기 위해서는 Version ID 를 DELETE해야한다)





  - GET 시 삭제 마커가 가장 위에 있을 때 404 Not Found 반환, 특정 버전 ID를 지정하여 GET 할 수 있다.

- **S3 보안 및 접근제어 (Private)**
  - 대표적으로 4가지 방법, 해당 관리 기능을 조합하여 사용하여 권한 부여가 가능하다.

IAM	사용자를 생성하고 사용자의 버킷 권한 엑세스를 관리
ACL	권한 있는 사용자에 대해 간단한 개별 객체를 엑세스 가능하게 만듬, 다른 AWS 계정 (요청자) 에 대한 기본 권한 허용 범위에 대한 설정 (버킷 또는 객체)
Bucket Policy	단일 S3 버킷 내 모든 객체에 대한 권한을 세부적으로 구성
Pre-signed URL (쿼리 문자열 인증)	임시 자격 증명서, 임시 URL을 사용하여 다른 사용자에게 기간 제한 (임시권한) 엑세스를 부여한다.

- **ACL vs Bucket Policy**
  - ACL과 버킷정책은 버킷에 대한 엑세스를 제한 하거나 허용하는 권한 설정
  - 버킷 정책은 버킷에 대한 권한 설정
  - ACL은 버킷과 객체에 대한 권한 설정
  - 버킷 정책은 JSON 을 통해 세분화된 권한 설정이 가능하지만, ACL은 세분화된 엑세스 모드를 지원하지 않는다.

- **Access Log 전송**
  - 모든 파일들에 대한 접근 기록을 다른 S3 버킷 또는 다른 계정으로 전송 가능하다.

- **S3 요금 정책**
  - S3는 다른 AWS 서비스와 마찬가지로 사용한 만큼 요금을 지불하며, 요금이 저렴한 편이어서 로그를 저장해 두는 용도로 많이 사용한다. (DELETE, CANCEL 요청은 무료)
  - S3 Glacier 같은 장기 보관용 Storage 의 경우 저장 비용은 정말 저렴한 반면 데이터를 꺼낼 때 요금이 세다.
  - 동일한 리전의 EC2와는 데이터 전송 요금이 발생하지 않으므로 S3와 EC2 의 리전은 동일하게 설계한다.

- **데이터 일관성 (Data Consistency Model)**
  - 같은 시간에 조회하는 데이터는 항상 동일한 데이터를 보증하는 것을 데이터 일관성 이라고 한다.
  - S3 에서는 PUT 동작에 대해서는 데이터 일관성을 보장
  - Update와 Delete 동작에서는 일정 시간 후 결과가 반응하여 원자성 확보 불가능 상태가 된다.

- **S3 일관성 모델**

Read After Write (데이터 일관성 보	S3 에서 객체를 Create 한 후 즉시 읽기 (GET) 시도 시 → 변경 사항이 이루어지고 나서 객체 X를 반환한다. (일관성 보장)

장)	
Eventually Consistent (**최종 일관성, 데이터 일관성 보장 안함**)	S3 에서 객체를 Create 한 후 기존 객체를 Overwrite 한 뒤, 즉시 읽기 시도 시 → Old 데이터를 반환할 수도 New 데이터를 반환할 수도 있다. 마찬가지로 Delete 시 → 삭제가 정상적으로 되어 Error 발생 또는 기존 파일이 그대로 읽혀 올 수 있다.

- **최종 일관성 (Eventual Consistency)**
  - NoSQL이 쓰이게 되면서 동시성 보장이 어려워 졌다. NoSQL은 분산 노드를 이용하여 빠른 데이터 처리가 주 목적이기에 데이터 변경이 발생 하였을 때 시간이 지남에 따라 여러노드에 전파되며 당장은 아니지만 최종적으로 일관성이 유지된다 이를 **Eventual Consistency(최종 일관성)** 라 한다

- **Amazon S3 Glacier**
  - 저장된 데이터를 거의 인출하지 않는 저렴하게 사용할 수 잇는 장기 보관용 스토리지
  - 아카이브 저장 용량은 40TB로 제한 (S3 는 제한 없음)
  - 아카이브 생성 시 기본적으로 저장 데이터를 암호화 (S3 에서는 옵션)
  - 아카이브 이름은 기계생성 ID 형식을 갖는다 (S3는 버킷네임)
  - 데이터를 인출하는데 오랜 시간이 소요된다. (S3는 즉각적으로 객체 인출) → 장기 보관용 스토리지
  - 볼트(Vaults)에 저장 (S3 버킷과 같은 개념)
  - Standard / Deep Archive 클래스가 있고 Deep Archive 가 저렴하고 인출 시간이 길다.

- **Amazon EFS**
  - Elastic File System, 리눅스 인스턴스를 위한 확장성, 공유성이 높은 파일 스토리지

- **Amazon FSx**
  - Lustre용 또는 Windows File Server 용으로 나뉜다.

    - Lustre 용 : Linux 클러스터가 고도의 컴퓨팅 작업을 수행할 때 고성능 파일시스템에 접속할 수 있게 해주는 오픈소스 분산 파일시스템
    - Windows File Server 용 : 윈도우 서버를 위한 EFS 라고 할 수 있다. SMB NTFS, Microsoft Active Directory등과 통합해서 사용 가능하다.

- **AWS Storage Gateway**
    - 로컬 스토리지와 클라우드 스토리지를 연결하는 백업 및 아카이브 통합 게이트웨이
    - VMware, Hyper-V, Linux KVM, EC2 등 다수의 가상 연결 인터페이스를 제공

- **AWS Snowball**
    - 대량의 데이터를 클라우드로 전송시 인터넷 연결방식을 이용하면 지나치게 많은 시간이 소모되고 전송 업무에도 차질이 생길 수 있어 이를 해결하기 위해 물리적인 256비트 암호화 스토리지 디바이스 Snowball을 사용자 요청에 따라 배송
    - Snowball에 대용량 데이터를 저장 후 Amazon으로 재배송 하면 전달 된 데이터는 S3에 업로드 된다.
    - 클라우드로 전송하는 다른 방법으로 AWS Direct Connect 가 있으나 다소 고가이며, AWS Snowball이 조금 저렴하다.
    - Snowball을 운송하는 차량을 AWS Snowmobile 이라 함

- **AWS DataSync**
    - 온프라미스에 저장된 데이터를 AWS 계정으로 옮기는 작업에 특화된 도구
    - 대규모 데이터 이전에는 적합하지 않지만, S3, RDS(AWS Database Migration Service 이용) 등 다양한 저장소에 데이터를 전송할 수 있다.
    - 최대 10GBps 수준으로 데이터 전송이 가능하며, 암호화 및 데이터 검증 기능을 제공한다.