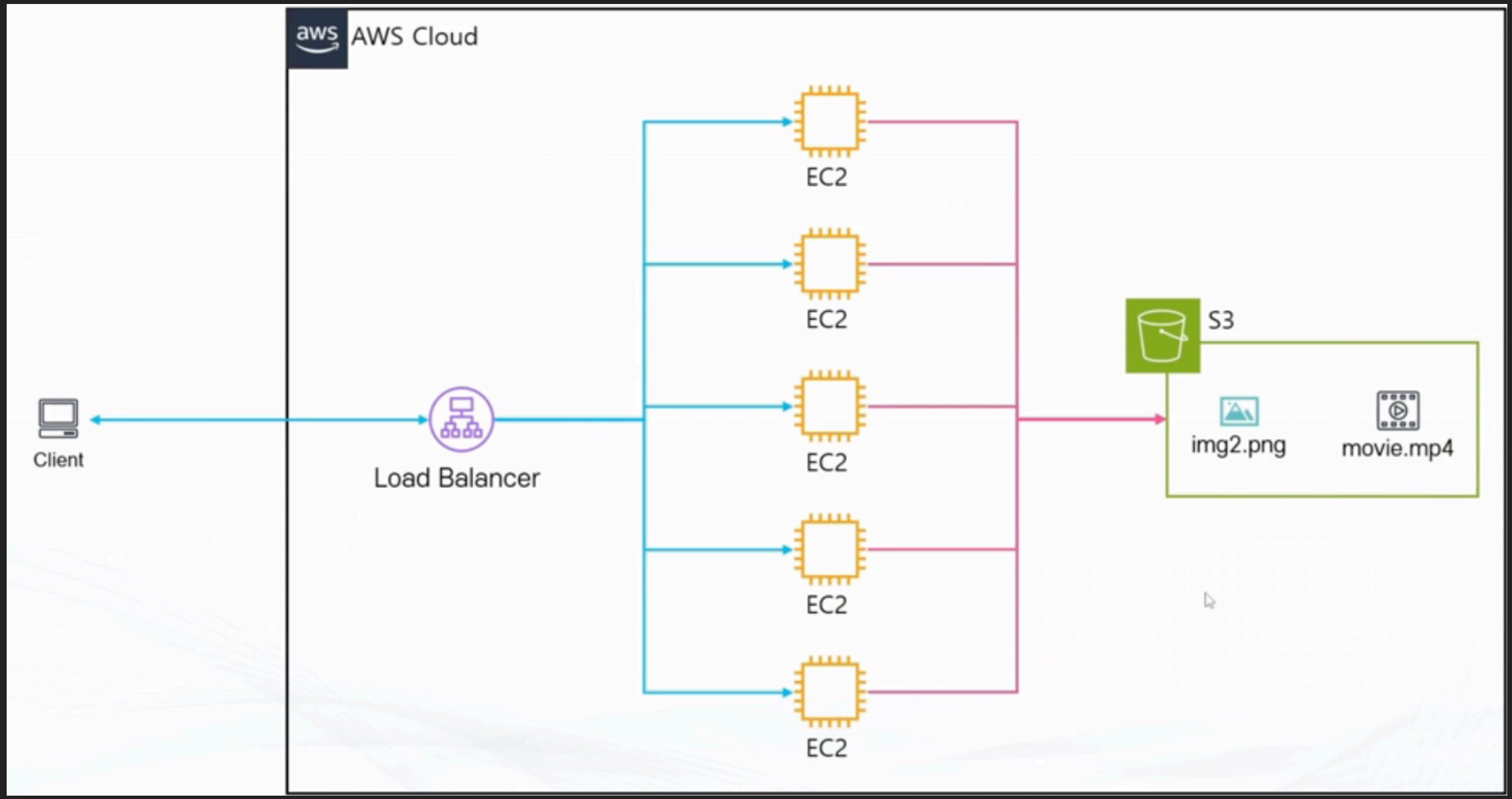
Amazon S3

> Amazon S3

- What: AWS에서 제공하는 Object 스토리지 서비스
- When:
  - 파일 저장하고 활용하고 싶을 때 (미디어, 로그, 소스코드, 파일, 백업)
  - Static Hosting 기능으로 서버 없이 웹페이지를 제공하고 싶을 때 (서버리스)
  - 기타 파일을 관리하고 싶을 때 (각각 저장하기엔 귀찮고, 교체시 매우 불편[특히 분산된 아키텍처 설계시])
- How:
  - 99.9999999999% 의 내구성(파일을 잃어버리지 않는 능력) /99.99% 의 가용성(원할 때 파일을 가져갈 수 있는 능력) 을 가진 분산 스토리지로 파일 저장
  - 다양한 기능
    - Presigned URL 제한된 사람에게만 전달, 버저닝/권환 관리

S3


aws AWS Cloud
EC2
EC2
EC2
EC2
EC2
S3
img2.png
movie.mp4
Client
Load Balancer

S3-1

Amazon S3 기초

Amazon S3

> Amazon S3

- 객체 스토리지 서비스: 파일 보관만 가능 <-> Block Storage Services(EBS, EFS 등)
  - 어플리케이션 설치 불가능
- 글로벌 서비스 단, 데이터는 리전에 저장
- 무제한 용량
  - 하나의 객체는 0byte 에서 5TB의 용량

버킷

> 버킷이란?

- S3의 저장공간을 구분하는 단위
- 디렉터리/폴더와 같은 개념
- 버킷이름은 전 세계에서 고유 값: 리전에 관계 없이 중복된 이름이 존재할 수 없음

S3 객체의 구성

> S3 객체의 구성

- Owner : 소유자
- Key : 파일의 이름
- Value : 파일의 데이터
- Version ID : 파일의 버전 아이디
- Metadata : 파일의 정보를 담은 데이터
- ACL : 파일의 권한을 담은 데이터 (요즘 안 쓰는 추세)
- Torrents : 토렌트 공유를 위한 데이터

S3의 내구성

> S3의 내구성

- 최소 3개의 가용영역(AZ)에 데이터를 분산 저장(Standard의 경우)
- 99.999999% 내구성
  - 0.000000001 % 확률로 파일을 잃어버릴 수 있음
  - 로또보다 어려움 (레전드 사건 발생 AWS는 신이다)
- 99.9 % SLA 가용성 (스토리지 클래스에 따라 다름)

보안 설정

> S3 보안 설정

- S3 모든 버킷은 새로 생성시 기본적으로 Private(비공개)
  - 따로 설정을 통해 불특정 다수에게 공개 가능 (i.e 웹 호스팅)
- 보안 설정은 객체 단위와 버킷 단위로 구성
  - Bucket Policy : 버킷 단위
  - ACL : 객체 단위
- MFA를 활용해 객체 삭제 방지 가능
- Versioning을 통해 파일 관리 가능
- 액세스 로그 생성 및 전송 가능
  - 다른 버킷 혹은 다른 계정으로 전송 가능

Demo - S3 버킷 생성, 업로드, EC2 유저데이터 활용

> Demo - S3 버킷 생성, 업로드, EC2 유저데이터 활용

- S3 버킷 생성
- 파일 업로드
- S3 접근 권한을 가진 EC2 IAM 역할 생성
- EC2 시작 구성 생성
    - 유저데이터에서 S3 파일을 가져와서 적용하도록 설정

S3 스토리지 | 클래스

> S3 스토리지 클래스

- S3는 다양한 스토리지 클래스를 제공
  - 클래스별로 저장의 목적, 예산에 따라 다른 저장 방법을 적용
  - 총 9가지 클래스

> S3 스탠다드

- 99.99% 가용성
- 99.999999999% 내구성
- 최소 3개 이상의 가용영역에 분산 보관
- 최소 보관 기간 없음, 최소 보관 용량 없음.
- 요청 비용 $0.0045/1000 requests (ap-northeast-2 기준)
- 저장 비용 $0.024/1

S3 스탠다드 IA (Infrequently Accessed)

- 자주 사용되지 않는 데이터를 저렴한 가격에 보관
- 최소 3개 이상의 가용영역에 분산 보관
- 최소 저장 요량: 128kb
- 최소 저장 기간 : 30일
- 데이터 요청 비용 발생: 데이터를 불러올 때 마다 비용 지불 (per GB)
    - 요청 비용 $0.01/1000 request vs $0.0045/1000 requets
- 사용 사례: 자주 사용하지 않는 파일 중 중요한 파일
- 저장 비용 : standard /2

S3 One Zone-IA

- 자주 사용되지 않고, 중요하지 않은 데이터를 저렴한 가격에 보관
- 단 한개의 가용 영역에만 보관
- 최소 저장 용량 : 128kb
- 최소 저장 기간: 30일
- 데이터 요청 비용 발생: 데이터를 불러올때마다 비용을 더 많이 지불
    - 요청 비용 $0.01 / 1000
- 사용 사례: 자주 사용하지 않으며 쉽게 복구 할 수 있는 파일
  예 : 오래된 썸네일

> S3 Express One Zone

- 매우 빠른 퍼포먼스를 위해서 하나의 가용영역에 위치한 특별한 저장소에 저장
  - millisecond 단위의 응답속도(약10배 빠름)
  - standar와 비교해 50 % 저렴한 요청 비용
- Amazon S3 Directory Bucket에 저장
- 컴퓨팅 리소스와 스토리지 리소르를 같은 공간에 위치시켜 더 빠른 액세스 가능
- 몇몇 리전만 사용 가능 (ap-northeast-2 사용 불가능)
- 저장 비용: $0.016/GB

S3 Glacier Instant Retrieval

- 아카이브용 저장소
- 최소 저장 용량 : 128kb
- 최소 저장 기간 : 90일
- 바로 액세스 가능
- 사용 사례: 의료 이미지 혹은 뉴스 아카이브 등
- $0.005/GB(ap-northeast-2기준)

> S3 Glacier Flexible Retrieval

- 아카이브용 저장소
- 최소 저장 용량 : 40kb
- 최소 저장 기간 : 90일
- 분 ~ 시간 단위 이후 액세스 가능
- 사용 사례 : 장애 복구용 데이터, 백업 데이터 등
- $0.0045

> S3 Glacier Deep Archieve

- 아카이브용 저장소
- 최소 저장 용량 : 40 kb
- 최소 저장 기간 : 90일
- 데이터를 가져오는데 12~48시간 소요
- 사용 사례: 오래된 로그 저장, 사용할 일이 거의 없지만 법적으로 보관해야 하는 서류 등
- 0.002/GB

> S3 Intelligent-Tiering

- 머신 러닝을 사용해 자동으로 클래스 변경
- 퍼포먼스 손해/오버헤드 없이 요금 최적화

> S3 on Ouptosts

- 온프레미스 환경에 S3 제공
- 내구성을 확보한 상태로 파일을 저장하도록 설계
- IAM, S3 SDK 등 사용 가능

정리

> 스토리지 클래스

- 목적과 비용에 따라 9가지 클래스

S3의 권환 관리 방법

> S3의 권한 관리 방법

- IAM 정책 : 자격증명(IAM 사용자, 그룹, 역할) 등에 부여하는 정책으로 S3에 대한 권한 부여/거부
- 버킷 정책 : 버킷 자체에 특정 주체가 행사할 수 있는 권한 부여/거부
    - 주체: IAM 사용자. 역할 등
- ACL : 잘 사용되지 않는 추세

S3의 계층 구조

> S3의 계층 구조

- AWS 콘솔에서는 S3의 디렉토리(폴더)를 생성하고 확인 가능
- S3 내부적으로 계층구조가 존재하지 않음.
  - 키 이름에 포함된 "/" 로 계층 구조를 표현
  - 예:
    - s3://mybucket/world/southkorea/seoul/guro/map.json
    - 버킷명: mybucket
    - 키 : world/southkorea/seouol/guro/map.json (단일 스트링)

S3 버킷 정책

> S3 버킷 정책

- 버킷 단위로 부여되는 리소스 기반 정책
- 해당 버킷의 데이터에 "언제 어디서 누가 어떻게 무엇을" 할 수 있는 정의 가능
  - 리소스의 계층 구조에 따라 권한 조절 가능
    - 예: resource : "arn:aws:s3:::my-bucket/images/*" -> my-bucket의 images/로 시작하는 모든 객체에 대해서 ...
  - 다른 계정에 엔티티에 대해 권한 설정 가능
  - 익명 상용자(Anonymous)에 대한 권한 설정 가능
- 기본적으로 모든 버킷은 Private => 접근 불가능

S3 버킷 관리 방법의 선택

> IAM 정책

- 같은 계정의 IAM 엔티티의 S3 권한 관리할 때
- S3이외에 다른 AWS 서비스와 같이 권한 관리할 때

> 버킷 정책

- 익명 사용자 혹은 다른 계정의 엔티티의 S3 이용 권한을 관리 할 때
- S3 만의 권한을 관리할 때

S3 Access Control List(ACL)

> S3 Access Control List(ACL)

- 버킷 혹은 객체 단위로 읽기, 쓰기 의 권한을 부여
- S3에서 설정을 통해 ACL을 활성화 시킨 후에 저굥ㅇ ㅏㄱ능
- 파일 업로드시 설정 가능
- 간단하고 단순한 권한 관리만 가능
- 점점 사용하지 않는 추세
    - 대부분의 경우 버킷 정책/IAM 정책으로 대체 가능

Demo - S3 권한 부여

> Demo - S3 권한 부여

- IAM 정책/버킷 정책으로 S3 버킷에 대한 권한 부여
  - IAM 사용자에 S3 접근을 허용하는 권한 부여(IAM 정책)
  - IAM 사용자에 대한 접근을 허가하는 버킷 정책을 만들어 S3에 붙여 접근 허용 (버킷 정책)

Demo - 나만의 S3 홈 디렉토리 만들기

> Demo - 나만의 S3 홈 디렉토리 만들기

- IAM 사용자를 생성해서 해당 사용자만 접근 가능한 S3 버킷 디렉토리 만들기