네트워크 및 콘텐츠 전송 서비스(2)

다른 AWS 서비스와 결합된 구성 예

1. VPC 구성 예
    - AWS 서비스는 실행 위치에 따라 3가지 유형으로 나뉨
        - **글로벌 서비스**
            - 특정 리전에 의존하지 않고 실행되는 서비스
            - CloudFront, IAM 등
        - **리전 서비스**
            - 리전 내, VPC 외부에서 실행되는 서비스
            - S3, DynamoDB 등
        - **AZ 서비스**
            - VPC 내에서 실행되는 서비스
            - EC2, RDS 등
    - **AZ 서비스는 VPC 안에서, 그 외 서비스는 VPC 밖에서 실행됨**
    - 구성 1: Web + DB + Amazon CloudFront
        - 온프레미스 환경의 웹서버, DB 서버 환경을 AWS로 마이그레이션할 때 자주 볼 수 있는 구성
    - 구성 2: VPC 엔드포인트를 사용하는 S3 연결
        - 구성 1에 VPC 엔드포인트와 S3 버킷을 추가한 구성
        - RDS에서 취득한 데이터를 S3에 저장하거나 S3에서 얻은 데이터를 다른 데이터베이스로 가져오는 프로세스를 가정
    - 구성 3: 온프레미스 환경에서 프라이빗 연결

    - Direct Connect와 Site-to-Site VPN을 모두 사용해 온프레미스 환경과 프라이빗 연결을 하는 구성
    - 온프레미스 환경 전용 프라이빗 네트워크
    - VPC와 온프레미스 환경만 통신할 수 있고 인터넷과 소통할 수 없는 구성

ELB로 부하를 분산시켜 가용성 향상

1. ELB란
    - **Elastic Load Balancing(이후 ELB): AWS에서 제공하는 로드 밸런서 서비스**
    - 주요 기능
        - 응용 프로그램으로 트래픽을 로드 밸런싱
        - 트래픽을 보내는 서버가 멈추지 않고 실행 중인지 정기적으로 확인해 가용성 확인 가능
    - 부하 분산
        - 트래픽을 여러 대상으로 전달하도록 지정 시 사용자의 접속을 자동으로 분산 가능
        - 대량 접속이 발생하더라도 부하를 나눌 수 있음
        - 각 대상을 다른 AZ에 배치할 수 있으므로 지리적으로 분산할 수 있어 재해가 발생했을 때의 가용성 향상 가능
        - ELB 자체는 부하 상황에 따라 자동으로 스케일 → **사용자는 ELB 성능 저하를 신경 쓸 필요가 없음**
    - 대상 모니터링
        - ELB는 항상 대상(트래픽 도착지)에 대한 연결과 상태를 감시하고 확인

          → 요청 추적이나 CloudWatch 지표 취득 가능
        - **감시를 통해 비정상적 동작 감지 시 대상을 자동으로 분리, 안정적인 작동 유지**
    - 보안 기능
        - 보안 그룹을 비롯한 AWS의 기본적인 보안 서비스 적용 가능
        - SSL/TLS 서버 인증서 설정해 암호화 통신 수행 가능

- NLB(Network Load Balancer)는 보안 그룹 설정 불가

2. ELB 유형
   - ELB는 용도에 따른 로드 밸런서 제공
   - 기본적으로 요건에 따라 ALB 또는 NLB 중 하나 선택
     - **일반적으로 웹 사이트, 웹 시스템의 부하 분산 → ALB**
     - **ALB로는 구현할 수 없는 미세한 제어나 HTTP/HTTPS 이외의 프로토콜 이용 → NLB**

ALB Application Load Balancer	- HTTP 트래픽과 HTTPS 트래픽의 부하 분산 가능 - 레이어 7(응용 프로그램 계층)로 동작 → 다양한 응용 프로그램에 대응 가능
NLB Network Load Balancer	- 레이어 4(전송 계층)에서 동작 → HTTP/HTTPS 외에 TCP, UDP, TLS 트래픽의 부하 분산도 가능 - 수백만 건 이상 요청이 발생하는 대규모 트래픽에서도 속도 빠름
CLB Classic Load Balancer	- ALB, NLB 서비스 이전부터 제공된 구형 로드 밸런서 - 레이어 4(전송 계층) 및 레이어 7(응용 프로그램)에서 동작 - 예전 아키텍처를 이용해야 하는 등 특별한 경우를 제외하고는 기본적으로 ALB나 NLB의 이용 권장
GWLB Gateway Load Balancer	- AWS에서 제공하는 타사 보안 제품의 배포 및 관리 가능 - 레이어 3(네트워크 계층)에서 동작 - 기존 NLB 및 VPC 피어링, Transit Gateway에서 구현하던 아키텍처를 더욱 단순하게 구현 가능

3, ELB 요금 예
   - 1시간당 로드 밸런서 사용료(고정)과 로드 밸런서 커패서티 유닛(Load Balancer Capacity Unit - LCU) 이용료(변동)을 합산해 계산
   - **LCU**
     - 초당 새 연결 수, 활성 연결 수, 처리된 바이트, 규칙 평가 측정
       → 가장 사용량이 많은 것에 대해서만 요금 부과
     - 대규모 시스템을 운영하거나 처리하는 데이터가 많다면 LCU 비용도 고려해야 함

간편하게 사용할 수 있는 DNS 서비스

1. Route 53란
    - Amazon Route 53(이후 Route 53)
    - AWS가 제공하는 DNS 서비스
    - **완전 관리형으로 제공**
      → **DNS 서버와는 달리 유지 관리 및 작업 필요X**
      → **AWS 관리 콘솔에서 모든 설정과 관리 가능**
    - 글로벌 서비스이므로 모든 리전에서 공통으로 사용 가능
    - 관리는 호스팅 영역 별로 수행
        - **호스트 존:** 도메인과 하위 도메인의 트래픽 라우팅 방법에 대한 정보 보관 상자 같은 것
        - 도메인 이름 등록 시 같은 이름의 호스팅 영역이 자동으로 생성
    - 주요 특징
        - 높은 가용성
            - SLA(서비스 품질 보증) 100%로 정의, 다른 AWS 서비스에 비해 높은 가용성 제공

              → Route 53 서비스를 제공하는 기반 시스템이 전 세계에 걸쳐 이중화 되어있기 때문
        - 높은 비용 성능
            - 주요 제공 서비스인 도메인 등록: 처음 25개의 호스팅 영역 1개 당 0.5USD/월 정도로 이용 가능
            - 트래픽량에 의한 과금은 발생하지만 이용료에서 차지하는 비율은 낮음

2. Route 53 기능
    - 도메인 등록 기능
    - 도메인 트래픽 라우팅
    - 자원에 대한 상태 확인

3. 도메인 등록 기능
    - 임의의 호스팅 영역을 생성해 도메인 등록
    - 임의의 도메인 이름을 Route 53에서 DNS 레코드로 등록 가능 → 일부 제약 존재
    - **DNS 레코드**
        - DNS가 관리하는 도메인과 어떤 IP 주소, 정보가 연결돼 있는지를 기록한 데이터
        - 이 DNS 레코드를 기반으로 질의한 곳에 도메인에 해당하는 IP 주소 반환
    - 신규 도메인 등록은 유료, TLD(Top Level Domain-최상위 도메인, .com/.kr)의 종류에 따라 도메인 이용 요금이 달라짐

4. 도메인으로 트래픽 라우팅
    - 생성한 DNS 레코드별로 라우팅 정책 설정 가능
    - 라우팅: 도메인 이름에 대한 IP주소를 어떻게 반환하는지 의미
    - 라우팅 정책 설정을 통해 이름 확인을 할 때의 라우팅 동작을 세밀하게 제어 가능
    - 단순 라우팅
        - DNS와 같은 라우팅 수행
        - 하나의 도메인에 대해 하나의 IP 주소만 연결
    - 가중치 기반 라우팅
        - 라우팅 대상을 여러 개 등록하고 각각에 트래픽을 할당하는 정도를 0에서 255 사이의 값(가중치)로 지정
        - 가중치에 따라 어느 IP 주소를 반환할 지 결정
    - 지리적 위치 라우팅
        - 조회한 곳의 위치 정보에 따라 어떤 IP 주소를 반환할 지 결정
    - 지연 시간 라우팅
        - **레이턴시(데이터 처리 지연 시간)**가 최소인 자원의 IP 주소를 우선적으로 반환
    - 장애 조치 라우팅

    - 프라이머리에 장애 밥ㄹ생 시 보조로 라우팅
    - 장애 발생 여부는 상태 확인 기능을 이용해 판단
- 다중 값 응답 라우팅
    - 다중 값 응답을 설정하면 Route 53이 질의에 대해 항상 여러 IP 주소를 무작위로 반환하도록 할 수 있음
    - 사용자가 여러 서버에 무작위로 할당돼 부하 분산 역할
    - 상태 확인이 실패한 서버에는 할당되지 않으므로 ELB처럼 작동 가능

5. 자원 상태 확인
    - 대상이 정상적으로 실행 중인지 확인 가능
    - 정상 판단 기준
        - 보통 라우팅을 하는 곳인 웹 서버나 메일 서버에서 반환되는 응답 결과 확인
        - 더 명확한 판단을 위해 다른 서비스의 상태 확인 결과도 함께 확인하거나 CloudWatch 정보를 확인하기도 함
    - 상태 확인 결과를 바탕으로 자동 라우팅 변경 or 알람 등의 동작 추가로 서비스가 안정적으로 실행될 수 있게 함

상태 확인 대상	설명
엔드포인트	- 엔드포인트에 IP 주소 또는 도메인 이름 지정, 반환되는 응답으로 작동 확인 - 대상 엔드포인트, 프로토콜, 포트, 대상 경로 지정 - 고급 설정 항목으로 요청 간격 및 상태를 확인하는 곳의 리전 선택 가능
다른 상태 확인의 상태 (산출된 상태 확인)	- 지정한 다른 상태 확인 결과에서 정상 여부 확인 - 여러 상태 확인 결과 대상 가능, 정상 수에 대한 기준 설정 가능
CloudWatch 알람 상태	- 생성된 CloudWatch 알람 상태 확인, 정상 여부 판단

CloudFront로 빠르고 안정적인 서비스 제공

1. CloudFront란
    - Amazon CloudFront: AWS가 제공하는 콘텐츠 전달 네트워크(CDN)

- **CDN: 대용량 디지털 콘텐츠를 인터넷에서 효율적으로 사용자에게 전달하기 위한 네트워크**
  - 원본 서버: 데이터 본체를 저장
  - 캐시 서버: 데이터의 복사본(캐시)를 저장
  - **사용자의 위치 파악 → 자동으로 가장 가까운 곳에 있는 캐시 서버로 연결 → 데이터 취득**
  - 지리적 위치 라우팅과 같은 개념 사용
- 캐시 서버를 전 세계 엣지 로케이션에 배치, AWS가 가진 네트워크를 통해 AWS 리전에 기능 제공
- 엣지 로케이션: 전 세계에 CDN 서비스 제공 가능

2. CloudFront의 장점
   - 대용량 콘텐츠의 빠른 배포
     - 전 세계에 구축된 CDN → 대용량 콘텐츠를 전 세계 사용자에게 효율적으로 전달 가능
   - 보안 향상
     - 자동으로 통신의 SSL/TLS 암호화 수행
     - 기본적으로 자동으로 생성된 도메인 이름 할당, 해당 도메인 이름을 가진 인증서 설정
     - AWS Shield 라는 무료 DDoS 보호 서비스도 자동으로 적용 → DDoS 공격 대처 가능
     - CloudFront 적용만으로도 보안 개선 가능
   - 가용성 향상
     - 전 세계에 엣지 로케이션, 대상 데이터의 캐시 저장
     - 원본 서버에 대한 부하 분산으로 가용성 향상으로 이어짐
     - 원본 서버에서 장애 발생 시 동작도 설정 가능해 유연한 서비스 제공 가능

3. CloudFront 설정
    - 배포(Distribution)
        - 원본 서버에 배치된 파일에 대한 정보를 배포라는 단위로 취급
        - 하나의 배포에 하나의 도메인 할당
        - 사용자가 전용 도메인에 접속 시 엣지 로케이션을 통해 통신하도록 함
    - 원본 설정
        - 콘텐츠의 원래 데이터가 저장되는 원본이 되는 자원에 대해 설정
        - 도메인 단위로 설정 가능
        - AWS 자원은 S3나 ELB 등을 대상으로 할 수 있음

4. 기타 설정

설정 항목	설명
동작	- CloudFront에서 사용할 수 있는 프로토콜 및 HTTP 방법 설정, 캐시 설정을 수행 - ‘*.mp4’와 같이 웹 서비스에서 사용되는 경로 패턴 단위로 제어 - 캐시 정책에서 상세한 캐시 설정을 할 수 있음
오류 페이지	- 원본에서 장애가 발생했을 때의 동작 설정 가능 - HTTP 오류 코드별 응답 정의 - ‘동작’ 설정과 조합해 에러가 발생했을 때의 동작을 설정
지리적 제한	- 특정 위치로부터의 접속을 허가 또는 차단하는 설정
무효화	- CloudFront에서 캐시를 수동으로 삭제할 때 사용

5. CloudFront 이용료
    - **종량 과금제**
    - 실제 사용한 데이터 전송량과 요청 수에 따라 요금 결정

다양한 네트워크 기능을 제공하는 서비스 7가지

1. 전용선 및 VPN
    - 온프레미스 환경과 AWS에서 생성한 VPC 연결 시 전용선이나 VPN 사용 가능
    - 전용선
        - 거점 간 물리적으로 연결된 전용의 통신 회선
        - 안전하고 속도가 빠르지만 비용이 많이 듦
    - VPN
        - 인터넷을 가상으로 전용선처럼 취급하는 기술
        - 통신을 하는 기기 간 암호화 수행, 경로 제어
          → 각 거점을 전용선으로 연결하고 있는 것처럼 통신 가능
        - 사이트 간 VPN과 원격 VPN 존재
        - 통신량 증가에 따른 회선 부족의 영향 있을 수 있음, but 비교적 저렴

2. AWS Direct Connect
    - AWS와 온프레미스 환경 사이에 전용선을 만드는 서비스로 DX라고도 함
    - 사용자가 직접 통신 사업자와 계약해 연결 거점까지의 전용선을 설치할 수도 있고, AWS의 파트너사를 통한 이용도 가능

3. AWS VPN
    - AWS Site-to-Site VPN
        - 두 사이트를 연결하는 VPN을 구성하기 위한 서비스
        - IPsec VPN이라는 기술 사용
    - AWS Client VPN
        - 원격 VPN을 이용해 AWS에 연결하는 서비스
        - SSL-VPN이라는 기술 사용
    - 둘 다 온프레미스 환경에서 AWS와 가상 전용선을 구축해 통신하는 서비스

- Site-to-Site VPN: 거점 별 AWS와 VPN을 연결하고자 하는 경우
  Client VPN: 특정 단말만 일시적으로 VPN을 연결하고자 하는 경우
- 통신 속도의 저하 등이 발생할 가능성 있음, but Direct Connect에 비해 저렴
- Site-to-Site VPN은 Direct Connect와 함께 사용할 수 있음

4. AWS Transit Gateway
   - VPC 연결을 통합하는 서비스
   - VPC 간 통신을 더욱 깔끔하게 정리 가능
   - 개별 VPC와 접속하는 구성에 비해 요금이 높지만 전체 구성을 파악하기 쉽고 운영이 쉬워짐

5. AWS PrivateLink
   - VPC 엔드포인트를 생성하는 서비스
   - 인터넷을 통하지 않고 내부적으로 다른 VPC와 통신 가능
   - 접속 제어와 같은 설정도 가능

6. Amazon API Gateway
   - 웹 API 생성 서비스
   - 데이터 처리 프로그램만 구현해도 API 서비스를 제공할 수 있음
   - 처리한 요청 수와 데이터 전송량에 대해서만 이용료 발생
   - 인증 기능, 에러 발생률/처리 시간 등 감시 가능

7. AWS Global Accelerator
   - AWS 네트워크망을 이용해 클라이언트가 AWS에 더 빠르게 접근할 수 있게 하는 서비스
   - 최대 60% 가량 네트워크 성능 향상

- 시스템에 접근하기 위한 고정 IP 주소가 발급돼 글로벌 트래픽 관리 간소화 가능

8. AWS Ground Station
    - 인공위성 이용 예약과 AWS가 소유한 기지국과의 통신
    - AWS 사업 범위의 넓이와 가능성을 보여주는 서비스