AWS 구분

- 컴퓨팅
- 스토리지
- 네트워킹
- 데이터베이스
- 보안
- 애널리틱스
- 애플리케이션 서비스
- 배포 및 관리

컴퓨팅 서비스

EC2(Elastic Compute Cloud)

> 가상 서버를 제공하는 서비스

- 가상화 기술 : 하드웨어를 가상화하여 여러 서버를 하나의 물리서버에서 실행

EC2 요금제

- On Demand : 시간 단위로 요금을 지불하는 방식
- Reserved : 1년 또는 3년 단위로 요금을 지불하는 방식
- Spot : AWS에서 이용하지 않는 자원을 활용해 인스턴스를 생성하는 방식
- Dedicated Host : 전용 호스트를 사용하는 방식
- Dedicated Instance : 전용 인스턴스를 사용하는 방식
- Savings Plan : 1년 또는 3년 단위로 요금을 지불하는 방식.인스턴스 유형과 운영 체제를 선택할 수 있다.
  - Compute Savings Plan : 인스턴스 패밀리, 크기, AZ, 리전, OS 또는 테넌시와 관계없이 인스턴스 사용량에 적용
  - EC2 Instance Savings Plan : 인스턴스 패밀리에 적용되지는 않음. 인스턴스 크기, AZ, 리전, OS 또는 테넌시와 관계없이 인스턴스 사용량에 적용
- **Spot Fleets : set of Spot Instances + (optional) On-Demand Instances**
  - Strategy
    - lowestPrice : the Spot Instances with the lowest price are launched first

        - diversified : the Spot Instances are launched across all the Spot pools (Great for availability , long workloads)
        - capacityOptimized : pools with highest capacity available , then select the pool with the lowest price (Great for short workloads that are urgent or for big data jobs)
- Capacity Reservations : Instance를 예약하는 것이 아니라 Capacity를 예약하는 방식

EC2 인스턴스 유형

- General Purpose :
- Compute Optimized :
    - Batch Processing workloads
    - Media transcoding
    - Scientific modeling & Machine Learning
- Memory Optimized :
    - Large Data Sets in Memory
    - in memory db Optimized for BI
    - distributed web scale cache store
    - Application performing real-time processing of big unstructured data
- Storage Optimized :
    - 대량의 데이터셋을 로컬 스토리지에 저장하고 처리
    - High Frequancy online transaction processing(OLTP) systems
    - Relational & NoSQL databases

EC2를 외부에 노출하기

- EC2를 퍼블릭 서브넷에 배치
- 퍼블릭 IP 주소를 EC2에 부여
- 보안 그룹에서 외부로부터의 접근을 허가

EC2 보안 그룹

> EC2 인스턴스에 대한 인바운드/아웃바운드 트래픽을 제어하는 가상 방화벽

- 인바운드 : EC2로 들어오는 트래픽
- 아웃바운드 : EC2에서 나가는 트래픽
- 기본적으로 보안그룹에 지정하는 규칙은 허용만 가능하다.

EC2 User Data

- bootstrapping : process of starting up a machine and loading the initial set of instructions
- the script is **only run once** at the instance first start
- EC2 User Data is used to automate boot tasks such as
  - installing updates
  - installing software
  - download common files from the internet
  - anything you can think of
- 기본적으로 instance가 처음 시작될 때, 한 번만 실행된다. ec2 user data script에 이것저것 추가할 수록 부팅 시간이 보다 길어진다.

EC2 Placament Group

- Cluster : Same AZ
  - 클러스터 배치 그룹을 사용하면 인스턴스를 AZ내에서 서로 가깝게 배치할 수 있으므로 높은 네트워크 처리량 가능.
- Spread : Different AZ
  - 스프레드 배치 그룹을 사용하면 인스턴스를 서로 다른 AZ에 배치할 수 있으므로 재해 복구 기능을 제공
  - AZ간 퍼블릭 IP 트래픽 비용이 발생할 수 있음
- Partition : Different Partitions within an AZ
  - Can have up to 7 partitions per AZ
  - 파티션 그룹은 AZ에 걸쳐 있기 때문에 대역폭이 줄어든다.

EC2 AMI(Amazon Machine Image)

> EC2 인스턴스를 생성할 때 사용하는 템플릿

- OS, 소프트웨어, 설정 등이 포함된다.
- 같은 AZ(Availability Zone)에서만 생성할 수 있다.

Elastic Network Interface(ENI)

> VPC의 가상 네트워크 카드를 나타내는 논리적인 네트워킹 구성요소

- logical component in a VPC that represents a **virtual network card**
- [VPC(Virtual Private Network) 개념](https://medium.com/harrythegreat/aws-가장쉽게-vpc-개념잡기-71eef95a7098)

- Failover 관리 : instance에서 instance로 ENI를 붙여서 failover를 관리할 수 있다.
- ENI 컨셉 관련 참고
  - https://aws.amazon.com/ko/blogs/aws/new-elastic-network-interfaces-in-the-virtual-private-cloud/

EC2에서 미들웨어 기능 사용

- 비즈니스, 데이터, 어플리케이션 계층을 EC2인스턴스에서 모두 호스팅해야할 수 있다.

EC2 Hibernate

> EC2 인스턴스를 중지하고 다시 시작할 때, 이전 상태를 그대로 유지하는 기능

EC2 Auto Scaling

> 부하에 따라 서버를 자동으로 추가/삭제

- Scale Out : 서버를 추가
- Scale In : 서버를 삭제
- 규칙 ex):
  - CPU 사용률이 70%를 넘으면 서버를 추가
  - CPU 사용률이 30%를 넘지 않으면 서버를 삭제
- 대상추적조정(target tracking policy) : 특정 지표를 기준으로 서버를 추가/삭제
  - A target tracking policy allows the Auto Scaling group to automatically adjust the number of EC2 instances in the group based on a target value for a metric. In this case, the target value for the CPU utilization metric could be set to 40% to maintain the desired performance of the application. The Auto Scaling group would then automatically scale the number of instances up or down as needed to maintain the target value for the metric.
- 스케줄 스케일 : 주말 등 특정 시간대에 서버를 추가/삭제

다중 AZ를 사용해야 하는 상황

- 기본적으로 리전 간 Auto Scalinging은 불가능하다.
- 지리적 이중화의 안전성과 안정성을 활용하려면 Auto Scaling 그룹을 리전 내의 여러 가용 영역에 걸쳐 확장하고 로드 밸런서를 연결하여 해당 가용 영역에 들어오는 트래픽을 분산시켜야 한다.

EC2 Lambda

> 서버를 관리하지 않고 코드를 실행할 수 있는 컴퓨팅 서비스

EC2 vs Lambda

- Lambda:
  - 보안
  - 비용
  - 가용성
  - 확장성
- EC2:
  - 온프레미스 os 설정 이전 가능
  - 인스턴스 유형, os ,네트워크 설정 유연성
  - 대량의 트래픽이나 접속을 상시처리할 경우 EC2 가 저렴
  - 서버에 프로그램을 배포하는 방식으로 개발

Lambda+API Gateway

- API Gateway를 통해 HTTP 요청을 받으면 Lambda를 실행한다.
- 서버를 구축하지 않고도 웹 서비스를 구축할 수 있다.

Lambda + S3

- S3에 파일이 업로드되면 저장된 파일을 Lambda를 통해 자동처리

Lambda + EventBridge

- EventBridge를 통해 특정 이벤트가 발생하면 Lambda를 실행한다.
- Cron 처럼 주기적으로 실행할 수 있다.

Lambda + CloudWatch

- CloudWatch를 통해 Lambda의 실행상태를 모니터링할 수 있다.
- 모니터링 정보
  - 실행시간
  - 실행횟수
  - 에러횟수, 성공률

Lambda@Edge

- 들어오는 요청의 User-Agent Header를 분석해 모바일 기기인 경우 모바일용
  페이지를 반환하는 등의 처리를 할 수 있다.-> 정보를 기반으로 사용자 지정 응답을 하거나 적절한 버전의 콘텐츠를 사용자에게 보낼수 있음

AWS Step Functions

> AWS에서 제공하는 서버리스 오케스트레이션 서비스

- It allows you to coordinate and sequence multiple AWS services into serverless workflows, making it easier to build and visualize applications that require multiple steps, error handling, and conditional logic.

Container

- 1개의 물리서버에 여러 컨테이너가 동작한다.
- 서버의 OS와 물리 자원을 공유한다.

Container Orchestration

- 상태 모니터링
  - 이상 상태가 된 컨테이너 감지
  - 컨테이너가 종료된 노드에 새 컨테이너를 시작
- 스케일링
  - 컨테이너를 추가/삭제

ECS(Elastic Container Service)

- AWS에서 관리하는 컨테이너 오케스트레이션 서비스
- ECR(Elastic Container Registry) : 컨테이너 이미지를 AWS에서 관리하는 레지스트리에 저장하는 서비스
- ECS Cluster : 컨테이너를 실행하는 EC2 인스턴스의 집합. EC2 인스턴스 내에서 실행되는 컨테이너 런타임에서 컨테이너를 실행한다.
- Fargate : AWS에서 관리하는 서버에서 컨테이너를 실행하는 서비스

ECS Cluster

- OS, 미들웨어 업데이트, 패치 등의 관리 책임은 사용자에게 있다.

Fargate

- 런타임, OS는 PV(platfrom version)에 의해 결정된다.
- 사용자 책임 범위는 컨테이너 내에서 실행되는 응용프로그램
- 상대적으로 비쌈.
- 서버측을 AWS가 알아서 관리

EKS(Elastic Kubernetes Service)

- 쿠버네티스를 사용해야할 경우

기타 컴퓨팅 서비스

AWS Lightsail

> 일반적으로 자주 사용되는 구성의 가상서버를 쉽고 빠르게 구축

AWS Elastic Beanstalk

> Java, .NET, PHP, Node.js, Python, Ruby, Go, Docker, Tomcat, Apache, Nginx, 등 주요 언어나 환경에서 개발된 응용프로그램을 배포하기 위한 실행환경을 자동으로 생성

- 여러 배포방식을 지원
- 배포 방식
  - All at once : 모든 인스턴스의 응용프로그램을 한번에 교체하는 방식
  - Rolling : 각 인스턴스의 app을 순서대로 교체하는 방식. 교체중인 인스턴스만 서비스 중단
  - Immutable : 새로운 인스턴스를 추가하고, 기존 인스턴스를 삭제하는 방식. 서비스 중단 없음

AWS Batch

> 지정된 프로그램을 EC2나 Fargate에서 실행하는 서비스

- Lambda와 유사하지만 실행 프로그램의 순서 관리나 다수 프로그램의 병렬 구동과 같은 복잡한 제어에 특화된 서비스

AWS Outposts

> 사용자가 온프레미스 환경에서 AWS와 같은 서비스를 이용할 수 있도록 AWS가 물리 서버를 대여하는 서비스

- 데이터 센터에 설치할 수 있는 서버 기기 세트가 제공
- 데이터 센터에 AWS 일부 서비스를 가져온 것처럼 이용할 수 있다.
- AWS 서비스와 동일한 API를 사용할 수 있다.

S3(Simple Storage Service)

> 객체 스토리지 서비스

- 객체 키로 데이터를 고유하게 식별해 데이터의 입출력과 관리 실행
- 용량 무제한(객체당 5TB까지)
- 높은 내구성(데이터가 3개 이상의 AZ에 복제)
- 저렴한 비용
- 다양한 AWS 서비스에서 데이터 연계를 위해 사용
  - VPC 흐름로그 저장
  - CloudTrail 로그 저장
  - Amazon CloudFront 접속로그 저장
- 다른 도구에서 공통창구를 통해 S3의 데이터 조작

버킷 : 객체 스토리지를 저장하는 공간

객체 : 버킷에 저장된 데이터 본체

키 : 객체의 저장 URL 경로

Storage Class

- 수명주기설정기능 : 생성한지 일정 시점이 지난 객체를 다른 스토리지 클래스로 이전
- S3용 엑세스 분석기 : 얼마나 접근이 있었는지 데이터의 접근 상황을 확인해 참고
- S3 버전관리 기능 : 모든 세대의 객체에 대한 이력 정보 보존됨
- S3 Standard : 기본 스토리지 클래스
- S3 Intelligent-Tiering : 자동으로 스토리지 클래스를 변경하는 기능이 추가된 스토리지 클래스. 접근 빈도에 따라 4개의 접근 계층으로 자동으로 나눠 비용 절감
- S3 Standard-IA : S3 Standard보다 저렴한 스토리지 클래스. 자주 접근하지 않는 데이터에 사용
- S3 One Zone-IA : 1AZ에만 데이터를 저장. 데이터 검색에 요금 발생
- S3 Glacier Instance Retrieval : S3 Standard-IA보다 저렴한 스토리지 클래스. 데이터를 검색하는 시간이 길다.
- S3 Glacier Flexible Retrieval : S3 Glacier Instance Retrieval보다 저렴한 스토리지 클래스. 데이터를 검색하는 시간이 길다.
- S3 Glacier Deep Archive : S3 Glacier Flexible Retrieval보다 저렴한 스토리지 클래스. 데이터를 검색하는 시간이 길다.(12시간 이상)

S3 수명 추기

- 객체가 수명 주기동안 비용 효율적으로 저장되도록 개체를 관리할 수 있게 해주는 기능
- 불완전한 멀티파트 업로드를 정리하도록 S3 수명주기 정책을 구성함으로서 스토리지 비용을 줄일 수 있다.

Storage Lens

> 객체 스토리지 사용량, 활동 추세 및 비용 최적화를 위한 권장사항에 대한 종합적인 보기를 제공하는 완전관리형 S3 스토리지 분석 솔루션

교차 리전 복제(CRR : Cross Region Replication)

- 데이터를 한 리전에서 다른 리전으로 복제

재해 복구(DR : Disaster Recovery)

- 시스템을 구축할 때 가용성을 위해 하나의 리전 전체가 중단되더라도 시스템이 정상 동작하도록 구성

S3 데이터 외부 공개 및 접근제어

S3 Object Lock

- 두 Retention Mode 제공
  - Governance Mode : 특별 권한이 있는 사용자만 삭제 가능
  - Compliance Mode : 일정 기간이 지나기 전까지는 모든 사용자가 삭제 불가능

S3 객체 잠금(S3 Object Lock)을 사용하면 write-once-read-many(WORM) 모델을 사용하여 객체를 저장할 수 있습니다. 객체 잠금은 고정된 시간 동안 또는 무기한으로 객체의 삭제 또는 덮어쓰기를 방지하는 데 도움이 될 수 있습니다. 객체 잠금을 사용하면 WORM 스토리지가 필요한 규제 요구 사항을 충족하거나 객체 변경 및 삭제에 대한 보호 계층을 추가하는 데 도움이 됩니다.

S3 Gateway Endpoint

> EC2 인스턴스-S3 버킷 간 통신이 인터넷에 노출되지 않음 = S3 Gateway Endpoint

- VPC에서 게이트웨이 VPC 엔드포인트를 사용하여 Amazon S3에 액세스할 수 있습니다.
- 게이트웨이 엔드포인트를 생성한 후 VPC에서 Amazon S3로 전송되는 트래픽에 대해 해당 엔드포인트를 라우팅 테이블의 대상으로 추가할 수 있습니다.

- Amazon S3는 게이트웨이 엔드포인트와 인터페이스 엔드포인트를 모두 지원합니다.
- 게이트웨이 엔드포인트를 사용하면 VPC 인터넷 게이트웨이 또는 NAT 디바이스를 사용하지 않고 추가 비용 없이 VPC에서 Amazon S3에 액세스할 수 있습니다.
- 하지만 게이트웨이 엔드포인트는 온프레미스 네트워크, 다른 AWS 리전의 피어링된 VPC 또는 전송 게이트웨이를 통한 액세스를 허용하지 않습니다.
- 이러한 시나리오에서는 추가 비용을 지불한 후 사용할 수 있는 인터페이스 엔드포인트를 사용해야 합니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3용 VPC 엔드포인트 유형을 참조하세요.

Gateway Endpoint vs Interface Endpoint

Gateway Endpoint:

Purpose: A Gateway Endpoint is used to connect your VPC to AWS services over an Amazon VPC-specific gateway. This is typically used for services that have a gateway option, such as Amazon S3 and DynamoDB.

Routing: Traffic to services via Gateway Endpoints is routed over the AWS private network, not the public internet.

Service Support: Not all AWS services support Gateway Endpoints; it's only available for a subset of AWS services like Amazon S3, DynamoDB, and Kinesis.

Endpoint Type: Gateway Endpoints use a VPC endpoint type called "Gateway" and are associated with a specific route table within your VPC.

Interface Endpoint:

Purpose: An Interface Endpoint is used to connect your VPC to AWS services using Elastic Network Interfaces (ENIs) in your VPC. This is often used for AWS services that don't have a VPC gateway option, like AWS Systems Manager (SSM) or AWS Elastic Load Balancing.

Routing: Traffic to services via Interface Endpoints is also routed over the AWS private network, not the public internet.

Service Support: Interface Endpoints are available for a wider range of AWS services, making them more versatile. You can create Interface Endpoints for services like AWS Systems Manager, AWS Key Management Service (KMS), and Amazon CloudWatch.

Endpoint Type: Interface Endpoints use a VPC endpoint type called "Interface" and are associated with a specific subnet in your VPC.

접근제어방식

- IAM 정책 : 사용자 권한 설정
- 접근제어 목록 (ACL) : 객체 또는 버킷 단위러 설정할 수 있는 접근제어 방식. ex) 데이터 A는 계정 X에 접근허용
- 버킷 정책 : 버킷단위로 설정하는 접근 방식. json으로 복잡한 설정 수행 가능

퍼블릭엑세스 차단기능 : 버킷이나 객체가 외부 공개가 되지 않도록 주의

S3 + CloudFront : Static Web Hosting

- S3의 웹 사이트 호스팅 기능을 활성화
- HTML, CSS, JS, 이미지 등의 정적 파일을 S3에 저장하고 CloudFront를 통해 배포하는 방식
- S3 자체적으로 https를 지원하지 않기 때문에 CDN 서비스인 CloudFront를 통해 https 통신이 가능하게끔 구성

KMS(Key Management Service)

- 버킷의 기본 암호화 기능을 활성화하면 객체를 저장할 때 AWS에서 자동으로 암호화 수행
- 암호화용 키는 AWS에서 제공하는 키 관리 기능인 KMS를 사용
- 사용자 관리키(SSE-C)를 사용하는 경우 사전에 키 생성 필요

Client Side Encryption(클라이언트 사이드 암호화)

데이터를 Amzaon S3에 업로드 하기 전에 데이터를 암호화 하는 방법

S3에서 제공되는 기능은 객체 저장시 암호화이므로 S3로 전송할 때 암호화하고 싶다면 미리 데이터를 응용 프로그램에서 암호화해 전송해야 하는 데, 이를 Client Side Encryption이라고 한다.

Server Side Encryption

Server Side Encryption은 S3에서 제공하는 기능으로 객체 저장시 암호화를 수행한다.

KMS Multi Region Key (다중 리전 키)

여러 리전에서 동일한 키를 가지고 암호화를 수행할 수 있게끔 하는 기능

재해 복구
백업 및 복구 아키텍처에서 다중 리전 키를 사용하면 AWS 리전 중단이 발생한 경우에도 중단 없이 암호화된 데이터를 처리할 수 있습니다. 백업 리전에서 유지 관리되는 데이터는 백업 리전에서 해독할 수 있으며, 백업 리전에서 새로 암호화된 데이터는 해당 리전이 복원될 때 기본 리전에서 해독할 수 있습니다.

글로벌 데이터 관리
전 세계적으로 운영되는 비즈니스에는 AWS 리전에서 일관되게 사용할 수 있는 전 세계적으로 분산된 데이터가 필요합니다. 데이터가 상주하는 모든 리전에서 다중 리전 키를 만든 다음 교차 리전 호출의 지연 시간 또는 각 리전의 다른 키로 데이터를 다시 암호화하는 비용 없이 단일 리전 키인 것처럼 키를 사용할 수 있습니다.

분산 서명 애플리케이션
교차 리전 서명 기능이 필요한 애플리케이션은 다중 리전 비대칭 서명 키를 사용하여 다른 AWS 리전에서 일관되고 반복적으로 동일한 디지털 서명을 생성할 수 있습니다.

단일 글로벌 신뢰 스토어(단일 루트 CA(인증 기관) 및 루트 CA에서 서명한 리전의 중간 CA에 대해 인증서 체인을 사용하는 경우 다중 리전 키가 필요하지 않습니다. 그러나 시스템에서 애플리케이션 서명과 같은 중간 CA를 지원하지 않는 경우 다중 리전 키를 사용하여 리전 인증에 일관성을 유지할 수 있습니다.

여러 리전에 걸친 활성/활성 애플리케이션
일부 워크로드 및 애플리케이션은 여러 리전에 걸쳐 활성/활성 아키텍처에 있을 수 있습니다. 이러한 애플리케이션의 경우 다중 리전 키는 리전 경계를 넘어 이동할 수 있는 데이터에 대한 동시 암호화 및 해독 작업에 동일한 키 구성 요소를 제공하여 복잡성을 줄일 수 있습니다.

클라이언트 측 암호화 라이브러리(예: AWS Encryption SDK, DynamoDB 암호화 클라이언트 및 Amazon S3 클라이언트 측 암호화)와 함께 다중 리전 키를 사용할 수 있습니다. Amazon DynamoDB 글로벌 테이블 및 DynamoDB 암호화 클라이언트에서 다중 리전 키를 사용하는 예는 AWS 보안 블로그의 AWS KMS 다중 지역 키로 글로벌 데이터 클라이언트 측 암호화를 참조하세요.

EBS(Elastic Block Store)

> EBS는 EC2와 함께 사용하는 스토리지 서비스다. EC2의 HDD/SSD와 같은 역할을 하며 EC2에서 실행되는 응용 프로그램의 데이터,로그, 설정 정보 등을 저장하는데 주로 사용한다.

EC2의 HDD/SSD로 이해하면 된다

EBS 볼륨 유형

IOPS(I/O per second)

EBS의 읽기/쓰기 성능을 나타내는 지표. 초당 쓰기/읽기 횟수를 나타낸다.

- 범용 SSD(gp2, gp3) : 일반적인 응용 프로그램에 사용
- 프로비저닝된 IOPS SSD(io1, io2) : 초당 IOPS가 높은 응용 프로그램에 사용.
  필요한 IOPS를 미리 예약해야 한다.
  - Provisioned IOPS : 50 IOPS ~ 64,000 IOPS

    - storage performance 가 키워드이다.
- 처리량 최적화 HDD(st1) : 대량의 데이터를 처리하는 응용 프로그램에 사용. 저비용 마그네틱 스토리지
- Cold HDD(sc1) : st1보다 훨씬 저렴한 비용의 마그네틱 스토리지. 접근 빈도가 낮을 때 사용

특별히 요구되는 성능 사항이 없다면 범용 SSD 선택, 고성능 응용 프로그램을 실행하는 경우 프로비저닝 된 IOPS SSD, 가능한 저렴하게 사용하고자 한다면 최적회 HDD나 Cold HDD를 선택한다

EBS Snapshot

- Snapshot을 활용해 EBS 볼륨을 백업하고, 복원할 수 있다.
- Snapshot과 몇가지 설정 정보를 조합해 **사용자 전용AMI** 생성 가능

빠른 스냅샷 복원

빠른 스냅샷 복원을 활성화 하면 스냅샷에서 새 Amazon Machine Image를 빠르게 생성할 수 있음
-> 프로시져닝할 때 초기화 지연시간을 줄일 수 있다.

EFS(Elastic File System)

> 비교적 고속으로 데이터를 전송할 수 있는 NFS(Network File System)

- Managed NFS(Network File System) that can be mounted on many EC2
- works with Linux EC2 instances in multi-AZ
- Highly available, scalable, expensive (3x gp2), pay per use, no capacity planning
- Compatible with only linux based AMI

기타 스토리지 서비스

FSx

> 파일서버를 쉽게 구축할 수 있는 서비스

- Amazon FsX for Windows File Server : Windows용 파일서버
- Amazon FsX for Lustre : Lustre용 파일서버(고성능 파일시스템)

- Amazon FSx for NetApp ONTAP : 리눅스와 윈도우 파일 시스템 사이의 데이터 공유를 위한 파일 서버

Amazon FsX for Lustre

컴퓨팅 워크로드를 위한 비용효율적이고 확장가능한 고성능 스토리지를 제공하는 **완전관리형 서비스**

Amazon FsX for Windows File Server

온프레미스-AWS간 스토리지 서비스 중 SMB 지원하는건 Storage Gateway File Gateway, Amazon Fsx for Windows라고 보면 됨

SMB(Server Message Block)

서버 메시지 블록(Server Message Block, SMB)은 도스나 윈도우에서 파일이나 디렉터리 및 주변 장치들을 공유하는데 사용되는 메시지 형식이

AWS Storage Gateway

> 온프레미스에 서버 기기 혹은 가상서버에 설치해 온프레미스와 AWS의 S3, FSx, EBS를 직접 연결하는 서비스

키워드는 SFTP, FTP
, No change to customer applications, Fully managed service

AWS Transfer Family

> SFTP, FTPS, FTP 와 같은 FTP 기반 프로토콜로 통신하기 위한 서버를 구축하는 서비스

- 수동 관리 또는 운영 오버헤드 없이 고가요성 SFTP 솔루션 제공

AWS Backup

> 스토리지 , RDS , DynamoDB 등의 데이터를 백업하는 서비스

- 사용자가 AWS 서비스 전체에서 데이터 백업을 중앙 집중화하고 자동화할 수 있는 완전관리형 서비스.
- 백업 빈도 및 보존 기간을 지정하는 백업 계획을 생성하고 관리할 수 있다.
- 백업 데이터를 저장하는 컨테이너인 백업 Vault에 백업 리소스 할당 가능.

AWS DataSync

> 온프레미스와 AWS혹은 AWS 스토리지 서비스 간 데이터 전송을 위한 서비스

- 온프레미스 서버에 DataSync라는 에이전트를 설치해 스토리지 서비스와 연결

AWS Snow Family

> 테라바이트 단위의 데이터를 AWS로 전송하는 서비스

- 물리 스토리지를 AWS에서 빌려 거기에 데이터를 저장하고 AWS로 반환하면 해당 데이터를 직접 AWS내의 스토리지에 옮겨주는 서비스
- 물리스토리지를 Snow 디바이스라 한다.
  - Snowcone : 8TB
  - Snowball : 80TB
  - Snowmobile : 100PB

네트워킹 서비스

VPC(Virtual Private Cloud)

> AWS에서 생성할 수 있는 프라이빗 가상 네트워크

- 일반적으로 Private IP 주소를 사용
- **테넌시**라는 라이센스 및 보안 요구사항이 있다.

VPC 구성요소

- 인터넷 게이트웨이 : VPC와 인터넷을 연결하는 게이트웨이
- 서브넷 : VPC 내부의 네트워크 영역
- 라우팅 테이블 : 서브넷과 인터넷 게이트웨이를 연결하는 라우팅 테이블
- 보안 그룹 : 인스턴스에 대한 인바운드/아웃바운드 트래픽을 제어하는 가상 방화벽
- DNS 서버 : VPC 내부에서 사용하는 DNS 서버
- NTP : VPC 내부에서 사용하는 NTP 서버

서브넷

- VPC 만으로는 EC2와 같은 자원을 네트워크에 만들 수 없다.
- **서브넷을 만들어야 EC2와 같은 자원을 네트워크에 연결할 수 있다.**
- 서브넷은 하나의 AZ에 속해야 하며 여러 AZ에 걸쳐 있을 수 없다.
- 서브넷은 VPC의 CIDR 범위 내에서 생성해야 한다.
- 서브넷은 두 가용영역에 걸쳐 생성할 수 없다.

- 퍼블릭 서브넷을 생성하고 이를 ALB와 연결해 인터넷 트래픽이 프라이빗 서브넷에 있는 EC2 인스턴스에 인바운드로 도달하게끔 할 수 있다.

라우팅 테이블

> 네트워크 경로 정보 테이블

- 기본적으로 VPC 내의 라우팅 정보만 있으므로 VPC 외부로는 통신할 수 없다.
- VPC 외부로 통신하려면 라우팅 테이블에 인터넷 게이트웨이를 추가해야 한다.

인터넷 게이트웨이

> 서브넷 안에 있는 EC2와 같은 자원이 인터넷과 통신할 수 있게 하기 위한 기능

- 퍼블릭 서브넷 : 인터넷 게이트웨이를 통해 인터넷과 통신할 수 있는 서브넷
- 프라이빗 서브넷 : 인터넷 게이트웨이를 통해 인터넷과 통신할 수 없는 서브넷

NAT 게이트웨이(Nwetwork Address Translation)

> 프라이빗 서브넷에 있는 EC2와 같은 자원이 인터넷과 통신할 수 있게 하기 위한 기능

- Private IP 주소를 Public IP 주소로 변환해 인터넷과 통신할 수 있게 한다.
- NAT 게이트웨이를 이용해 통신하기 위해서는 외부 통신을 수행하는 서브넷의 라우팅 테이블에 경로 정보를 등록해야한다.

VPC 보안사항

네트워크 ACL vs 보안그룹

네트워크ACL

- **서브넷 단위로 적용**
- 허용 및 거부 규칙을 지정할 수 있다.
- Stateless. 단일 패킷만 확인하므로 정보를 저장하지 않음
- 등록된 규칙의 번호 순으로 트래픽 허용 및 거부

보안 그룹

- **인스턴스 단위로 적용**
- 허용만 설정 가능

- Stateful. 패킷과 관련된 세션까지 확인하므로 정보를 저장
- 등록된 모든 규칙을 평가해 트래픽 허용

ENI(Elastic Network Interface)

- VPC의 가상 네트워크 카드
- EC2 인스턴스에 연결되어 인스턴스의 네트워크를 제어
- 로그는 네트워크 인터페이스 별로 출력됨

VPC 흐름로그(VPC Flow Logs)

> VPC 내의 IP 트래픽 상황을 로그로 저장할 수 있는 기능.

VPC log + CloudWatch

- 로그는 모니터링 서비스인 CloudWatch Logs 또는 S3에 저장할 수 있다.

VPC끼리 연결

VPC 피어링

> VPC 피어링 연결을 사용하면 인터넷 게이트웨이, VPN연결 또는 NAT장치 없이 private ip 주소를 사용하여 서로 다른 VPC의 인스턴스간 안전한 통신 가능.

- VPC피어링을 설정하면 VPC-A에서 실행주인 어플리케이션이 공용 인터넷이나 단일 장애 지점을 거치치 않고 VPC-B의 EC2에 직접 엑세스 가능
- 서로 다른 두 개의 VPC를 연결해 통신
- 3개의 VPC가 서로 통신하는 경우 각 VPC끼리 따로 피어링 구성
- VPC간에 피어링 연결을 생성하는 것은 연결을 설정하는 비용 효율적인 방법이다. 두 VPC에서 피어링 연결을 위한 라우팅 테이블 항목을 추가하면 두 VPC간에 트래픽이 흐를 수 있다.

AWS Transit Gateway

- VPC연결을 하나의 중앙 허브에서 관리
- 요금은 VPC피어링을 사용하는 것보다 높음

VPC와 다른 AWS 서비스 연결

VPC 엔드포인트(VPC Endpoint)

- 프라이빗 네트워크로 통신
- 인터넷을 통하지 않고 AWS내부 네트워크를 통해 연결할 수 있다.
- 게이트웨이 엔드포인트(gateway VPC endpoint) : S3와 DynamoDB에 연결
  - **A gateway VPC endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. Gateway endpoints support services such as Amazon S3 and DynamoDB. Gateway endpoints are available in all AWS Regions.**
- 인터페이스 엔드포인트 : AWS PrivateLink라는 기능을 사용해 서브넷에 서비스 접속용 ENI를 생성해 다른 AWS 서비스에 연결

VPC와 온프레미스 연결

AWS Site to Site VPN

- VPN(Virtual Private Network)을 사용해 온프레미스와 VPC를 연결
- VPN은 IPsec라는 프로토콜을 사용해 암호화된 터널을 만들어 통신
- VPN을 통해 외부 네트워크와 Private IP로 통신

AWS Client VPN

- 온프레미스 환경의 클라이언트 단말(PC)과 VPN을 연결하는 AWS Client VPN

AWS Direct Connect

- **전용선을 사용해 온프레미스와 VPC를 연결**
- 대역폭이 크고 안정적이다.
  - 어떤 매체나 기기를 경유하여 정보를 전송할 때의 전송량을 대역폭 또는 밴드 폭이라 한다.
- VPC외의 AWS 서비스에도 연결 가능
- VPN보다 안정적이고 빠르다.
- 이용 비용이 높고 서비스 이용 신청 후 일정 기간이 지나야 사용 가능

VPC 구성 예시

Web + DB + Amazon CloudFront

- 온프레미스 환경의 웹 서버
- VPC외부에 CloudFront를 이용해 웹 콘텐츠를 캐싱해 사용자가 콘텐츠에 빠르게 접근할 수 있게끔 함
- CloudFront를 사용해 세계 각지에 있는 엣지 로케이션에 웹 콘텐츠가 캐시됨-> latency 최소화

Web + DB + Amazon CloudFront + VPC Endpoint + S3

- VPC엔드포인트와 S3 버킷 추가
- RDS에서 취득한 데이터를 S3에 저장하거나 S3에서 얻은 데이터를 다른 데이터베이스로 가져오는 프로세스를 가정한다.

온프레미스 환경에서 프라이빗 연결

- VPC와 온프레미스 환경만 통신 가능

ELB(Elastic Load Balancing)

> AWS에서 제공하는 로드 밸런서 서비스

- 부하 분산 기능 : 트래픽을 여러 대상으로 분산
- 대상 모니터링 기능 : Cloudwatch를 통해 대상의 상태를 모니터링. 감시를 통해 비정상적 동작 감지시 대상을 자동으로 분리
- 보안 기능 : SSL/TLS 암호화를 지원. 암호화 통신 수행

ELB 유형

- Application Load Balancer : HTTP, HTTPS 트래픽을 분산(7계층)
- Network Load Balancer : TCP, UDP 트래픽을 분산(4계층)
  - Only accept either TCP or UDP traffic
  - Support http, https, tcp health check
  - only accept either selectiing ec2 instance or ip address as target
  - can not provide a url to endpoint
- Classic Load Balancer : 구형 로드 밸런서. 기본적으로 사용하지 않는다.

- Gateway Load Balancer :
  - AWS에서 제공하는 타사 보안 제품의 배포 및 관리 기능
  - 레이어 3(네트워크 계층)에서 동작
  - 기존 NLB 및 VPC 피어링, Transit Gateway 에서 구현하던 아키텍쳐를 더욱 단순하게 구현 가능

Route 53

> AWS가 제공하는 완전관리형 DNS 서비스

- 호스팅 존 별로 수행됨
  - 호스팅 존 : 도메인과 해당 도메인의 트래픽 라우팅 방법에 대한 정보를 보관하는 상자 같은 것
- 도메인 등록 기능
- 트래픽 라우팅 기능
- 자원상태 확인 기능

도메인 등록기능

- `example.com` 과 같은 도메인 이름을 Route 53에서 DNS 레코드로 등록

트래픽 라우팅 기능

- 사용자의 요청을 적절한 서버로 라우팅하는 기능
- 기본적으로 도메인 이름에 대한 IP주소를 어떻게 반환하는 지를 의미

라우팅 정책(Routing Policy)

> AWS Route53이 쿼리에 응답하는 방식

- 단순 라우팅 : 하나의 도메인에 대해 하나의 IP 주소 연결
- 가중치 라우팅 : 라우팅 대상을 여러 개 등록하고 각각에 트래픽을 할당하는 정도를 0에서 255 사이로 조정.가중치 기반 트래픽 분산
- 지리적 위치 라우팅 : 사용자의 지리적 위치에 따라 트래픽을 분산
- 지연 시간 라우팅 : 항상 레이턴시(데이터 처리 지연시간)이 최소인 자원의 IP 주소를 우선적으로 반환
- 장애 조치 라우팅 : 일반적인 프라이머리 IP로 라우팅 하지만 프라이머리 IP가 다운되면 세컨더리 IP로 라우팅

=> 로드 밸런싱 용으로 사용하기 어려움. 첫번째 리소스가 비정상인 경우에만 두 번째 리소스로 라우팅 하기 때문

- 다중 값 응답 라우팅 : 여러 IP주소를 무작위로 반환

자원 상태 확인 기능

- 라우팅하는 웹서버 응답 결과 확인

CloudFront

> AWS에서 제공하는CDN(Content Delivery Network . 컨텐츠 전달 네트워크) 서비스

- 원본서버(Origin Server)에 있는 콘텐츠를 복사해서 전세계에 존재하는 캐시 서버에 저장
- 캐시서버는 전세계 **엣지 로케이션**에 배치됨
- 동영상 파일과 같은 대용량 컨텐츠는 가장 가까운 캐시 서버에서 가져온다.
- 장점
  - 대용량 컨텐츠의 빠른 배포
  - 보안 향상 : AWS Shield와 AWS WAF를 사용해 DDoS 공격 대응. WAF 설정을 할 경우 사용료가 부과
  - 가용성 향상

CloudFront 캐시 삭제

- CloudFront의 캐시를 삭제함으로써 Static 페이지를 빠르게 갱신할 수 있다.(최신버전으로 유지)

필드 레벨 암호화(Field Level Encryption)

- Amazon CloudFront를 사용하면 Https를 통해 오리진 서버에 대한 종단 간 보안 연겨를 적용할 수 있음.
- 필드 레벨 암호화는 추가 보안 레이어를 추가하여 시스템 처리 전체에서 특정 데이터를 보호하고 특정 어플리케이션만 이를 볼 수 있도록 함

CloudFront Origin Access Identity(OAI)

> CloudFront에서 S3 버킷에 접근할 때 사용하는 엔터티

- CloudFront OAI의 엑세스를 허용하도록 버킷 정책을 구성하면 CloudFront를 통해서만 S3에 안전하게 엑세스 가능

I want to restrict access to my Amazon Simple Storage Service (Amazon S3) bucket so that objects can be accessed only through my Amazon CloudFront distribution. How can I do that?
Create a CloudFront origin access identity (OAI)
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/

Accept-Language 헤더

- Accept Language 헤더를 사용해 캐시동작 설정 => 사용자의 언어에 맞는 콘텐츠를 제공할 수 있다.
- Caching content based on the Accept-Language header
  https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html#header-caching-web-accept-language

CloudFront Signed URL

- CloudFront Signed URL을 사용하면 CloudFront에 캐시된 개별 파일에 대한 엑세스를 제한할 수 있다.

기타 네트워킹 서비스 7개

전용선 및 VPN 연결

> 전용선 : 거점 간에 물리적으로 연결된 전용의 통신회선
> VPN : Virtual Private Network. 인터넷을 가상으로 전용선처럼 취급하는 기술.

AWS Direct Connect

> AWS와 온프레미스 환경을 전용선으로 연결하는 서비스(DX)

AWS VPN

- AWS Site-to-Site VPN : 온프레미스 환경과 AWS간의 VPN 연결
- AWS Client VPN : 온프레미스 환경의 클라이언트 단말과 VPN 연결

AWS Transit Gateway

> 여러 VPC를 하나의 중앙 허브에서 관리하는 서비스.

- VPC간 통신을 깔끔하게 정리할 수 있다.

AWS Ground Station

> 인공위성과의 통신 제공

AWS PrivateLink

> VPC 엔드포인트를 생성해 인터넷을 통하지 않고 내부적으로 다른 VPC와 통신을 할 수 있다.

- 접속 제어와 같은 설정 가능

Amazon API Gateway

> 웹 API를 생성하는 서비스

- 자체적으로 웹 서버를 구축하지 않아도 API를 생성할 수 있다.
- 문제에 RestFul 웹 서비스 => API 게이트웨이

AWS Global Accelerator

> 전세계에 퍼져있는 AWS네트워크 망을 이용해 클라이언트가 AWS에 더 빠르게 접근할 수 있게 해주는 서비스

- AWS 자체 네트워크 사용
- TCP, UDP 트래픽을 가속화
- 상태 확인을 기반으로 최적의 정상 엔드포인트로 트래픽 전달
- 가장 가까운 엔드포인트로 트래픽을 전달

Endpoint Group

:

Endpoint Groups: By creating endpoint groups in both the us-west-2 and eu-west-1 Regions, the company can effectively distribute traffic to the NLBs in both Regions. This improves availability and allows traffic to be directed to the closest Region based on latency.

데이터베이스 서비스

Amazon Relational Database Service(RDS)

스토리지 유형

- 범용 SSD : 고성능으로 용량에 따라 읽기/쓰기 성능 결정
- 프로비저닝된 IOPS SSD : 고성능 지정한 읽기/쓰기 성능 확보
- 마그네틱 HDD : 저렴한 비용

Standby Replica and Read Only Replica

Standby Replica

> 프라이머리 인스턴스 외에 복제본(Standby Replica) 을 사용해 가용성을 높일 수 있다.

- 다중 AZ 배포를 통해 고가용성 구현
- Fail Over : 프라이머리 인스턴스가 다운되면 복제본이 프라이머리로 승격

Read Only Replica

> 프라이머리 인스턴스에서 복제된 레플리카 -> 읽기 요청이 늘어나면 인스턴스의 수를 늘리는 Scale Out 방식으로 성능을 향상할 수 있다.

읽기 전용 레플리카를 구현하기 전에 할 일

- 원본 DB인스턴스에서 장기 실행 트랜잭션이 완료되도록 허용: 진행 중인 모든 트랜잭션이 변경사항을 구현하기 전에 완료되도록 함 -> 무결성과 일관성 유지
- 백업 보존기간을 0 이외의 값으로 설정 : 자동 백업 활성화

RDS Proxy

> 관계형 DB에서 커넥션 연결을 효율적으로 관리해주는 서비스

- 데이터 베이스 연결 최적화
- 읽기 성능 개선
- 어플리케이션 아키텍쳐 변경 최소화

https://aws.amazon.com/rds/proxy/

RDS Proxy minimizes application disruption from outages affecting the availability of your database by automatically connecting to a new database instance while preserving application connections. When failovers occur, RDS Proxy routes requests directly to the new database instance. This reduces failover times for Aurora and RDS databases by up to 66

보안설정과 백업

- RDS 접근 제어
  - 최소 두 개의 서브넷 필요
  - 서브넷은 리전 내의 서로 다른 AZ 지정
- DB엔진 업데이트
- 데이터 백업
  - 자동 백업 : 사용자가 지정한 일 수 만큼의 스냅숏이 자동 유지
  - 특정 시점 복구(PITR) : Point in Time Recovery

Aurora

> DB 클러스터라는 단위로 관리되며 처리를 수행하는 하나 이상의 DB인스턴스와 데이터를 관리하는 클러스터 볼륨으로 구성

- Multi AZ에 걸친 글로벌 데이터 베이스
- 두 개의 기본 인스턴스가 있는 멀티 마스터 클러스터
- 스토리지 관리를 AWS가 수행
- 자체 자동 백업 기능
- 인스턴스 크기 지정이 필요하지 않은 Aurora Serverless
- S3와 연계한 파일 내보내기, 가져오기 기능

WARM Standby

- 감소된 수준의 트래픽 즉시 처리 가능
- 기존 배포를 확장해야 하기 때문에 파일럿 라이트보다 RTO 시간이 짧음

Pilot Light

> 복구를 위해 필요한 최소한의 리소스만을 미리 준비해두는 것
> 복구를 위한 리소스가 준비되어 있어야 한다.

Aurora Replica

- 1개 레플리카로 가용성 향상과 읽기 성능 향상을 모두 달성 가능
- 장애가 발생하면 그 즉시 프라이머리 인스턴스로 전환

Aurora Cross Region Replica

- 글로벌 웹 어플리케이션을 사용할 경우 데이터를 복제헤 인스턴으를 다른 리저에 생성하는 것보다 복제본을 사용해 각 지역에서 읽기 쿼리를 할 때 지연시간을 줄이는 것이 더 좋음

Amazon Aurora Global Database

> 단일 Amazon Global Aurora 데이터베이스를 여러 AWS리전으로 확장할 수 있는 기능

Amazon RDS 다중 AZ 배포

> 단일 AWS리전 내의 데이터베이스 인스턴스에 대한 향상된 가용성 제공

Amazon Aurora Global Database와 RDS 다중 AZ 배포의 차이

Global Database는 여러 리전에 걸쳐 확장되지만 RDS 다중 AZ 배포는 단일 AWS 리전 내의 데이터베이스 인스턴스에 대한 향상된 가용성 제공

DynamoDB

> AWS에서 제공하는 Key-Value Database

- **시나리오에서 계층적 구조로 데이터 저장이라는 말이 나오면 DynamoDB**
- 예약량을 초과하는 요청에 대해 오류를 반환하지만 Auto Scaling을 사용하면 실제 요청 수에 따라 지정된 범위 내에서 예약량을 자동으로 변경할 수 있다.
- 사용자는 레코드의 집합체인 테이블을 생성할 뿐 테이블 조작 요청은 DynamoDB가 직접 처리
- 사용자가 인스턴스를 소유한다는 개념이 없고 DynamoDB라는 하나의 서비스가 요청을 처리
- 커패시티 유닛(처리량)
    - RCU : Read Capacity Unit
    - WCU : Write Capacity Unit

DynamoDB Accelerator(DAX)

> DynamoDB의 읽기 성능을 향상시키는 서비스

- DynamoDB와 DAX가 결합되면 성능을 한 단계 업그레이드 하여 읽기 중심의 워크로드에서 초당 수백만개의 요청에도 마이크로 초의 응답 시간을 지원함
- 완전 관리형 서비스

DynamoDB 이용 예

- 하루에 10조건 이상, 초당 2000만 건 이상의 요청을 고속 단위로 처리할 수 있다.
- 모바일, 웹, 게임, 광고, IOT와 같이 데이터 교환이 매우 많고 사용자에게 빠른 응답이 필요한 응용 프로그램에 이용됨

Redshift

> 데이터 웨어하우스 서비스

- 기본적으로 데이터 분석을 위한 서비스
- 분석하기 쉽게 열별로 데이터를 저장
- 분석 및 데이터 읽기에 특화된 데이터베이스이므로 insert나 update 대신 COPY 명령을 사용해 S3 버킷에서 여러 개의 텍스트 데이터를 병렬로 업로드

Redshift 구성

- 리더 노드 : SQL 연결을 받아들이는 노드
- 컴퓨터 노드 : 스토리지 및 SQL문을 실행하는 컴퓨터 노드
- RA3 : 최신 Redshift에서 사용. RA3는 캐시(임시) 데이터를 컴퓨팅 노드로 가져오고 실제 데이터는 S3에 보관한다.

Data Migration Service

- 시스템 마이그레이션을 할 때 데이터베이스 마이그레이션이 가장 어려우며 다운타임(서비스 중단)이 발생할 수 있다.

AWS Database Migration Service(DMS)

> 데이터베이스 마이그레이션 서비스

AWS Schema Conversion Tool(SCT)

> 데이터베이스 스키마 변환 서비스

- 스키마는 데이터 베이스 설계도 역할을 한다.

기타 데이터베이스 서비스

Amazon ElastiCache

> 인 메모리 데이터 스토어 서비스

- 인메모리 캐시 서비스
- 주기억 장치에 데이터를 저장해 빠른 읽기 성능을 제공
- Redias와 Memcached를 지원

Amazon MemoryDB

> 데이터의 지속성을 확보하면서 빠른 읽기, 쓰기 성능 제공

Amaczon DocumentDB

> AWS에서 제공하는 MongoDB 호환 문서지향 데이터베이스 서비스

Amzaon Neptune

> AWS에서 제공하는 그래프 데이터베이스 서비스

AWS Quantum Ledger Database(QLDB)

> 원장 데이터를 관리하는 데이터베이스

- 저널이라는 로그 데이터에 기록되는 데이터의 변경 이려글 차례로 기록하는 방식
- 저널은 추가만 가능하며 변경이나 삭제를 할 수 없는 구조로 되어있어 신뢰성이 높다.

AWS Managed Blockchain

> 블록체인 네트워크를 구축하는 서비스

- 데이터의 변경 내역을 기록하는 원장을 네트워크에 참여한 여러 서버에서 협력해 관리하는 시스템

AWS Timestream

> 시계열 데이터베이스를 제공하는 서비스

보안 서비스

재해 복구 서비스

AWS CloudFormation

- 보조 리전에서 인프라 배포 자동화=> 재해발생시 템플릿에서 리소스 스택을 신속하게 시작할 수 있음

모니터링

AWS EventBridge

> Amazon EventBridge는 다양한 소스의 데이터와 애플리케이션을 연결하는 데 사용할 수 있는 서버리스 이벤트 버스 서비스

- 응용 프로그램이나 AWS에서 발생하는 이벤트를 다른 응용프로그램 또는 AWS와 연동하는 서비스
- 이벤트를 수신하고 이벤트를 대상으로 라우팅하는 규칙을 적용

AWS CloudTrail

> AWS 리소스의 API 호출 로그를 수집하는 서비스. 기본적으로 관리콘솔이나 프로그램에서의 작업, AWS에서 수행한 모든 작업 기록

- CloudTrail is a service that enables you to log and monitor all AWS API (Application Programming Interface) activity within your AWS account.
- It records events such as API calls made on your AWS resources, who made the calls, the source IP address, the time of the call, and more.
- CloudTrail provides a history of changes to resources, helping with security, compliance, and auditing requirements.
- It is often used for security and compliance purposes, tracking changes, and diagnosing issues.

You can configure CloudTrail to store logs in Amazon S3 and trigger ┣ CloudWatch Events based on certain criteria.

AWS CloudWatch

> AWS 리소스의 모니터링 및 이벤트 처리 서비스

- CloudWatch is a monitoring and observability service that collects and tracks metrics, collects and monitors log files, and sets alarms.
- It allows you to collect and visualize metrics about your AWS resources and applications in real-time.
- **CloudWatch Metrics can be collected from various AWS services, and you can create custom metrics for your applications.**
- **CloudWatch Alarms** enable you to set up alerts based on certain thresholds or patterns in your metrics.
- Combining CloudWatch Alarms with Auto Scaling enables you to scale your resources automatically based on the metrics.
    - With CloudWatch, you can combine several alarms into one composite alarm to create a summarized, aggregated health indicator over a whole application or group of resources.
- CloudWatch Logs is a feature of CloudWatch that allows you to collect, monitor, and store log files from various sources.
- It can be used to gain insights into the performance and health of your applications and infrastructure.

CloudWatch Logs

- CloudTrail은 로그를 S3나 CloudWatch Logs에 저장할 수 있다.
- S3에 저장하는 경우 파일 형태로 저장
- CloudWatch Logs에 저장하는 경우 스트림 형식으로 저장

IAM(Identity and Access Management)

> AWS를 사용하는 계정의 보안을 관리

IAM Role

- IAM 역할을 생성하고 외부 공급업체의 IAM 역할에 대한 엑세스 권한을 위임함으로서 계정간 신뢰 관계 형성 가느
- 공급업체의 자동화 도구가 회사 계정의 역할을 맡고 필요한 리소스에 엑세스 가능

AWS Config

> AWS 리소스의 구성 정보를 모니터링하고 관리

- create tags for resources

- 설정정보 모니터링

CloudTrail 과의 차이

- CloudTrail은 계정의 활동 이력을 저장하지만
- AWS Config는 AWS자원의 설정 내용 기반으로 이력을 저장한다.

AWS Certificate Manager

> AWS 서비스 및 연결된 리소스를 통해 SSL/TLS 인증서를 쉽게 발급, 프로비저닝 하고 배포
> https://aws.amazon.com/vpc/faqs/#:~:text=Can a subnet span Availability,within a single Availability Zone.

- ACM Private CA : AWS에서 제공하는 프라이빗 인증서 관리 서비스
- ACM does not support wildcard certificates
  - wildcard certificates : `*.example.com` 과 같이 서브도메인을 포함한 도메인에 대해 인증서를 발급하는 것
- ACM does not manage the renewal process for imported certificates
  - ACM은 인증서를 발급하지만 인증서 갱신은 직접 수행해야 한다.

AWS Trusted Advisor

> 구성된 AWS 인프라에 대한 평가를 통해 기존 모범 구성 사례들을 달성할 수 있는 권장사항을 제시하여 비용절감, 보안 향상, 서비스 최적화 등을 제시하는 서비스

AWS 작업 내용 감시

AWS GuardDuty

> AWS 계정 내의 모든 활동을 감시하는 위협 탐지 서비스

- 기계학습으로 이용 패턴을 학습해 루트 사용자로 로그인하는 행위를 탐지

탐지내용 예시

- 루트 계정 액세스
- IAM 액세스키 대량사용
- EC2가 DDos 공격을 위한 좀비 PC가 됐을 가능성

탐지 수행 출처

- CloudTrail을 사용해 AWS자원을 감시
- VPC흐름 로그를 사용해 네트워크 트래픽을 감시
- DNS 로그를 사용해 DNS 통신을 감지

웹 응용프로그램 방화벽

AWS WAF(Web Application Firewall)

> 네트워크 방화벽과는 달리 웹 응용프로그램의 취약점에 대한 공격을 탐지하고 방어하는 역할을 수행

Web ACL

> IP를 제한하거나 공격 코드를 탐지하는 등 요청에 대한 제어규칙을 만들고 이를 보호할 AWS 서비스에 적용만 하면 바로 WAF서비스 사용가능

- ACL : Access Control List

시스템 보안 관련 6가지 서비스

AWS Network Firewall

> VPC를 통한 통신에 대한 웹 방화벽 역할 수행

- 관리형 서비스이며 통신량에 따라 자동으로 처리량을 확장하기 때문에 가용성이 높다.

Amazon Inspector

> EC2 인스턴스에 대한 보안 취약점을 검사하는 서비스

AWS Shield

> DDoS 공격 대응 서비스. 별도의 설정 없이 자동으로 적용됨

- Standard
- Advanced

AWS Secrets Manager

> AWS Secrets Manager을(를) 사용하면 수명 주기 동안 데이터베이스 보안 인증, 애플리케이션 보안 인증, OAuth 토큰, API 키 및 기타 암호를 관리, 검색, 교체할 수 있습니다. 다수의 AWS 서비스는 Secrets Manager에 보안 암호를 저장하고 사용합니다.

- Secrets Manager를 사용하면 더 이상 애플리케이션 소스 코드에 하드 코딩된 보안 인증 정보가 필요하지 않으므로 보안 태세를 개선할 수 있습니다. Secrets Manager에 보안 인증 정보를 저장하면 애플리케이션 또는 구성 요소를 조사할 수 있는 누군가로 인해 손상될 가능성을 방지할 수 있습니다. 하드 코딩된 보안 인증 정보를 Secrets Manager 서비스에 대한 런타임 호출로 대체하여 필요할 때 동적으로 보안 인증 정보를 검색합니다.
- Secrets Manager를 사용하면 암호에 대한 자동 교체 일정을 구성할 수 있습니다. 따라서 단기 보안 암호로 장기 보안 암호를 교체할 수 있어 손상 위험이 크게 줄어듭니다. 보안 인증 정보가 더 이상 애플리케이션에 저장되지 않으므로 보안 인증 정보를 교체할 때 더 이상 애플리케이션을 업데이트하거나 애플리케이션 클라이언트에 변경 사항을 배포하지 않아도 됩니다.
- Rotate user credentials for database

AWS Security Hub

AWS Macie

> Amazon Macie는 기계 학습 및 패턴 일치를 사용하여 민감한 데이터를 검색하고, 데이터 보안 위험에 대한 가시성을 제공하며, 이러한 위험으로부터 데이터를 자동으로 보호하는 데이터 보안 서비스입니다.

- Amazon Macie는 Amazon S3 환경을 지속적으로 평가하고 계정 전반의 데이터 보안 태세를 요약하여 보여줍니다. 메타데이터 변수(예: 버킷 이름), 태그, 그리고 보안 제어(예: 암호화 상태 또는 공개적 접근성)를 기준으로 S3 버킷을 검색 및 필터링하고 정렬할 수 있습니다
- Amazon Macie를 사용하면 Amazon S3 버킷의 모든 객체나 일부 객체에 대해 **민감한 데이터 검색** 작업을 한 번, 매일, 매주 또는 매월 실행할 수 있습니다. 민감한 데이터 표적 검색 작업의 경우 Amazon Macie는 버킷의 변경 내용을 자동으로 추적하고, 시간이 지남에 따라 수정된 객체나 새 객체만 평가합니다.

AWS Cognito

> 웹 응용 프로그램이나 모바일 앱의 사용자 인증 및 권한 부여를 위한 서비스. 기본적으로 End User를 위한 것으로 IAM과 다르다.

- 인증된 사용자에게 IAM의 권한을 부여하는 것이 가능하다.

AWS Directory Service

> AWS에서 제공하는 Active Directory 서비스

- 파일시스템이 인증 및 엑세스 제어를 위해 기존 AD 인프라를 활용할 수 있다.
- Fsx for Windows File Server 파일시스템을 온프레미스 Active Directory에 결합하면 회사에서 기존 Active Directory그룹을 사용해 AWS로 이동한 수 파일공유, 폴더 및 파일에 대한 엑세스 제한 가능

AWS Security Token Service(STS)

기타 서비스

데이터 인식

Amazon Textract

> 이미지나 PDF 파일에서 텍스트를 추출하는 서비스

AWS Transcribe

> 다중 스피커 인식 서비스

Amazon Rekognition

> 이미지 및 비디오를 분석하고 분석 결과를 제공하는 서비스

- 부적절한 콘텐츠 감지 가능

Amazon Comprehend

> Amazon Comprehend는 기계 학습을 사용하여 텍스트를 분석하고, 감정 및 감정 키워드를 식별하며, 텍스트를 분류하고, 텍스트에서 키 구문을 추출하고, 텍스트에서 개체 및 키 구문을 추출하여 텍스트를 분석하는 완전관리형 서비스입니다.

데이터 분석(데이터 변환)

AWS Athena

> 표준 SQL을 사용해 S3에 저장된 데이터를 질의하는 서비스

- S3에 저장된 파일의 데이터구조를 스키마로 정의하고 Athena를 사용해 SQL로 데이터를 질의할 수 있다.

AWS Glue

> ETL처리 자동화

- **ETL기능을 활용하여 규모에 맞게 데이터 변환 작업을 정의하고 실행**
- AWS Glue + lambda(ETL job을 호출하는 lambda)
- job bookmarks : ETL 작업을 수행할 때마다 처리한 데이터의 위치를 저장해 다음 작업에서는 중복 데이터를 처리하지 않도록 함
- 원시 데이터를 수신하고, 원시데이터를 변환하고 .. => AWS Glue

This is the purpose of bookmarks: "AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data."
https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html

Amazon OpenSearch Service

> AWS 클라우드에서 OpenSearch 클러스터를 쉽게 배포, 운영 및 확장할 수 있는 완전관리형 서비스

- OpenSearch : Elasticsearch를 기반으로 만들어진 데이터분석용 엔진

Amazon EMR

> Apache Hadoop 및 Apache Spark 등의 분산처리 프레임워크를 사용해 데이터를 분석하는 서비스

Amazon QuickSight

> 데이터 시각화. 기계학습을 통한 특징추출, 추이 예상

Amazon Kinesis

- Kinesis Data Streams : 데이터를 실시간으로 수집, 처리, 분석하는 서비스
- Kinesis Data Firehose : 데이터를 수집해 S3, Redshift, Elasticsearch Service, Splunk 등의 서비스로 전송하는 서비스(실시간)
- Kinesis Data Analytics : 데이터 스트림을 분석하는 서비스
- Kinesis Video Streams

분석 파이프라인 예시

Amazon Kinesis Data Firehose + S3 + Amazon Kinetics Data Analytics

: 데잍터 스트림을 수집해 S3에 저장하고 Amazon Kinesis Data Analytics를 사용해 분석하는 파이프라인

Amazon Kinesis Data Streams + Amazon Kinetics Data Analytics

: 실시간 데이터 스트림을 분석하는 파이프라인

Amazon Elastic Transcoder

> 비디오 변환 서비스

AWS Lake Formation

> 데이터 레이크 생성 서비스

- **다양한 팀에서 모든 데이터를 사용할 수 있도록 해야할 경우**

지표 스트림을 사용한 대시보드 구축

- Amazon Cloudwatch 지표 스트림을 사용하여 EC2 Auto Scaling 상태 데이터를 Amazon Kinesis Data Firehose로 보냄

기계학습

Amazon SageMaker

시스템 관리(운영관리)

Amazon CloudFormation

Amazon CloudWatch

> AWS 리소스의 모니터링 및 이벤트 처리 서비스

Amazon CloudWatch Logs

Amazon CloudTrail

> AWS 리소스의 API 호출 로그를 수집하는 서비스

AWS Systems Manager

> EC2를 관리하는 서비스. AWS와 통신할 수 있는 환경이라면 온프레미스도 관리 가능

- Session Manager : EC2에 SSH 접속 없이 웹 콘솔에서 EC2에 접속
  - 인바운드 포트를 열거나 SSH 키를 관리할 필요 없이 안전하고 감사 가능한 노드 관리를 제공함
- Parameter Store : 시스템 환경변수로 사용할 수 있는 정보를 저장하는 기능. 소스코드에 인증정보를 저장하지 않고 Parameter Store에 저장해 사용
- Run Command : EC2에 명령을 실행
- Inventory : 관리 대상 서버에 설치된 소프트웨어 목록을 표시
- Patch Manager : OS나 미들웨어 패치 적용 및 관리
- Parameter Store : EC2에 설정 정보를 저장
- Document : Run Command, Automation, State Manager에서 사용하는 스크립트를 저장
  - Run command : EC2에 명령을 실행
  - Automation : EC2에 명령을 실행하는 스크립트를 저장
  - State Manager : 정기적으로 Document를 실행하는 것으로 EC2의 상태를 일정하게 유지

Amazon 코드 시리즈

AWS Appflow

> Amazon AppFlow는 클릭 몇 번으로 Salesforce, SAP, Google Analytics, Facebook Ads, ServiceNow와 같은 서비스형 소프트웨어(SaaS) 애플리케이션과 Amazon Simple Storage Service(S3) 및 Amazon Redshift와 같은 AWS 서비스 간에 데이터를 안전하게 전송할 수 있게 해 주는 완전관리형 통합 서비스입니다.

Amazon Pinpoint

> 다중 채널 고객 커뮤니케이션을 위한 서비스.Amazon Pinpoint Pinpoint는 여러 메시징 채널을 통해 고객과 소통하는 데 사용할 수 있는 AWS 서비스입니다. Amazon Pinpoint Pinpoint를 사용하여 푸시 알림, 이메일, SMS 문자 메시지 또는 음성 메시지를 보낼 수 있습니다.

- 양방향 메시징
- 고객 여정분석
- A/B 테스팅
- 특정 키워드가 포함된 메시지를 보낼 때 자동응답 생성 가능
- Amazon Lex를 사용해 대화형 봇을 만들 수 있음

Decoupling Applications

SQS(Simple Queue Service)

- Amazon Simple Queue Service(SQS)를 사용하면 메시지 손실을 우려하거나 다른 서비스를 제공할 필요 없이 소프트웨어 구성 요소 간에 어떤 볼륨의 메시지든 전송, 저장 및 수신할 수 있습니다.
- ChangeMessageVisibility : 메시지의 가시성을 변경
- 서버들끼리 사용할 수 있는 메세지 큐를 제공하는 서비스-
- 해야할 일을 나중에 처리하거나, 다른 시스템이 처리할 수 있도록 하기위한 비동기 메세징 서비스
- **시스템이 처리해야할 TO-DO List**
- 애플리케이션 간 비동기 처리를 도와줌
- 서비스가 점점 커질수록 서버 한대로는 처리가 힘들어진다.
- 자연스럽게 각 기능들을 여러 서버에서 처리하게 되면서, 서버들끼리 주고 받는 메세지를 잃어버리지 않고 - 정확하게 처리하는 것이 중요해졌다. SQS는 서버들끼리 주고받는 메세지를 정확하게 처리해준다.

요약하자면, 사용자에게 결과를 빨리 보여줘야 하는 작업과 시간이 오래 걸리는 작업을 분리할 때, 중요한 작업과 중요하지 않은 작업을 분리할때 SQS 큐를 유용하게 사용할 수 있다.

SNS(Simple Notification Service)

Active MQ

Kinesis