

클라우드 컴퓨팅

- 인터넷에서 종량 요금제 방식으로 클라우드 서비스 플랫폼을 통해 컴퓨팅 파워, 데이터베이스 스토리지, 애플리케이션, 기타 IT 리소스를 온디맨드로 제공하는 서비스

on-demand

- 사용자가 필요한 리소스를 필요한 순간에 전달할 수 있음
- 리소스가 필요하다고 미리 알릴 필요 없음
- 스토리지가 필요없어지게 된다면 반환 가능 (유연성)

장점

- 자본 비용을 가변 비용으로 대체
- 규모의 경제로 얻게 되는 이점
- 용량 추정 불필요
- 속도 및 민첩성 개선
- 데이터 센터 운영 및 유지 관리에 비용 투자 불필요
- 몇 분만에 전 지역으로 확대
- global footprint : 사용자와 가까운 위치에 데이터 저장

유형

1. IaaS

- 클라우드 IT 기본 요소 포함
- IT 리소스에 대한 최고 수준의 유연성 및 관리 제어 기능 제공

2. PaaS

- 기본 인프라 관리 필요 없음

3. SaaS

- 소프트웨어의 활용만 고려

배포 모델

1. 클라우드

- 모든 부분이 클라우드 상에서 실행
- 클라우드 내에서 생성 / 기존 인프라에서 마이그레이션

2. 하이브리드

- 클라우드 - 기존 리소스 인프라와 연결

3. 온프레미스

- = 프라이빗 클라우드
- 전용 리소스 제공

글로벌 인프라

- 리전 / AZ 중심 구축
- 리전 속 여러 AZ / AZ 속 1개 이상의 개별 데이터 센터
- AZ는 서로 격리되어 있지만 같은 리전 내에서는 지연시간이 짧은 링크로 연결됨

리전

- 디규모 그룹의 자체 데이터 센터를 구축해 재난 발생에 대비
- **비즈니스 트래픽 수요가 많은 지점** 과 가까운 곳에 리전 구축
- 컴퓨팅, 스토리지 및 기타 서비스가 포함된 데이터 센터 존재

AZ (Availability Zone)

- **단일 데이터 센터 또는 데이터 센터의 그룹**
- 예비 전원, 네트워킹을 구비한 1개 이상의 독립적인 데이터 센터 존재
- 1개 리전에서 **2개 이상** 의 가용 영역을 사용하는 것을 권장 ←
- 수십 마일 떨어져 있음 → 자연재해에 대비

보안 및 규정 준수

보안

- AWS : 클라우드 자체 보안
- 고객 : 클라우드 내 보안 (선택한 것)

혜택

- 데이터를 안전하게 유지
- 규정 준수 요구사항 충족
- 비용 절감
- 빠르게 확장

AWS 플랫폼

1. AWS Management Console
2. AWS CLI
3. AWS SDK
4. 컴퓨팅

Amazon EC2

- 클라우드에서 안전하고 규모 조절이 가능한 컴퓨팅 파워 웹 서비스
- 중지 및 종료 시 저장소의 모든 스토리지 재설정

장점

1. 탄력적인 웹 규모 컴퓨팅
2. 완전 제어
3. 유연한 클라우드 호스팅 서비스
4. 통합
5. 안정성
6. 보안
7. 비용

EC2 보안

- 지정 IP 주소 범위의 VPC에 위치
- ACL로 인바운드 / 아웃바운드 제어
- VPN연결로 기존 리소스에 연결
- 전용 인스턴스로 프로비저닝
- 고객 전용 프로비저닝

비용

1. 온디맨드 인스턴스

- 약정 없음
- 사용량에 따른 요금 지불
- 큰 규모의 고정 비용 감소
- 안전망 용량 필요 없음
- 중단 없음, 불규칙한 단기 워크로드

2. 예약 인스턴스

- 온디맨드에 비해 저렴
- 전환형은 패밀리, OS 유형, 테넌시 변경 가능
- 꾸준한 사용, 예측 가능한 워크로드에 적합

3. 스팟 인스턴스

- 예비 컴퓨팅 용량 입찰 가능
- AWS가 필요 시 인스턴스 용량 회수

4. Saving Plan

- 일정 사용량을 약정하는 대가로 저렴하게 제공
- 사용 시간 중 약정 용량만큼 할인된 비용 청구
- AWS Fargate와 AWS Lambda 에도 적용 가능

Amazon EC2 Container Service

- 도커 지원
- 클러스터 관리 / 인프라 설치 / 운영 확장

Amazon EC2 Container Registry (ECR)

- 도커 컨테이너 레지스트리
- 워크플로 간소화
- IAM과 통합하여 리포지토리를 리소스 수준에서 제어 가능
- 선수금 없음 / 전송 데이터 양만큼 요금 지불

Amazon Lightsail

- 가상 프라이빗 서버 시작, 관리
- 예측 가능한 요금으로 사용

AWS Batch

- 배치작업의 볼륨 및 리소스 요구사항에 따라 최적의 수량, 리소스를 동적으로 프로비저닝

AWS Elastic Beanstalk

- 웹 애플리케이션 / 서비스 배포, 확장 서비스
- EC2 기반 프로비저닝 지원 서비스
- 리소스에 대한 가시성, 제어 기능 유지
- 용량 조정, 로드 밸런싱, 모니터링 등

AWS Lambda

- 서버 없이 코드 실행 가능
- 사용량만큼만 비용 지불
- 트리거 감지 시 함수 자동 실행

Auto Scaling

- 가용성 유지, EC2 용량 축소 및 확장
- 수요 급증 시 자동으로 인스턴스 수 확장

컨테이너 관리 시스템

- docker 컨테이너 오케스트레이션 도구

1. ECS (Amazon Elastic Container Service)

- 컨테이너식 애플리케이션을 실행, 확장 가능한 고성능 컨테이너 관리 시스템
- **Docker** 지원 -> API 호출을 사용하여 Docker 지원 애플리케이션을 시작 및 중지 가능

2. EKS (Amazon Elastic Kubernetes Service)

- Kubernetes를 실행하는데 사용하는 완전 관리형 서비스

AWS Fargate

- 컨테이너용 서버리스 컴퓨팅 플랫폼
 - **인스턴스 관리까지** AWS에 맡길 수 있다.
 - 서버 프로비저닝 / 관리 필요 없음
-

AWS 공동 책임 모델

AWS는 사용자 환경의 일부를, 고객은 다른 부분을 책임짐

고객 : 클라우드 내부 보안

- AWS 클라우드 **내에서** 생성하고 배치하는 모든 것의 보안을 책임짐
- 보안 요구사항 관리, 액세스 권한의 부여, 관리, 해지
- 데이터 / IAM / OS / 네트워크 방화벽 구성
- 트래픽 방어 / 서버 인프라

AWS : 클라우드 자체의 보안

- AWS는 클라우드 **자체의** 보안 책임짐
- 인프라의 모든 계층에서 구성 요소 운영, 관리 및 제어 (물리적 보안 포함)
- 컴퓨팅 / 스토리지 / DB / 네트워킹
- AZ / 리전 / 엣지로케이션

물리적 인프라

- 데이터 센터의 물리적 보안
- 하드웨어 및 소프트웨어
- 인프라
- 네트워크 인프라
- 가상화 인프라

공통 책임

- 클라우드 인식 및 교육
 - 패치 관리
-

스토리지

Amazon S3

- 용량에 관계없이 데이터 저장, 검색 객체 스토리지
- 기본 스토리지, 벌크 리포지토리, 데이터 레이크, 백업, 복구, 재해 복구 대상, 서버리스 컴퓨팅 사용 가능
- 장기 클라우드 스토리지 클래스로 자동 티어링
- 파일 업로드 시 권한 설정 → 파일에 대한 표시 여부 및 액세스 제어 가능
- 고려 요소 데이터 검색 빈도 필요 데이터 가용성

기능

- 간편함
- 내구성
- 확장 가능
- 보안 (자동 암호화, IAM을 통한 버킷 정책 구성)
- 저렴한 비용 (수명 주기 정책 사용 시 데이터의 오래됨에 따라 Glacier로 자동 마이그레이션)
- 간편한 데이터 전송 (네트워크 최적화, 물리적 디스크 기반, 타사 커넥터 방식)
- 통합

1. S3 Standard

- 자주 액세스하는 데이터용으로 설계
- 최소 3개의 가용 영역에 데이터 저장
- 객체에 대한 고가용성 제공 → 웹사이트, 콘텐츠 배포, 데이터 분석 등 광범위하게 적용
- 비용이 높음

2. S3 Standard-Infrequent Access (S3 Standard-IA)

- 자주 액세스하지 않는 데이터
- S3 Standard와 유사하지만 저렴하고 검색 가격은 높음
- 자주 액세스하지 않지만 필요에 따라 고가용성이 요구되는 데이터에 이상적
- Standard와 마찬가지로 3개의 가용 영역에 데이터 저장

3. S3 One zone-Infrequent Access (S3 One Zone-IA)

- 단일 가용 영역에 데이터 저장
- S3 Standard-IA 보다 낮은 스토리지 가격
- 스토리지 비용을 절감하려는 경우 가용 영역 장애가 발생했을 때 데이터를 쉽게 재현

4. S3 Intelligent-Tiering

- 가장 저렴함
- 액세스 패턴을 알 수 없거나 자주 변화하는 데이터에 이상적
- 객체당 소량의 월별 모니터링 및 자동화 요금 부과
- 연속으로 액세스하지 않으면 자동으로 S3 Standard-IA 로 이동
- 자주 사용하지 않는 액세스 계층에 액세스하면 S3 Standard 로 이동

5. Glacier

- 데이터 보관용 으로 설계된 저비용 스토리지
- 객체를 몇 분에서 몇 시간 이내에 검색
- 고객 레코드, 이전 사진, 비디오 파일 저장

6. Glacier Deep Archive

- 보관에 이상적인 가장 저렴한 객체 스토리지 클래스
- 객체를 12시간 이내에 검색
- Glacier 보다 더 빠른 검색 가능
- 로드 시 비용 발생

AWS Storage Gateway

- 온프레미스 데이터 스토리지를 AWS에 저장
- 로컬에서 원격 접근 가능
- 하이브리드 스토리지 환경

Amazon Macie

- 민감 데이터 (개인식별 정보) 식별, 경고
- 완전 관리형 데이터 보안 및 데이터 프라이버시 서비스
- 기계 학습 및 패 일치를 활용하여 AWS에서 민감한 데이터를 검색하고 보호
- 민감한 데이터를 대규모로 자동 검색하고 데이터 보호 비용을 절감

Amazon Elastic Block Store (EBS)

- 영구적인 스토리지용, 고가용성
- 암호화는 KMS
- AZ에 자동 복사되어 장애로부터 보호
- 지연시간이 짧고 일관된 성능

AWS Global Accelerator

- 중단 상태 지속 모니터링 -> 즉시 대응 서비스
- 인터넷 트래픽 -> AWS 리전에서 실행되는 애플리케이션으로 전송
- 글로벌 엣지 로케이션 사용

기능

1. 고성능 볼륨

- SSD 또는 HDD 기반 중 선택 가능

2. 가용성

- AZ 내에서 자동 복제

3. 암호화

4. 액세스 관리

5. 스냅샷

Amazon Elastic File System(Amazon EFS)

- 네트워크 관리형 파일 시스템
- 여러 인스턴스가 EFS의 데이터에 동시 액세스 가능
- Amazon EBS 볼륨 : 가용 영역 수준의 리소스
- EC2를 EBS에 연결하려면 같은 AZ에 있어야 함 (HDD 역할)
- EFS는 필요에 따라서 확장 / 축소 가능, EBS는 그렇지 않음
- 온프레미스 서버 : AWS Direct Connect로 액세스 가능

i EBS VS EFS

EBS

- 가용 영역 내 자동 복제 -> 장애로부터 보호,고가용성 및 내구성 제공
- 단일 가용 영역 에 데이터 저장
- EC2와 EBS 모두 동일한 가용 영역에 상주 필요

EFS

- 리전별 서비스, 여러 가용 영역 에 데이터 저장
- 중복 스토리지 사용 → 파일 시스템이 위치한 리전의 모든 가용 영역에서 데이터에 액세스 가능
- 온프레미스 서버 : AWS Direct Connect로 액세스 가능

Amazon EBS 스냅샷

- 증분 백업 : 처음 백업 시 모든 데이터 복사, 이후로는 가장 최근의 스냅샷 이후 변경된 블록만 저장
- 전체백업 : 가장 최근 백업하지 않았지만 이후 변경되지 않은 데이터도 포함

Elastic block store

- 인스턴스에서 사용할 수 있는 블록 수준 스토리지 볼륨 제공 서비스

S3

- 스토리지 외 데이터레이크, 백업, 복구, 재해복구 대상, 서버리스 컴퓨팅 사용에 가장 저렴한 비용 + 무한확장
- 인스턴스에 대한 네트워크 트래픽 차단

Amazon Elastic File System

- EC2에 사용할 수 있는 파일 스토리지
- 파일 추가 / 제거 시 마다 용량이 자동 확장 / 축소
- 광범위한 워크로드와 애플리케이션에 유용

AWS Storage Gateway

- 하이브리드 스토리지
- 온프레미스와 무한한 클라우드 스토리지를 함께 이용 가능
- 마이그레이션, 버스팅, 스토리지 티어링 수반

VPC

- AWS Direct Connect에 연결할 때마다 EFS파일 시스템을 온프레미스 데센에 탑재 가능
- 리전 내 AZ에 걸쳐 있음

VPNG

- 사이트간 VPC

데이터베이스

Amazon Aurora

- MySQL, PostgreSQL과 호환되는 RDBMS

장점

1. 고성능

2. 보안

- KMS를 통해 생성, 제어하여 암호화

- 동일 클러스터의 백업, 스냅샷, 복제본도 암호화

3. 호환성

4. 확장성

5. 가용성 & 내구성

6. 완전 관리형

Amazon RDS

- 클라우드에서 관계형 DB 설정, 운영, 확장 용이
- Aurora, PostgreSQL, MySQL, MariaDB, Oracle, MS-SQL 중 선택
- 빈번한 접근에 유용함
- S/W 설치는 AWS에서 진행
- DB 이중화 : AZ 늘리기로 수행

장점

1. 관리

2. 높은 확장성

3. 가용성 & 내구성

- 다른 AZ에 동기식으로 복제

4. 보안

5. 비용 절약

- 사용한 리소스에 대해서만 비용 지불

Amazon DynamoDB

- 서버리스 데이터베이스
- 데이터 중복 저장
- SQL 사용 X, 비관계형 DB
- 유동적이고 빠른 속도로 액세스 할 때 이용
- 용량 변화에 맞춰 자동으로 크기를 조정하면서도 일관된 성능 유지
- NoSQL DB 서버

장점

1. 빠르고 일관적인 성능

2. 높은 확장성

3. 완전 관리형

4. 이벤트 중심 프로그래밍

5. 세분화된 액세스 제어

- IAM과 통합되어 조직 내 액세스 세부 제어

6. 유연성

Amazon DocumentDB

- Dynamo DB 이상의 속성이 필요한 경우 사용
- **MongoDB** 워크로드를 지원하는 문서 DB 서비스
- 콘텐츠 관리 시스템에 적합 (사용자 프로필 등)

Amazon Neptune

- 그래프 DB
- 소셜 네트워킹 및 추천 엔진에 사용
- 불변성을 요구하는 은행 또는 재무기록
- 높은 처리량, 그래픽 쿼리

Amazon QLDB (Quantum Ledger Database)

- 변경 불가능한 기록 시스템
- 속도 개선 가능

Amazon ElasticCache

- 인메모리 캐시를 배포, 운영, 조정
- NoSQL DB, 애플리케이션 부하 감소

1. Redis

- 빠른 오픈소스 인메모리 데이터 스토어 및 캐시
- 단일 노드 + 최대 15개 샤드 클러스터
- 웹 / 모바일 앱 / 게임 / 광고 / IoT

2. Memcached

- 메모리 객체 캐싱 시스템
 - 프로토콜 호환
-

마이그레이션

AWS Application Discovery Service

- 온프레미스 데센에서 실행되는 앱 + 프로파일 자동식별해 마이그레이션

AWS Database Migration Service

- DB 마이그레이션
- 이기종 간 마이그레이션 지원
- 페타바이트 규모의 데이터 통합, 분석

AWS Server Migration Service

- 에이전트 없는 서비스
- 증분식 복제 자동화, 일정 예약 및 추적

AWS Snow 패밀리 멤버

- AWS - 고객 간 최대 엑사바이트 데이터를 물리적으로 이동 하는 디바이스 모음

1. AWS Snowcone

- 작은 엣지 컴퓨팅 및 데이터 전송
- CPU 2 / RAM 4GB / STORAGE 8TB

AWS Snowball

- 페타바이트 규모의 데이터 전송 솔루션
- 데이터 보안 및 완전한 연계보관성 보장
- 데이터 보호를 위한 다중 보안 계층 사용
- 전송 작업 처리 이후 소프트웨어 삭제 수행
- 온프레미스 -> AWS로 데이터 이동

AWS Snowball Edge

- 온보드 스토리지 및 컴퓨팅 기능을 포함하는 100TB 데이터 전송 디바이스
- 전송 중 전담 인력, GPS 추적, 모니터링, 감시 등 다중 보안 계층 사용
- AWS KMS를 통해 관리됨
- EC2를 기본적으로 지원

1. Snowball Edge Storage Optimized

- 대규모 마이그레이션 / 반복 전송 워크플로 / 대용량 로컬 컴퓨팅
- **스토리지** : 블록 볼륨, S3 호환용 80TB HDD, 1TB SSD
- **컴퓨팅** : EC2 인스턴스 지원용 40개의 vCPU와 80GiB 메모리

- 오프라인에서 데이터 수집, 지정 처리 후 데이터 이동

2. Snowball Edge Compute Optimized

- 기계 학습, 풀 모션 비디오 분석, 분석 및 컴퓨팅 스택
- **스토리지** : S3 호환 객체 스토리지, EBS 호환 블록용 42TB HDD, 7.68TB NVMe SSD
- **컴퓨팅** : 52개 vCPU, 208GiB 메모리, NVIDIA Tesla V100 GPU 등

AWS Snowmobile

- 엑사바이트 규모의 데이터 전송 서비스
- 비디오, 이미지, 데센 마이그레이션
- 전송 중 보안 전담 인력, GPS 추적, 경보 모니터링, 비디오 감시 등 보안 계층 채택
- 모든 데이터는 AWS KMS를 통해 관리되고 연계보관성 보장
- **스토리지** : 100PB

네트워킹 & 콘텐츠 전송

Amazon VPC

- AWS에서 사용 가능한 가상의 **프라이빗 네트워크**
- EC2 인스턴스와 ELB 요소 배치 가능
- 프라이빗 게이트웨이, 고객 게이트웨이로 **VPC 간의 VPN** 연결 생성
- 리전 내 모든 영역에 걸칠 수 있음
- 인터넷에 액세스하지 않고 EC2 -> S3 접근
- VPC간의 VPN 연결 생성

비공개 리소스만 존재하는 VPC 접근?

가상 프라이빗 게이트웨이

- 보호된 인터넷 트래픽이 VPC로 들어오도록 허용 하는 구성 요소
- 승인된 네트워크에서 나오는 트래픽만 VPC로 들어가도록 허용

네트워크 ACL(액세스 제어 목록)

- stateless
- 서브넷 수준에서 인바운드 / 아웃바운드 트래픽을 제어하는 **가상 방화벽**
- 트래픽 허용 여부를 결정할 때 **낮은 번호의 규칙부터 순서대로 처리** 함

Amazon CloudFront

- 동영상, 웹 자산 전송하는 콘텐츠 전송 네트워크 (CDN)
- 데이터, 동영상, 애플리케이션, API를 짧은 지연 시간 으로 빠르게 전달하는 서비스

- **CDN** : Content Delivery Network - 고객과 가까운 곳에 데이터 복사본을 캐싱
- 엣지 로케이션을 통해 콘텐츠 및 웹페이지 전송 (자동 라우팅)
- AWS 서비스와 연동 지원
- 사용량만큼 요금 지불
- DDOS 방어 제공 (AWS Shield)

엣지 로케이션

- Cloud Front가 더 빠른 콘텐츠 전송을 위해 CDN 작업을 하는 사이트
- 데이터 복사 및 캐싱을 하고 나면 고객이 파일을 요청할 때 **캐시에서 파일을 검색** 해서 전달

Amazon Route 53

- DNS 웹 서비스 등록, 관리
- 사용자 요청을 EC2, Load Balancer, S3과 같은 AWS인프라와 연결
- 외부 인프라로 연결 가능
- 모니터링, 트래픽 관리, 지연시간 감소
- 서버 다운 시 다른 곳으로 라우팅

AWS Direct Connect

- 온프레미스 -> AWS로 네트워크 연결 설정
- **데이터센터 - VPC** 비공개 전용 연결 설정 서비스
- 네트워크 비용 절감, 대역폭 증가
- 가상 LAN(VLAN)을 사용하여 여러 인터페이스로 분리 가능
-> 퍼블릭 / 프라이빗 분리하며 동일한 연결을 사용해 접근 가능

Elastic Load Balancing (ELB)

- 애플리케이션 트래픽 -> EC2에 자동 배포
- 인스턴스 전체에 워크로드를 균일하게 분산하는 주요 관리형 서비스

1. Classic Load Balancer

- TCP 라우팅
- 네트워크 수준 정보에 따라 트래픽 라우팅

2. Application Load Balancer

- HTTP(S) 라우팅
- 고급 애플리케이션 수준 정보에 따라 트래픽 라우팅
- 요청 콘텐츠 포함

3. Network Load Balancer

- TCP 라우팅

개발자 도구

AWS CodeCommit

- 완전관리형 소스 제어 서비스
- 프라이빗 리포지토리 호스팅
- 소프트웨어 버전 관리

AWS CodeBuild

- 코드 컴파일 및 테스트, 패키지 생성

AWS CodeDeploy

- 코드 배포 작업 자동화

AWS CodePipeline

- 인프라 업데이트하는 통합 및 지속적 전송 서비스
- 코드 수정 시 릴리스 프레스 자동화

AWS X-Ray

- 배포된 애플리케이션 개발자 분석하고 디버그

Amazon Managed Blockchain

- 오픈소스 프레임워크 사용 → 블록체인 네트워크 생성 및 관리
- 분산형 원장 시스템

Aamazon DynamoDb Acceleration

- DynamoDB 용 메모리 캐시 → 응답 시간 향상

관리 도구

Amazon Cloudwatch

- 리소스 및 AWS 애플리케이션 로그인 이벤트 모니터링 서비스
- 지표 수집 및 추적, 로그파일 모니터링, 경보 설정, 리소스 변경 자동 대응
- 지표 모니터링, 관리 → 경보 작업 구성 웹 서비스
- 지표를 사용하여 시간 경과에 따른 처리 그래프 자동
- 임계값 상회 / 하회 → 자동으로 경보 생성

- 예상 요금 모니터링 가능

Amazon EC2 Systems Manager

- SW 인벤토리 수집, OS 패치 적용, 시스템 이미지 생성, OS 구성 자동화
- 온프레미스 데센으로 확장되는 관리 접근 방식 제공
- EC2, 온프레미스 모두 무료 관리

1. Run Command

- 일반적인 관리 작업 자동화

2. State Manager

- 방화벽과 같은 OS 구성을 일관성 있게 정의, 유지

3. 재고

- 인벤토리 정보 수집, 쿼리 수행 -> 시스템 구성 추적 및 감사

4. 유지 관리 기간

5. Patch Manager

6. 자동화

7. Paramter Store

AWS CloudFormation

- 서비스 구성 모델링 및 코드 배포
- AWS 리소스 모음 생성, 관리, 순서에 따라 예측 가능한 방식으로 프로비저닝, 업데이트
- 템플릿으로 종속성 기술 가능
- 코드로서 인프라 설명

AWS Outposts

- 대기 시간 요구 사항으로 인해 온프레미스를 유지해야 하는 워크로드를 위해 설계
- 한 자릿수 밀리초의 지연 시간이 필요한 워크로드를 실행하도록 설계된 새로운 유형의 AWS 인프라
- AWS는 온프레미스 데이터 센터 제거 + 클라이언트는 워크로드만 마이그레이션
- 하이브리드 아키텍처

AWS CloudTrail

- AWS API 호출 기록, 로그 파일 전달
- 보안 분석, 변경 추적, 규정 준수 감사 수행
- 계정 활동 기록

- 보안 그룹이 변경되었는지 확인

AWS Market place

- 클라우드에 사용할 S/W 구입
- 다른 사용자에게 솔루션 판매

CloudTrail Insight

- 비정상적인 API활동 자동 감지

AWS Trusted Advisor

- AWS **환경 검사**, **실시간 권장 사항 제시** 웹 서비스
- 비용 최적화, 성능, 보안, 내결함성, 서비스 한도 비교
- **녹색 체크** : 문제가 감지되지 않은 항목 수
- **주황 삼각형** : 권장 조사 항목 수
- **빨간색 원** : 권장 조치 수
- 오픈 액세스 권한이 설정된 보안 검사 시행

AWS Config

- 리소스 인벤토리, 구성 변경 알림 -> 보안 실현
- AWS 리소스 자동 점검, 감사
- 규정 준수 감사, 보안 분석, 리소스 변경 추적, 문제 해결 가능

AWS OpsWorks

- 구성 관리 서비스, Chef, Puppet 사용
- 서버 구성, 배포, 관리 작업

AWS Service Catalog

- AWS에서 사용 승인된 IT 서비스 카탈로그 생성, 관리

AWS Trusted Advisor

- AWS 최적화, 보안 개선 온라인 리소스
- 비용 최적화, 성능, 보안, 내결함성, 서비스 제한
- AWS 정밀조사 -> 권장사항
- AWS 분석, 권장사항 및 모방사례 제공

☰ Amazon S3 버킷 권한 상태

- AWS 루트 사용자에게 다단계(2중) 인증 활성화 여부
- 보안 그룹이 무제한 액세스 허용 구성

AWS Personal Health Dashboard

- 영향도 있는 이벤트 시 알림, 수정 지침 제공
- AWS 서비스 성능 및 가용성에 대한 맞춤형 보기 제공
- 예약된 화동에 대한 사전 알림 제공

AWS Managed Services

- AWS 인프라 지속적 관리
-

Amazon Cloud Directory

- 데이터 계층 조직할 수 있는 클라우드 기반 디렉터리 구축
- AD LDS, LDAP -> 단일 계층 구조만 지원
- 수억 개의 객체로 자동 확장, 공유 스키마 제공

AWS Certificate Manager

- SSL/TLS 인증서를 프로비저닝, 관리 배포 서비스
- AWS 리소스에 신속하게 배포, 인증서 갱신 작업 진행

AWS CloudHSM

- 클라우드 내 전용 하드웨어 보안 모듈을 사용하여 데이터 보안에 도움
- HSM 내 암호화 키 보호 가능
- CloudHSM 인스턴스에 대한 독점 및 전용 액세스 권한 제공

AWS Directory Service

- 관리형 Active Directory 활용 가능
- Group Policy, 트러스트, SSO 등 Active Directory 기본 기능 활용 가능

ACL

- 인스턴스 네트워크 트래픽 차단
- 무국적자
- 트래픽 허용 여부 결정 시 가장 낮은 번호 규칙부터 순서대로 처리

IAM

- AWS 서비스와 리소스에 대한 액세스 안전하게 관리
- 보안 요구사항에 따른 유연성 제공
- IAM 사용자, 그룹 및 역할, IAM 정책, Multi-Factor Authentication

- 무료 이용
- 권한에 따라 AWS 리소스 액세스 허용 / 거부 가능

AWS 계정 루트 사용자

루트 사용자

- 모든 AWS 서비스 및 리소스에 대한 **전체 액세스 권한** 을 가짐
- 일상 작업에는 사용 X

IAM 사용자

- AWS 서비스 및 리소스와 상호작용하는 **사람** 또는 **애플리케이션**
- (이름 + 자격 증명) 구성
- 권한을 부여받아 사용

IAM 정책

- AWS 서비스 및 리소스에 대한 권한을 허용하거나 거부하는 문서

IAM 그룹

- IAM 사용자의 모음

IAM 역할

- **임시로 권한에 액세스** 하기 위해 수입하는 자격 증명
- 이전 역할에 대한 권한을 포기하고 새 역할에 지정된 권한을 수입

IAM 사용자 관리 / 액세스 관리

- 사용자 생성 후 보안 자격 증명 할당
- 임시 보안 자격 요청 -> 작업 제어

IAM 역할 관리 / 권한 관리

- IAM에서 역할을 생성하고 맡은 개체 또는 서비스 제어 권한 관리
- 역할 엔티티 정의

연합된 사용자 관리 / 권한 관리

- 자격 증명 연동 사용 -> IAM 생성하지 않고 사내 기존 자격 증명
- AWS API 호출 및 리소스 액세스

AWS 보안의 혜택

1. 데이터를 안전하게 유지
2. 규정 준수 요구사항 충족

- 3. 비용 절감
- 4. 빠르게 확장

AWS Organizations

- 여러 계정을 통합하고 관리
- 조직 생성 시 상위 컨테이너 루트 자동 생성
- 서비스 제어 정책(SCP)→ 중앙 제어 : 개별 멤버 계정, 조직 단위 적용

조직 단위

- 정책 적용 시 지정된 권한 자동 상속
- 특정 보안 요구 사항이 있는 워크로드 / 애플리케이션 간편하게 격리

AWS Artifact

- 보안 및 규정 준수 보고서 및 일부 온라인 계약에 대한 온디맨드 액세스 를 제공하는 서비스

1. AWS artifact Agreements

- 특정 유형의 정보를 사용하기 위해 AWS와 계약 체결
- 계정에 대한 계약 검토, 수락 및 관리 가능

2. AWS Artifact Reports

- 외부 감사 기관이 작성한 규정 준수 보고서 제공 (ISO)
- 최신 상태로 유지됨

Amazon Inspector

- 자동 보안 평가 실행 → 애플리케이션 보안 및 규정 준수 개선
- EC2 인스턴스에 대한 오픈 액세스, 취약 SW 설치와 같은 보안 취약성 검사
- 배포된 앱 보안 및 규정 준수 자동 보안 평가 서비스
- 취약점 또는 모범 사례와의 차이 평가
- 평가 수행 후 보안 평가 목록 제공, 심각도 수준에 따라 우선순위 지정

AWS CloudHSM

- 클라우드 기반
- 자체 암호화 생성, 사용 하드웨어 보안 모듈

Amazon GuardDuty

- AWS 인프라 및 리소스에 대한 지능형 위협 탐지 기능 제공
- 네트워크 및 계정 활동 모니터링 - 소스 데이터 지속적으로 분석
- DynamoDB에 저장된 데이터 암호화 자동 수행

AWS Key Management Service (AWS KMS)

- 저장 시 / 전송 중 암호화
- 암호화 키를 사용하여 암호화 가능 (IAM에서 관리 가능)
- HSM으로 키 보안 유지

AWS WAF

- SQL Injection, XSS
- 웹 애플리케이션으로 들어오는 네트워크 요청을 모니터링할 수 있는 방화벽
- CloudFront, Application Load Balancer 와 함께 작동
- ACL (액세스 제어 목록) 사용
- 외부에서 SQL 인젝션 공격 완화 자동화

AWS Shield

- DDoS 보호 서비스
- 애플리케이션 가동 중지 및 지연 시간 최소화하는 상시 탐지 및 자동 인라인 통합 제공

AWS Shield Standard

- 모든 AWS 고객 자동 보호 무료 서비스 (DDOS)
- 실시간 으로 악성 트래픽을 탐지하고 완화
- 추가 비용 없이 자동 보호

AWS Shield Advanced

- 정교한 DDOS 공격 탐지 및 완화
- CloudFront, Route 53, Elastic Load Balancing 과도 통합됨
- 사용자 지정 규칙 작성 → WAF와 통합
- 리소스에서 실행되는 공격을 높은 수준에서 방어
- 공격 가시성, 방화벽과의 통합 제공
- AWS DDoS 대응 팀(DRT) 액세스 가능

VPC Flow Logs

- VPC에서 수신 / 발신하는 트래픽 정보 캡처

보안 그룹

EC2 가상 방화벽

1. stateful

- 서버측에 클라이언트, 서버 상태 정보 저장
- 세션 상태에 따라 서버 응답 변화

2. stateless

- 서버측에 클라이언트, 서버 상태 정보 저장하지 않음
 - 서버 응답이 클라이언트와 독립적
-

분석

Amazon Athena

- 표준 SQL을 사용해 S3에 저장된 데이터 분석하는 대화식 쿼리 서비스
- 비용 및 사용 보고서 데이터에서 시각적 보고서 생성 지원
- 서버리스 서비스 -> 인프라 관리하지 않음
- 1회성 쿼리를 빠르게 실행함

Amazon EMR

- 클라우드 빅데이터 플랫폼 (Elastic Map Platform) -> 분산처리 후 합침
- 동적 확장 가능 EC2 인스턴스 전반에 걸쳐 대량의 데이터를 효율적으로 처리하는 **하둡 프레임워크** 제공
- 분산 프레임워크 (Apache Spark, HBase, Presto, Flink) 실행
- 데이터 스토어의 데이터와 상호작용 가능

Amazon CloudSearch

- 검색 솔루션 효율적으로 설정 가능

Amazon Elasticsearch Service

- Elasticsearch 배포, 운영, 확장
- 분석 도구 통합 제공

Amazon Kinesis

- 스트리밍 데이터 로드 및 분석 서비스

1. Amazon Kinesis Firehose

- 스트리밍 데이터 캡처 및 변형 후 로드 -> **실시간에 가까운 분석**
- 데이터 처리량에 대응하여 자동으로 확장, 지속적 관리 필요 없음

2. Amazon Kinesis Analytics

- 표준 SQL을 통해 실시간 스트리밍 데이터 처리 가능한 가장 쉬운 방법
- 비즈니스 및 고객 요구에 신속하게 대응 가능

3. Amazon Kinesis Streams

- 특수요구에 맞는 데이터 처리 및 애플리케이션 구축 가능
- 다중 소스에서 대량의 데이터를 지속적으로 캡처 및 저장 가능
- KCL 사용하여 동적 요금 및 알림 등 작업 수행 가능
- 다른 AWS 서비스로 데이터 전달 가능

Amazon Redshift

- **빅데이터 분석**에 사용할 수 있는 **데이터 웨어하우징 서비스**
- 원본에서 데이터 수집 → 데이터 관계 및 추세 파악
- 빈번한 데이터 접근에 적합
- 컬럼 방식 스토리지, 데이터 압축 및 매핑 → 쿼리 사용의 I/O 감소
- 대량 병렬 처리 사용 → 분산하여 리소스 모두 활용

Amazon QuickSight

- AWS 비용 및 사용 **보고서(CUR)**를 수집하고 시각화
- 보고 목적으로 대시보드 사용

AWS Data Pipeline

- 지정된 간격으로 데이터를 안정적으로 처리, 이동 웹 서비스
- 정기적으로 액세스해 규모에 맞게 변형 및 처리 후 서비스로 전송

AWS Glue

- 분석을 위해 데이터 준비
- 데이터 스토어 사이에 데이터 이동하는 완전관리형 ETL 서비스
- 오래걸리는 검색, 변환 매핑 등 단순화 및 자동화
- JDBC와 호환되는 모든 데이터 스토어 연결 가능
- 서버리스 서비스, 사용량에 따라서만 지불 가능

AWS X-Ray

- 마이크로서비스 프로덕션 / 애플리케이션 분석 및 디버그 서비스
- 기본 구성 용소를 맵으로 보여줌

인공지능

- **Amazon Transcribe** - 음성 → 텍스트 변환
- **Amazon Comprehend** - 텍스트 패턴 검색, 기계학습 경험이 없는 사용자를 위한 서비스
- **Amazon Fraud Detector** - 잠재적인 온라인 사기 행위 식별
- **Amazon Lex** - 음성 및 텍스트 챗봇 빌드
- **Amazon Polly** - 텍스트 → 음성 변환 (transcribe와 반대)

- **Amazon Rekognition** - 이미지 분석 / 딥러닝 기반 시각 검색 및 이미지 분류 기능 추가 가능, 사진 객체 자동 감지

기계 학습

- **Amazon SageMaker** : 모델 빌드, 훈련, 배포

모바일 서비스

title: 기능

- 앱 분석
- 앱 콘텐츠 전송
- 클라우드 로직
- NoSQL DB
- 푸시 알림
- 사용자 데이터 스토리지
- 사용자 로그인
- 커넥터
- 대화형 봇
- 사용자 참여

Amazon Cognito

- 로그인 기능 추가 서비스
- 디바이스에 데이터 로컬 저장 - 오프라인 상태일때 동작가능
- 임시 액세스 자격증명 생성 가능

Amazon Pinpoint

- 캠페인을 생성하여 모바일 앱에서 사용자 참여 유도
- 사용자 행동 기반 푸시 알림으로 참여율 증가

AWS Device Farm

- 앱 테스트 서비스
- 상호작용 및 실시간 디바이스 문제 재현

AWS Mobile SDK

- 다양한 AWS 서비스 액세스 가능

Amazon Mobile Analytics

- 앱 사용량 및 수익 측정 가능

- S3과 Redshift로 커스텀 분석 실행 가능

애플리케이션 서비스

AWS Step Functions

- 시각적 워크플로 사용- 분산 앱 및 구성요소 조정 가능
- 구성 요소를 단계적으로 배열 및 시각화 가능한 그래픽 콘솔 제공
- 각 단계를 트리거 및 추적, 오류 발생 시 재시도

Amazon API Gateway

- API를 생성, 유지 관리 가능한 완전 관리형 서비스
- 백엔드 서비스로부터 로직 또는 기능에 액세스 가능

Amazon Elastic Transcoder

- 미디어 트랜스코딩 기능 제공

Amazon SWF

- 병렬적 / 순차적 백그라운드 작업을 빌드, 실행, 조정 가능
- 완전관리형 상태 추적기 / 작업 조정자 기능

Cloud Endure

1. 온프레미스 클라우드 재해 복구

- 데센 -> AWS 클라우드 이동

2. 리전 간 재해 복구

- 이미 AWS에 있는 경우 경제적 보호 계층 추가
- RPO, RTO 요구사항 충족

3. 클라우드 간 재해 복구

- 소스머신 자동 변환 - 워크로드 복제, 복구

메시징 및 대기열

메시징 메시지를 완충 기억 장치에 배치 밀결합된 상태를 벗어나 프로세스 개선

페이로드 메시지에 포함된 데이터

Amazon SQS (Amazon Simple Queue Service)

- 규모에 상관 없이 소프트웨어 구성 요소 간에 메시지 전송, 저장, 수신
- **다중화 내재** -> 메시지 손실이나 서비스 중단 X
- 메시지가 처리되기 전까지 배치되는 영역
- 처리 후 대기열에서 삭제
- 고처리량 / 최소 1회 처리 표준 대기열 / 1회처리 FIFO 대기열 포함

모놀리식 애플리케이션

- DB, 서버, 사용자 인터페이스, 비즈니스 로직 등이 모두 **직접 결합**된 아키텍처

마이크로 서비스

- 애플리케이션 구성요소가 소결합
- 단일 구성에 장애가 발생해도 다른 요소들은 계속 작동 (전체 장애 X)

Amazon SNS (Amazon Simple Notification Service)

- 빠르고 유연한 완전관리형 푸시 알림 서비스
- 모바일 디바이스 및 엔드포인트에 메시지 전송 가능
- 구독자 : 웹 서버, 이메일 주소, AWS 람다 함수 등

Amazon SES

- 비용 효율적인 이메일 서비스
- 최소 약정 없음 / 선불금 후 사용량 만큼 요금 지불

기업 생산성

Amazon WorkDocs

- 생산성을 개선하는 강력한 관리 제어 기능, 피드백 기능
- 완전관리형 엔터프라이즈 스토리지 및 공유 서비스

Amazon WorkMail

- 기존 데스크톱 및 모바일 이메일 클라이언트 애플리케이션 지원 이메일 및 일정 서비스
- 웹 브라우저를 통해 직접 접근 가능

Amazon Connect

- 관리자는 실시간 대화를 모니터링하고 과거 상담원 대화의 녹음을 검토 및 다운로드

Amazon Chime

- 온라인 미팅 획기적으로 변화시키는 통신 서비스

- 온라인 미팅, 전화, 채팅 등 외부 콘텐츠 공유 가능
-

데스크톱 및 앱 스트리밍

Amazon WorkSpaces

- 완전관리형 데스크톱 컴퓨팅 서비스
- 클라우드 기반 가상 데스크톱 프로비저닝, 디바이스에서 배포
- VDI에 비해 저렴함

Amazon AppStream 2.0

- 완전관리형 애플리케이션 스트리밍 서비스
 - 웹 브라우저를 실행하는 모든 디바이스로 스트리밍
-

사물인터넷

AWS IoT 플랫폼

- 디바이스 간 상호작용하는 관리형 클라우드 플랫폼

AWS Greengrass

- 로컬 컴퓨팅, 메시징, 데이터 캐싱 안전하게 실행
- 인터넷에 연결되지 않아도 Lambda, 동기화 등 통신 유지

AWS IoT 버튼

- Amazon Dash button 하드웨어 기반 프로그램 가능한 버튼
 - 디바이스별 코드 없이 웹 서비스 시작
-

게임 개발

Amazon GameLift

- 세션 기반 멀티플레이어 게임용 전용 게임 서버 배포, 운영, 확장
- 실제 사용 컴퓨팅 리소스, 대역폭 비용 지불

Amazon Lumberyard

- 무료 크로스플랫폼 3D 게임 엔진
-

AWS 요금

1. 상시 무료

- 만료되지 않음, 모든 AWS 고객에게 제공

2. 12개월 무료

- 가입날로부터 12개월 무료

3. 평가판

- 특정 서비스 활성화 날짜부터 시작

Cost Allocation tags (비용 할당 태그)

- 태깅으로 부서별 금액 조회 가능

요금 계산기

- AWS 기반 사용 사례에 대한 비용 추정 가능, 그룹별 구성

통합 결제

- 모든 AWS계정에 대한 단일 청구서
- 여러 계정을 결합하는 경우 사용량이 집계되어 모든 계정에 대해 혜택 제공
- 각 부서에 대해 보고싶은 경우

AWS 예산

- 서비스 사용, 서비스 비용 및 인스턴스 계획
- 예산 금액 초과에 대한 알림 기능

AWS Simply Monthly Calculator

- AWS 계정 없어도 서비스 예상 비용 알 수 있음

AWS 총 소유비용 (TCO) 계산기

- 온프레미스 -> AWS 이전 발생비용 확인

AWS Cost Explorer

- 발생 비용 기준 상위 5개 AWS 서비스 비용 및 사용량에 대한 기본 보고서 포함
- 시간별로 리소스 사용 확인 가능
- 사용된 항목 기준임에 주의 (과거 데이터 있어야 비용 탐색 가능)

AWS Support 플랜

1. Basic Support

- 모든 고객에게 **무료** 로 제공
- 백서, 설명서 및 지원 커뮤니티 액세스 포함
- **AWS Personal Health Dashboard** 사용 가능

2. Developer, Business 및 Enterprise Support

- 월 단위 비용 지불

2-1. Developer

- 모범 사례 지침
- 클라이언트 진단 도구
- AWS 설명 아키텍처 지원

2-2. Business

- 특정 요구 사항을 지원할 수 있는 AWS 제품, 기능 및 서비스 식별 사용 사례
- AWS Trusted Advisor 검사
- 타사 SW 제한된 지원
- 프로덕션 서비스 중단 시 지원 케이스 사용

2-3. Enterprise

- 컨설팅 애플리케이션 아키텍처 지침
- 인프라 이벤트 관리 지원 → 이벤트 기간 동안 회사가 아키텍처 및 운영 지원을 확장하는 방법에 대한 지침을 제공할 AWS 리소스
- 기술 계정 관리자

기술 지원 관리자 (TAM)

- 애플리케이션 계획, 배포, 최적화 시 TAM과 커뮤니케이션하며 아키텍처 검토

Cloud Adoption Framework

1. 비즈니스 관점

- 비즈니스 요구 사항 반영, 투자자 결과와 연계되도록 보장

역할

- 비즈니스 관리자
- 재무 관리자
- 예산 소유자

- 전략 이해당사자

2. 인력 관점

- 클라우드 채택을 성공하기 위한 조직 관리 전략 개발
- 조직 구조 역할 / 새로운 기술 및 프로세스 요구 사항 → 교육, 인력 배치, 조직 변화의 우선순위 지정

역할

- 인사 관리
- 인력 배치
- 인력 관리자

3. 거버넌스 관점

- IT전략이 비즈니스 전략에 부합하도록 조정
- 직언 기술 및 프로세스 업데이트 방법 제공

역할

- 최고 정보 책임자 (ICO)
- 프로그램 관리자
- 엔터프라이즈 아키텍트
- 비즈니스 분석가
- 포트폴리오 관리자

4. 플랫폼 관점

- 클라우드 기반 솔루션 구현 / 온프레미스 마이그레이션
- 인프라 설계, 구현 및 최적화

역할

- 최고 기술 책임자 (CTO)
- IT 관리자
- 솔루션스 아키텍트

5. 보안 관점

- 가시성, 감사 가능성, 제어 및 민첩성 보안 목표 충족

역할

- 최고 정보 보안 책임자 (CISO)
- IT 보안 관리자
- IT 보안 분석가

6. 운영 관점

- 비즈니스 이해당사자와 합의된 수준까지 IT 워크로드 구현, 실행, 사용, 운영 및 복구

역할

- IT 운영 관리자
- IT 지원 관리자

6가지 마이그레이션 전략

1. 리호스팅 (Rehosting)

- 리프트 앤 시프트 (lift and shift) - 애플리케이션 **변경 없이** 이전
- 마이그레이션 구현, 확장 → 레거시 시스템의 마이그레이션

2. 리플랫폼 (Replatforming)

- 리프트 앤 시프트 및 수정 (lift, tinker and shift)
- 클라우드 최적화 - **핵심 아키텍처 변경 X**

3. 리팩터링 (Refactoring) / 아키텍처 설계 (Re-architecting)

- 클라우드 네이티브 기능 → 애플리케이션 설계, 개발
- 기능 추가, 확장, 성능 개선의 필요성이 큰 경우

4. 재구매 (Repurchasing)

- **SaaS** 모델로 전환
- 다른 제품으로 전환

5. 유지 (Retaining)

- 소스 환경에 유지

6. 폐기 (Retiring)

- 필요하지 않은 애플리케이션 제거

AWS Well-Architected 프레임워크

- 클라우드 운영방법 이해

1. **운영 우수성** - *Operational Excellence*

- 시스템 실행, 모니터링 - 비즈니스 가치 제공 / 지속적으로 프로세스 절차 개선
- **오답** : 운영에 대한 통찰력 확보

설계 원칙

- 코드로 작업 수행
- 문서에 주석 추가
- 실패 예측
- 되돌릴 수 있는 소규모 변경 자주 수행

2. **보안성** - Security

- 위험 평가 및 완화 전략을 통해 비즈니스 가치 제공
- 정보 / 시스템 / 자산 보호
- 기록, 변화 평가 등

모범 사례

- 가능한 한 보안 모범 사례 자동화
- 모든 계층에 보안 적용
- 전송 중 / 저장 시 데이터 보호

3. **안정성** - Reliability

- 인프라 / 서비스 중단 복구
- 컴퓨팅 리소스 동적 확보, 수요 충족
- 잘못된 구성 또는 일시적 네트워크 문제와 같은 중단 완화

추가

- 복구 절차 테스트
- 수평 확장
- 장애 발생 시 자동 복구

4. **성능 효율성** - Performance Efficiency

- 컴퓨팅 리소스 효율적 사용 수요 변화와 기술 진화에 따른 효율성 유지

효율성 평가

- 실험 빈도 증가
- 서버리스 아키텍처 사용
- 배포 시스템

5. **비용 최적화** - Cost Optimization

- 가장 낮은 가격으로 비즈니스 가치 제공, 시스템 실행

추가

- 소비 모델 채택
- 비용 분석, 귀속
- 관리형 서비스 - 소유 비용 절감

6. 지속 가능성 - Sustainability

- 워크로드 실행이 환경에 미치는 영향을 최소화
-

AWS Well-Architected Framework

1. 운용 우수성

- 코드로 작업 수행
- 빈번하게 소규모로 되돌리는 변경
- 운영 절차 개선
- 장애 예측
- 장애로부터 학습

2. 보안

- 견고한 아이덴티티 기반 구현
- 트래이서빌리티 유효
- 모든 계층의 보안 적용
- 보안 학습 자동화
- 전송 중 미사용 데이터 보호
- 데이터 접근 금지
- 보안 이벤트 준비

3. 신뢰성

- 장애로부터 자동 회복
- 테스트 복구 절차
- 수평적 확장을 통한 가용성 향상
- 용량 추측 중지
- 자동화 변경 관리

4. 퍼포먼스 효율

- 선진 테크놀로지의 민주화
- 글로벌화
- 서버리스 아키텍처 사용
- 자주 실험

5. 비용 최적화

- 클라우드 재무 관리 구현
- 소비 모델 채용
- 효율성 측정
- 리프팅에 대한 비용 지출 중단
- 지출 분석 및 귀속

6. 지속성

- 활용률 극대화
- 관리 서비스 사용
- 효율적인 신규 하드웨어 / 소프트웨어 예측 및 선택
- 클라우드 워크로드의 다운스트림 영향 감소