

AWS CLOUD PRACTITIONER COURSE MATERIAL

SW Engineering Group
김영기 수석
[\(resious@gmail.com\)](mailto:resious@gmail.com)

Module 1

Amazon Web Services

- AWS ?
- 온디맨드 제공 및 클라우드 배포의 차이점 설명
- 종량과금제 요금 모델 요약

클라우드 컴퓨팅

❖ 클라우드 컴퓨팅 배포 모델

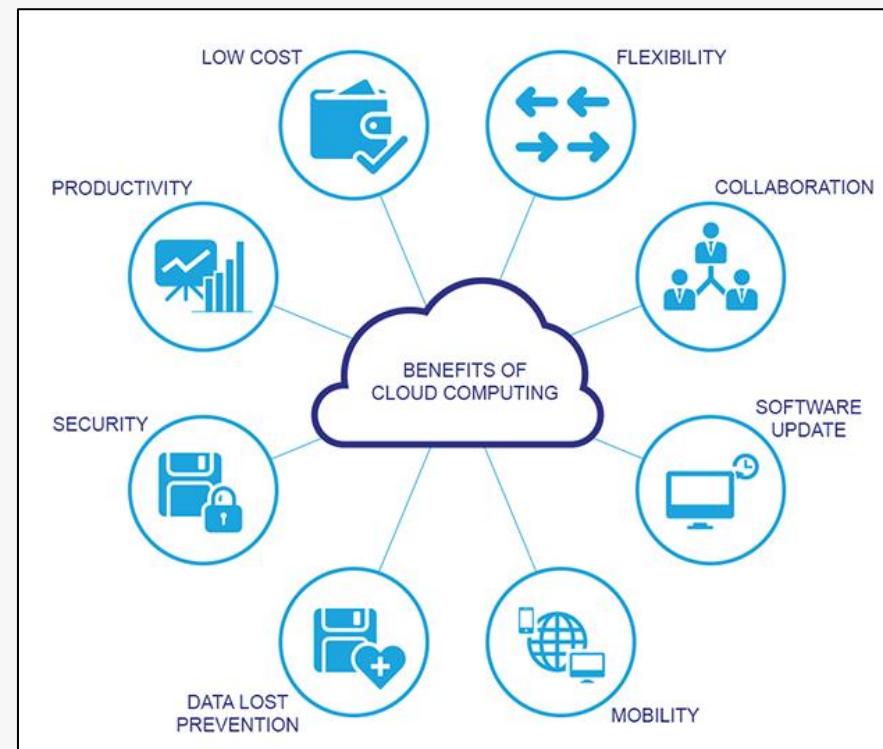
- 애플리케이션 구성 요소, 리소스 관리 도구, 레거시 IT 인프라 요구 사항 같은 요소를 고려해야 함

클라우드 기반 배포	온프레미스 배포	하이브리드 배포
<ul style="list-style-type: none">✓ 애플리케이션을 클라우드에서 실행✓ 기존 애플리케이션을 클라우드로 이전✓ 클라우드에서 애플리케이션을 설계 및 빌드✓ 하위 수준 인프라에 빌드 가능✓ 상위 수준 서비스를 사용해 빌드 가능 	<ul style="list-style-type: none">✓ 프라이빗 클라우드 배포✓ 가상화 및 리소스 관리 도구를 사용해 리소스를 온프레미스에 배포✓ 애플리케이션 관리 및 가상화 기술을 사용해 리소스 활용도를 높임✓ 레거시 IT 인프라와 매우 비슷하지만 애플리케이션 관리 및 가상화 기술이 통합 	<ul style="list-style-type: none">✓ 클라우드 리소스를 온프레미스 인프라에 연결✓ 클라우드 기반 리소스를 레거시 IT 애플리케이션과 통합✓ 온프레미스에서 더 잘 유지 관리되는 레거시 애플리케이션이 있거나 정부 규정에 따라 특정 레코드를 온프레미스에 보관하는 경우 

클라우드 컴퓨팅

❖ 클라우드 컴퓨팅의 이점

- **선행 비용을 가변 비용으로 대체**
 - ✓ 사용하는 컴퓨팅 리소스에 대해서만 비용을 지불
- **데이터 센터 운영 및 유지 관리에 비용 투자 불필요**
 - ✓ 인프라 작업에 신경을 덜 쓰고 애플리케이션과 고객에 집중
- **용량 추정 불필요**
 - ✓ 필요한 용량만 사용 가능, 수요에 따라 용량을 확장 또는 축소 가능
- **규모의 경제**
 - ✓ 인프라를 소유할 때보다 가변 비용이 낮아짐
- **속도 및 민첩성 향상**
 - ✓ 몇 분 만에 새로운 리소스에 액세스 가능 → 유연성 증가
- **몇 분 만에 전 세계에 배포 가능**
 - ✓ 신속한 배포 및 짧은 지연 시간 제공

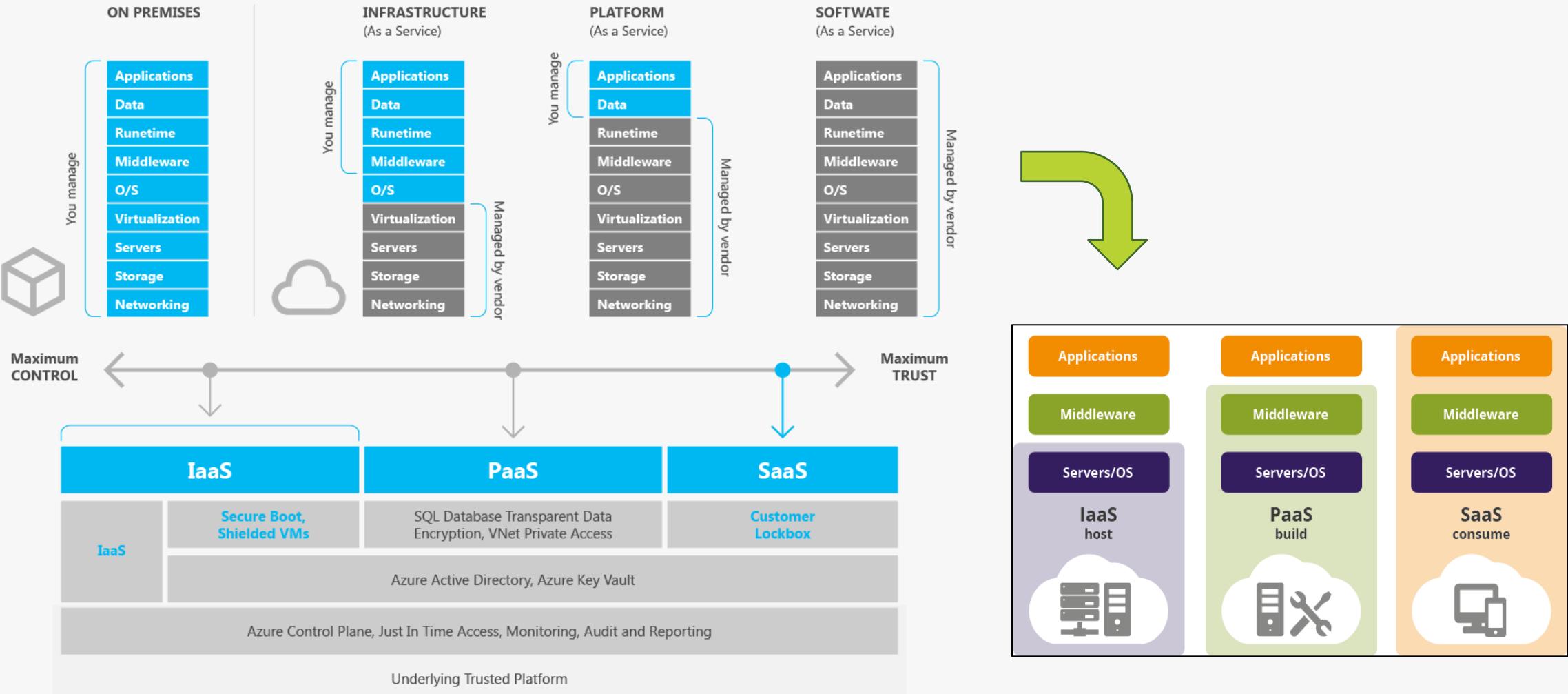


클라우드 컴퓨팅

❖ 클라우드 컴퓨팅 유형

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
<ul style="list-style-type: none">✓ IaaS에는 클라우드 IT를 위한 기본 빌딩 블록이 포함✓ 네트워킹 기능, 컴퓨터(가상 또는 전용) 및 데이터 스토리지 공간에 대한 액세스 제공✓ IT 리소스에 대한 최고 수준의 유연성과 관리 제어 기능 제공✓ 많은 IT 부서 및 개발자에게 익숙한 기존 IT 리소스와 가장 유사 	<ul style="list-style-type: none">✓ 기본 인프라 관리할 필요가 없음✓ 애플리케이션 개발과 관리에 집중 가능✓ 즉 애플리케이션 실행과 관련된 리소스 구매, 용량 계획, 소프트웨어 유지 관리, 패치 작업 또는 다른 모든 획일적인 작업에 대한 부담 없이 효율적인 운영 가능 	<ul style="list-style-type: none">✓ SaaS는 서비스 공급자에 의해 실행되고 관리되는 완전한 제품 제공✓ 대부분의 경우 SaaS는 최종 사용자 애플리케이션을 말함✓ SaaS 오퍼링의 경우 서비스 유지 관리 방법이나 기본 인프라를 관리하는 방법에 대해 생각 할 필요가 없음✓ 특정 소프트웨어의 활용 방법에 집중 

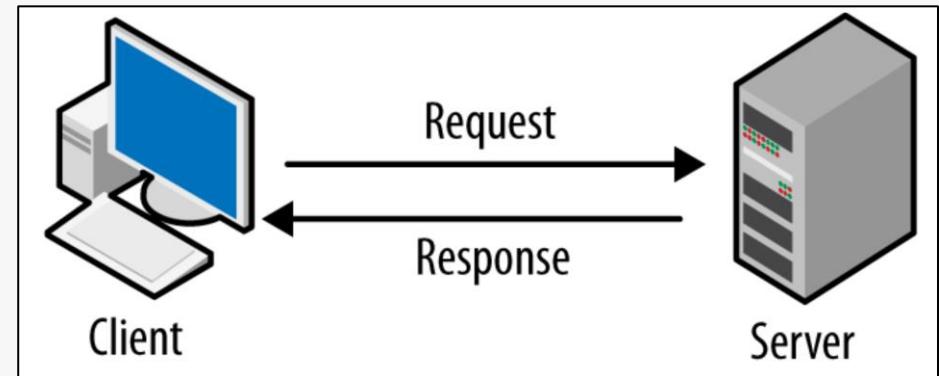
클라우드 컴퓨팅



클라이언트-서버 모델

❖ AWS

- Amazon Web Services(AWS)는 전 세계적으로 분포한 200개가 넘는 데이터 센터에서 완벽한 기능의 서비스를 제공하는, 가장 포괄적이며, 널리 채택되고 있는 클라우드 플랫폼
- AWS는 클라이언트-서버 모델을 사용
 - 클라이언트
 - ✓ 서버에 무언가를 요청
 - ✓ 웹 브라우저, 데스크톱 애플리케이션
 - 서버 :
 - ✓ 클라이언트의 요청을 평가하고 요청 정보를 반환
 - ✓ Amazon Elastic Cloud Compute (Amazon EC2)



Amazon Web Services 소개

❖ AWS

- 안정적이고 저렴한 확장형 인프라 플랫폼을 제공 장점
- 미국, 유럽, 브라질, 싱가포르, 일본 및 오스트레일리아에 데이터 센터 위치



저렴한 비용

- ✓ 사전 확약금이나 장기 약정 없이 저렴한 종량 과금제 방식

민첩성, 탄력성

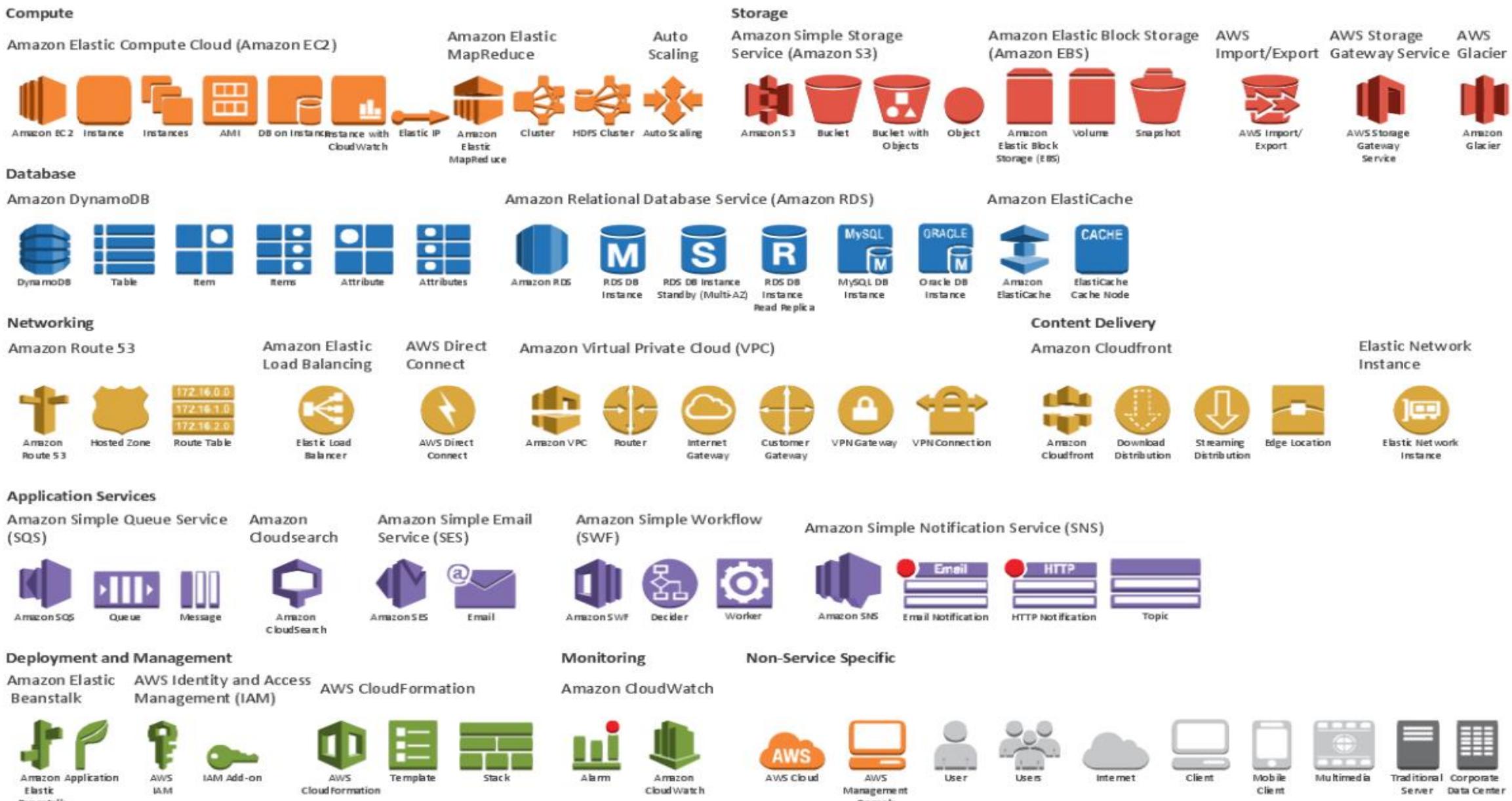
- ✓ 빠르게 혁신하고, 실험하고, 반복할 수 있는 대용량 글로벌 클라우드 인프라 제공
- ✓ 크로스d 증가에 따라 확장하고, 수요를 기준으로 축소

개방성, 유연성

- ✓ 언어 및 운영 체제에 구애 받지 않는 플랫폼
- ✓ 사용자의 비즈니스에 가장 적합한 개발 플랫폼 또는 프로그래밍 모델 선택

보안

- ✓ PCI DSS Level 1, ISO 27001 같이 업계에서 인정하는 인증 및 SOC 2 감사 보고서 등과 같은 감사 자료를 갖춘 안전하고 내구성 있는 기술 플랫폼
- ✓ 데이터의 무결성과 안전을 보장



AWS vs. Traditional

구분	아마존	기존 인프라
네트워크	Security Group VPC Route 53 Direct Connect ELB	Firewall Network DNS Dedicate Network L4 Switch
컴퓨팅	EC2	Server
스토리지	EBS S3 S3 Glacier	SSD, HDD NAS Archive
데이터베이스	RDS, Aurora DynamoDB	DBMS NoSQL

AWS 솔루션

❖ AWS에서 가장 많이 실행하는 솔루션

애플리케이션 호스팅

- 신뢰성 높은 온디맨드 인프라를 사용해 내부 호스팅 애플리케이션에서 SaaS 솔루션에 이르기까지 다양한 애플리케이션 운용

웹 사이트

- AWS의 확장형 인프라 플랫폼으로 동적인 웹 호스팅 요구 처리

백업 및 스토리지

- AWS의 저렴한 데이터 스토리지 서비스를 사용해 데이터를 저장하고 신뢰할 수 있는 백업 솔루션을 구축

엔터프라이즈 IT

- AWS의 안전한 환경에서 내부 또는 외부용 IT 애플리케이션을 호스팅

콘텐츠 전송

- 저렴한 비용과 빠른 데이터 전송 속도로 전 세계의 최종 사용자에게 콘텐츠를 빠르고 쉽게 배포

데이터베이스

- 호스팅 엔터프라이즈 데이터베이스 소프트웨어부터 비관계형 데이터베이스 솔루션까지 다양한 확장형 데이터베이스 솔루션을 활용

Module 2

클라우드 컴퓨팅

- Amazon Elastic Compute Cloud 설명
- Amazon EC2 인스턴스 유형과 Amazon EC2 결제 옵션
- Amazon EC2 Auto Scaling
- Elastic Load Balancing & 사용 예
- Amazon Simple Notification Service와 Amazon Simple Queue Service
- 추가 AWS 컴퓨팅 옵션

Amazon Elastic Compute Cloud(Amazon EC2)



- 안전하고 크기 조정이 가능한 컴퓨팅 용량을 Amazon EC2 인스턴스로 클라우드에서 제공



- Amazon EC2 작동 방식

1. 시작	2. 연결	3. 사용
<ul style="list-style-type: none">✓ 기본 구성 인스턴스가 포함된 템플릿을 선택해 인스턴스 시작<ul style="list-style-type: none">• 운영 체제, 애플리케이션 서버• 하드웨어 구성• 보안	<ul style="list-style-type: none">✓ 인스턴스에 연결<ul style="list-style-type: none">• 프로그램/애플리케이션이 인스턴스에 직접 연결• 사용자 로그인	<ul style="list-style-type: none">✓ 명령 실행<ul style="list-style-type: none">• 소프트웨어 설치• 스토리지 추가• 파일 복사 및 정리 등..

Amazon EC2 인스턴스 유형

❖ Amazon EC2 인스턴스 유형 선택 솔루션

- 워크로드 및 애플리케이션의 구체적 요구 사항을 고려
- 컴퓨팅, 메모리 또는 스토리지 기능에 대한 요구 사항이 포함

범용 인스턴스		<ul style="list-style-type: none">✓ 컴퓨팅, 메모리, 네트워킹 리소스를 균형 있게 제공✓ 어느 한 리소스 영역에 대한 최적화가 필요하지 않은 경우✓ 애플리케이션 서버, 게임 서버, 엔터프라이즈 애플리케이션 용 백엔드 서버, 중소 규모 데이터베이스
컴퓨팅 최적화 인스턴스		<ul style="list-style-type: none">✓ 고성능 프로세서를 활용하는 컴퓨팅 집약적인 애플리케이션에 적합✓ 고성능 웹 서버, 컴퓨팅 집약적 애플리케이션 서버 및 게임 전용 서버✓ 단일 그룹에서 많은 트랜잭션을 처리해야 하는 일괄 처리 워크로드
메모리 최적화 인스턴스		<ul style="list-style-type: none">✓ 많은 메모리가 필요한 워크로드✓ 메모리에서 대규모 데이터 세트를 처리하는 워크로드✓ 애플리케이션을 실행하기 전에 많은 데이터를 미리 로드해야 하는 워크로드
엑셀러레이티드 컴퓨팅 인스턴스		<ul style="list-style-type: none">✓ 하드웨어 액셀러레이터 또는 코프로세서를 사용✓ 부동 소수점 수 계산, 그래픽 처리, 데이터 패턴 일치 등✓ 그래픽 애플리케이션, 게임 스트리밍, 애플리케이션 스트리밍 등
스토리지 최적화 인스턴스		<ul style="list-style-type: none">✓ 로컬 스토리지의 대규모 데이터 세트에 대한 순차적 읽기 및 쓰기 액세스가 많이 필요한 워크로드✓ 지연 시간이 짧은 임의 IOPS를 애플리케이션에 제공하도록 설계✓ 분산 파일 시스템, 데이터 웨어하우징 애플리케이션, 고빈도 온라인 트랜잭션 처리(OLTP) 시스템 등

Amazon EC2 요금

❖ 다양한 요금 옵션

▪ 종량 과금제 기반



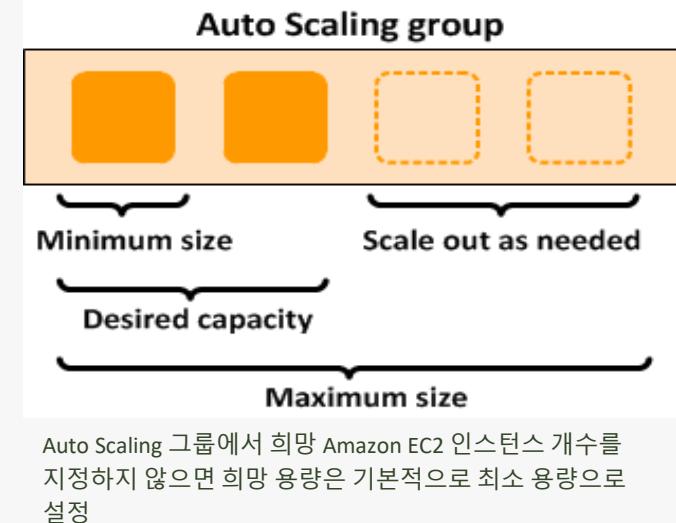
온디맨드	<ul style="list-style-type: none">✓ 중단할 수 없는 불규칙한 단기 워크로드가 있는 애플리케이션에 매우 적합✓ 애플리케이션 개발 및 테스트와 예측할 수 없는 사용 패턴이 있는 애플리케이션✓ 선결제 비용이나 최소 약정은 적용되지 않음✓ 인스턴스는 중지될 때까지 계속 실행되며, 사용한 컴퓨팅 시간에 대해서만 비용을 지불✓ 1년 이상 지속되는 워크로드에는 권장하지 않음 → 예약 인스턴스가 비용 절감 효과가 더 큼
Amazon EC2 Savings Plans	<ul style="list-style-type: none">✓ 1년 또는 3년 기간 동안 일정한 컴퓨팅 사용량을 약정하여 컴퓨팅 비용을 절감 (최대 72 %)✓ 약정 사용량까지는 할인된 Savings Plan 요금이 청구, 약정 초과 사용량은 일반 온디맨드 요금이 부과
예약 인스턴스	<ul style="list-style-type: none">✓ 계정에서 온디맨드 인스턴스를 사용할 때 적용되는 결제 할인 옵션✓ 표준 예약 및 컨버터블 예약 인스턴스는 1년 또는 3년 약정, 정기 예약 인스턴스는 1년 약정으로 구입 가능✓ 약정 기간이 끝나면 중단 없이 Amazon EC2 인스턴스를 계속 사용
스팟 인스턴스	<ul style="list-style-type: none">✓ 시작 및 종료 시간이 자유롭거나 중단을 견딜 수 있는 워크로드에 적합✓ 미사용 Amazon EC2 컴퓨팅 용량을 사용하며 온디맨드 요금의 최대 90%까지 비용을 절감✓ 필요에 따라 시작 및 중지할 수 있는 백그라운드 처리 작업(예: 고객 설문 조사 데이터 처리 작업)
전용 호스트	<ul style="list-style-type: none">✓ 사용자 전용의 Amazon EC2 인스턴스 용량을 갖춘 물리적 서버✓ 기존 소켓당, 코어당 또는 VM당 소프트웨어 라이선스를 사용하여 라이선스 규정 준수를 유지✓ 온디맨드 전용 호스트와 전용 호스트 예약 가능✓ Amazon EC2 옵션 중에서 가장 비용이 높음

Amazon EC2 확장

❖ Amazon EC2 Auto Scaling : 자동 조정 프로세스

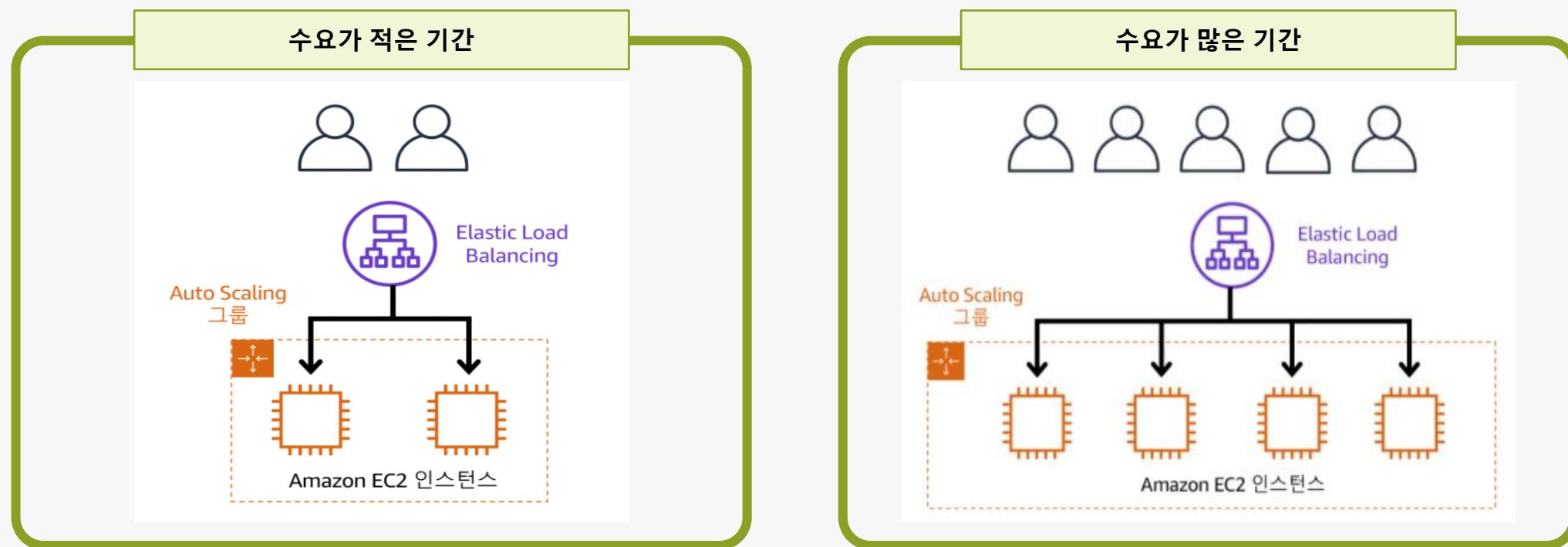
- 필요한 리소스만으로 시작하고 확장 및 축소를 통해 수요 변화에 자동으로 대응
- 접근 방식
 - 동적 조정 : 수요 변화에 대응
 - 예측 조정 : 예측된 수용에 따라 적절한 Amazon EC2 인스턴스를 자동으로 예약
- 핵심 구성 요소

Groups	<ul style="list-style-type: none">✓ EC2 인스턴스는 그룹에 정리되어 조정 및 관리 목적이 논리적 단위로 처리✓ 그룹 생성 시, EC2 인스턴스의 최소/최대/원하는 인스턴스 수를 지정
구성 템플릿	<ul style="list-style-type: none">✓ 그룹에서 시작 템플릿, 또는 시작 구성은 EC2 인스턴스의 구성 템플릿으로 사용✓ 인스턴스의 AMI ID, 인스턴스 유형, 키 페어, 보안 그룹, 블록 디바이스 매핑 등의 정보를 지정
조정 옵션	<ul style="list-style-type: none">✓ Auto Scaling 그룹을 조정하는 다양한 방법을 제공✓ 지정한 조건의 발생(동적 확장) 또는 일정에 따라 조정하도록 그룹을 구성



Elastic Load Balancing (ELB)

- Elastic Load Balancing : 애플리케이션 트래픽을 Amazon EC2 인스턴스 같은 여러 리소스에 자동으로 분산
- 로드 밸런서는 Auto Scaling 그룹으로 들어오는 모든 웹 트래픽의 단일 접점 역할
- Elastic Load Balancing과 Amazon EC2 Auto Scaling :
 - 별도의 서비스지만 서로 연동하여 EC2에서 실행되는 애플리케이션이 뛰어난 성능과 가용성을 제공하도록 함



Elastic Load Balancing (ELB)

■ 이점

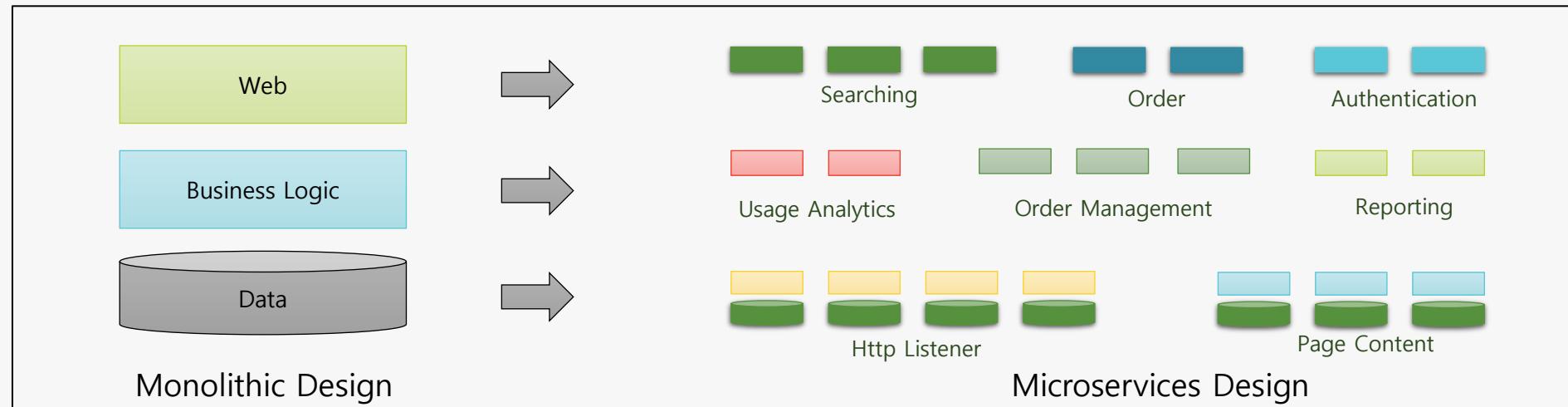
고가용성 및 탄력성	<ul style="list-style-type: none">✓ Elastic Load Balancing은 AWS 네트워크의 일부로서, AZ와 같은 장애 경계를 기본적으로 인식 → 글로벌 서버 로드 밸런싱(GSLB) 없이도 리전에서 애플리케이션을 계속 사용 가능✓ 완전관리형 서비스이므로 여러 로드 밸런서를 설치하지 않고 애플리케이션 제공에 집중✓ 용량은 기본 애플리케이션 서버의 사용률에 따라 자동으로 추가되거나 제거
보안	<ul style="list-style-type: none">✓ Amazon Virtual Private Cloud(VPC)와 연동✓ 통합 인증서 관리, 사용자 인증 및 SSL/TLS 복호화를 비롯한 강력한 보안 기능을 제공
기능 적용 범위	<ul style="list-style-type: none">✓ 규모에 관계없이 모든 비즈니스에 필요한 다양한 기능을 AWS 네이티브 환경에서 제공✓ Lambda 함수를 호출하기 위한 네이티브 HTTP 엔드포인트를 제공✓ 여러 타사 어플라이언스를 통해 송수신되는 트래픽을 라우팅하기 위한 단일 게이트웨이를 생성
강력한 모니터링 및 가시성	<ul style="list-style-type: none">✓ Amazon CloudWatch 지표, 로깅, 요청 추적을 통해 애플리케이션 상태와 성능을 실시간으로 모니터링✓ 애플리케이션 서비스 수준 계약(SLA)을 준수할 수 있도록 지원
통합 및 글로벌 접근성	<ul style="list-style-type: none">✓ 네이티브 AWS 서비스인 ELB는 EC2, ECS/EKS, Global Accelerator 및 운영 도구(예: AWS CloudFormation 및 AWS Billing) 등의 다른 AWS 서비스와 긴밀하게 통합

■ 종류

- Application Load Balancer, Network Load Balancer, Gateway Load Balancer, Classic Load Balancer

Monolith vs. Microservices

- AWS에서 애플리케이션을 설계 시 ...
 - 다양한 기능을 수행하는 서비스 및 구성 요소를 사용해 MSA 접근 방식을 취할 수 있음

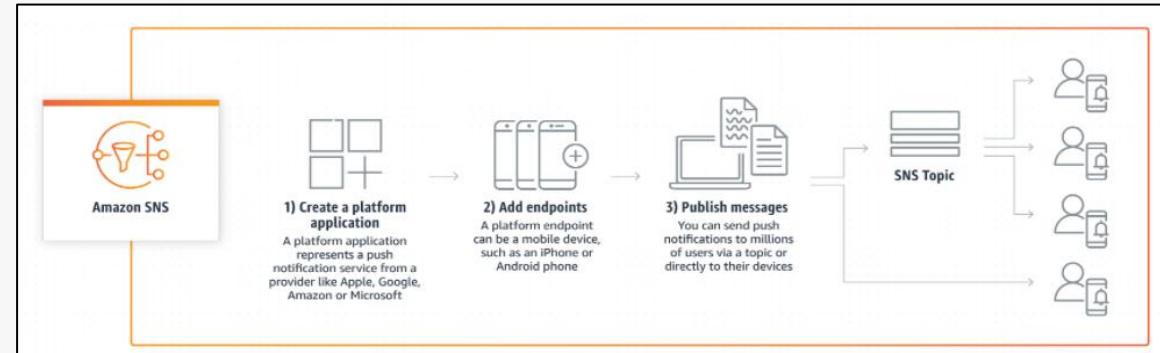
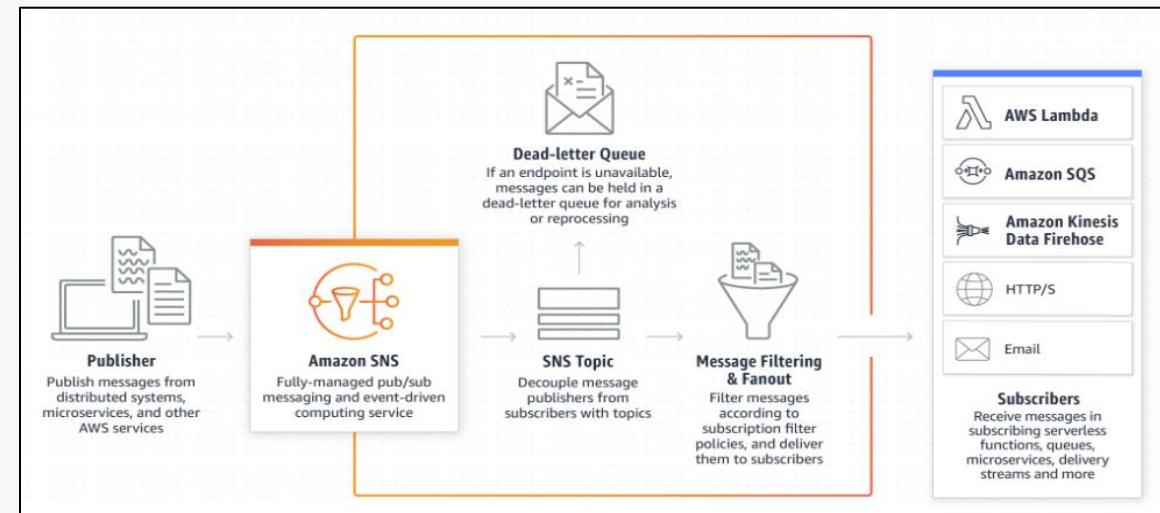


Monolithic Style	Microservices
Single Unit with all components interwoven	Applications are suite of service
Overall Scaling of the structure required	Each service independently scalable
Overall deployment	Independently deployable
Increases complexity for developers	More developer friendly
One errant component crashes the whole system	Fault diagnosis and isolation is easier
Testing is streamlined	Difficult to test

Amazon Simple Notification Service (Amazon SNS)

■ Amazon SNS

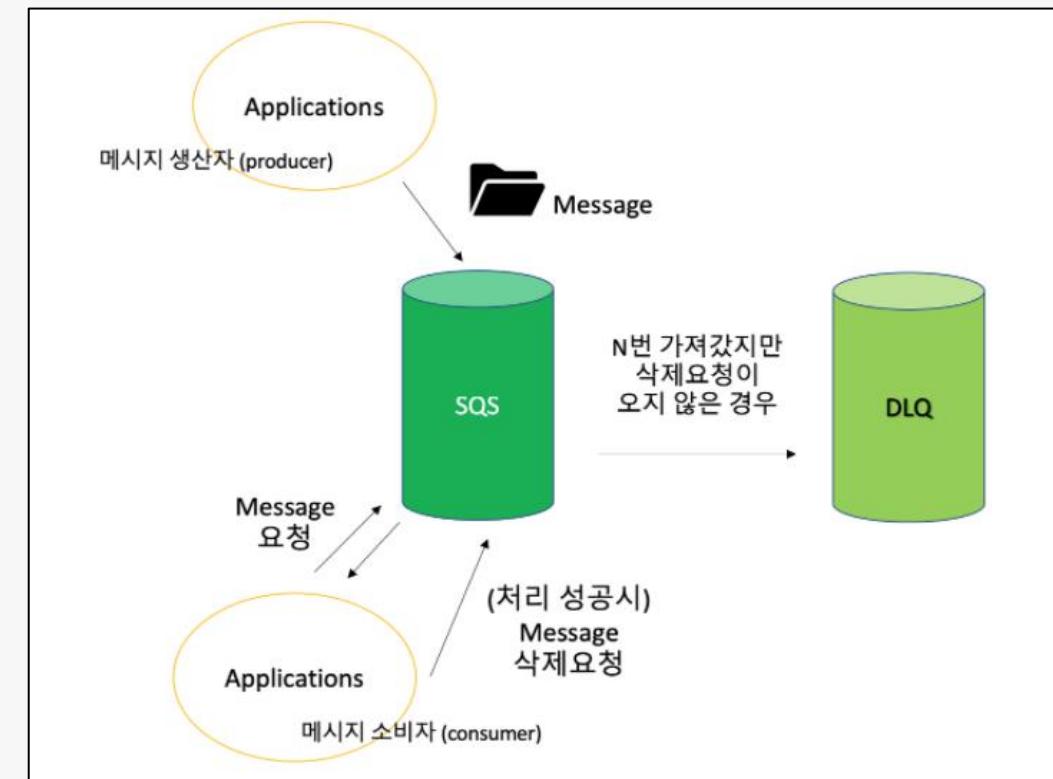
- 애플리케이션 간(A2A) 및 애플리케이션과 사용자 간(A2P) 통신을 위한 완전관리형 메시징 서비스
- 장점
 - ✓ 애플리케이션 현대화 및 분리
 - ✓ 수백만 사용자에게 직접 메시지 전송
 - ✓ 안정적인 메시지 전달
 - ✓ 워크로드 자동 확장
 - ✓ 메시지 순서 지정 및 중복 제거로 정확성 보장
 - ✓ 메시지 필터링을 통한 아키텍처 간소화



Amazon Simple Queue Service (Amazon SQS)

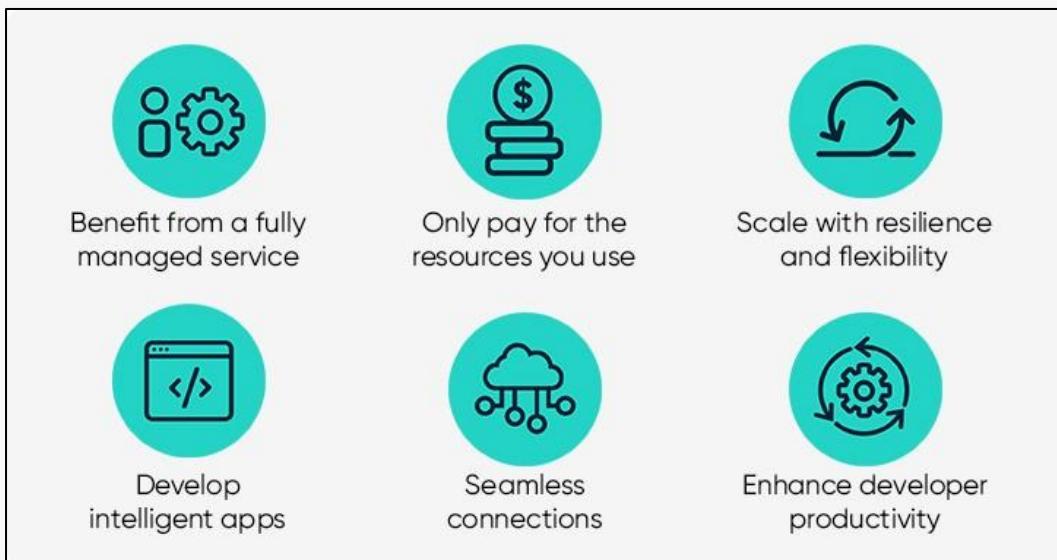
▪ Amazon SQS

- 마이크로 서비스, 분산 시스템 및 서비스 애플리케이션의 분리 및 확장을 지원하는 메시지 대기열 서비스
- SQS는 메시지 지향 미들웨어를 관리 및 운영에 따른 복잡성과 오버헤드를 제거 → 개발자가 차별화 작업에 집중
- 이점
 - 관리 오버헤드 제거
 - 안정적인 메시지 전달
 - 민감한 데이터를 안전하게 유지
 - 탄력적이고 효율적인 확장



서비스 컴퓨팅

- 코드가 서버에서 실행되지만 이러한 서버를 프로비저닝하거나 관리할 필요가 없다는 의미
 - 서버를 유지 관리하는 대신 새로운 제품과 기능을 혁신하는 데 더 집중 가능
 - 유연성
 - ✓ 서비스 애플리케이션을 자동으로 확장 가능
 - ✓ 처리량 및 메모리와 같은 소비 단위를 수정하여 애플리케이션의 용량을 조정



AWS Lambda



▪ 인프라에 대한 걱정 없이 코드 실행이 가능한 서버리스 컴퓨팅 서비스 → NoOps 실현

- 사용한 컴퓨팅 시간에 대해서만 비용을 지불
- 트리거를 이용해 애플리케이션을 자동으로 확장/축소 가능
- 모든 유형의 애플리케이션 또는 백엔드 서비스 코드를 실행 가능 : 관리 불필요
- 코드가 병렬로 실행되고 각 트리거는 개별적으로 처리되어 워크로드 규모에 맞게 조정
- AWS Lambda 작동 방식



컨테이너



- 컨테이너는 애플리케이션의 코드와 종속성을 하나의 객체로 패키징하는 표준 방식 제공
 - 보안성, 안정성, 확장성 요구 사항이 중요한 프로세스 및 워크플로에도 컨테이너 사용
- 컨테이너 오케스트레이션 서비스
 - Amazon Elastic Container Service(Amazon ECS)  **Amazon ECS**
 - ✓ AWS에서 컨테이너 애플리케이션을 실행하고 확장할 수 있는 고성능 컨테이너 관리 시스템
 - ✓ Docker 컨테이너를 지원 : Docker Community Edition 및 Docker Enterprise Edition
 - Amazon Elastic Kubernetes Service(Amazon EKS)  **Amazon EKS**
 - ✓ AWS에서 Kubernetes를 실행하는 데 사용할 수 있는 완전 관리형 서비스
 - ✓ Kubernetes 애플리케이션의 새로운 기능이 릴리스되면 Amazon EKS로 관리되는 애플리케이션에 이러한 업데이트 가능
- AWS Fargate  **AWS Fargate**
 - 컨테이너용 서버리스 컴퓨팅 엔진으로, Amazon ECS와 Amazon EKS에서 작동
 - AWS Fargate를 사용하는 경우 서버를 프로비저닝하거나 관리 불필요 : 자동으로 서버 인프라를 관리
 - 컨테이너를 실행하는 데 필요한 리소스에 대해서만 비용 지불

Module 3

글로벌 인프라 및 안정성

- AWS 글로벌 인프라
- 가용 영역
- Amazon CloudFront 및 엣지 로케이션
- AWS 서비스 프로비저닝 방법

리전

■ 말 그대로 지리적 위치

- 각 Amazon EC2 리전은 다른 Amazon EC2 리전에서 격리되도록 설계 → 내결함성 및 안정성
 - ✓ 지정한 리전에 연결된 리소스만 표시 : 여러 리전에 리소스가 자동으로 복제되지 않음
 - ✓ 인스턴스를 시작할 때 동일한 리전에 있는 AMI를 선택해야 함: 다른 리전에 있는 경우 복사 가능
 - ✓ 리전 간 데이터 전송 시 비용 청구
- 서비스 하려는 지역의 주 고객들이 거주하는 지역과 서버의 거리가 멀면 멀수록 느려짐
- 최소한 2개이상의 가용 영역(AZ)로 구성

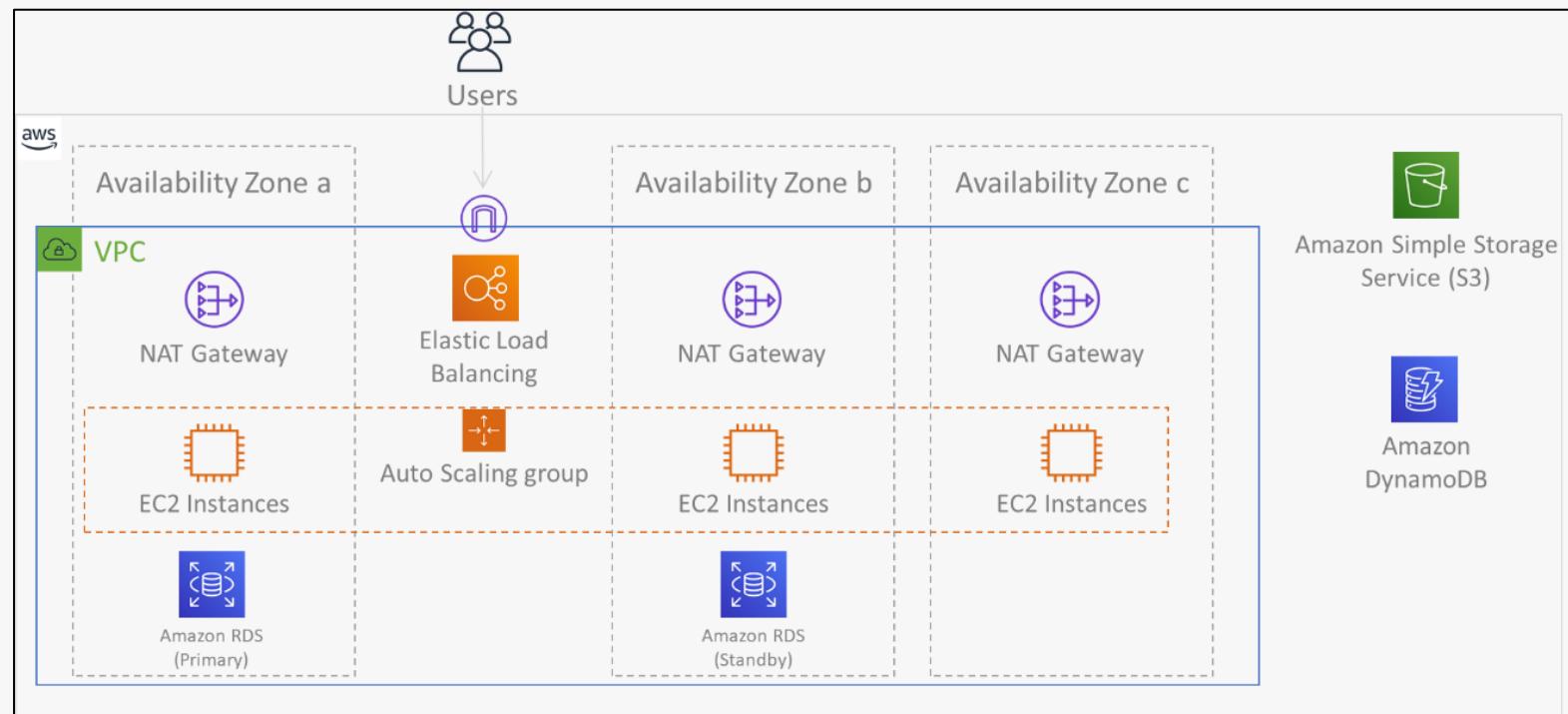


■ 리전 결정시, 고려해야 하는 비즈니스 요소

데이터 거버넌스 및 법적 요구 사항 준수	<ul style="list-style-type: none">✓ 회사와 위치에 따라 특정 영역에서 데이터를 실행해야 하는 경우✓ 모든 회사에 위치 기반 데이터 규정이 있는 것은 아니므로 다른 세 가지 요소에 더 집중해야 하는 경우 가능
고객과의 근접성	<ul style="list-style-type: none">✓ 고객과 가까운 리전을 선택하면 고객에게 콘텐츠를 더 빠르게 제공하는 데 도움
리전 내에서 사용 가능한 서비스	<ul style="list-style-type: none">✓ 경우에 따라 고객에게 제공하려는 기능이 가장 가까운 리전에 없을 수도 있음<ul style="list-style-type: none">• Ex) Amazon Braket(AWS 양자 컴퓨팅 플랫폼)
요금	<ul style="list-style-type: none">✓ 비스 비용이 리전마다 다를 수 있음

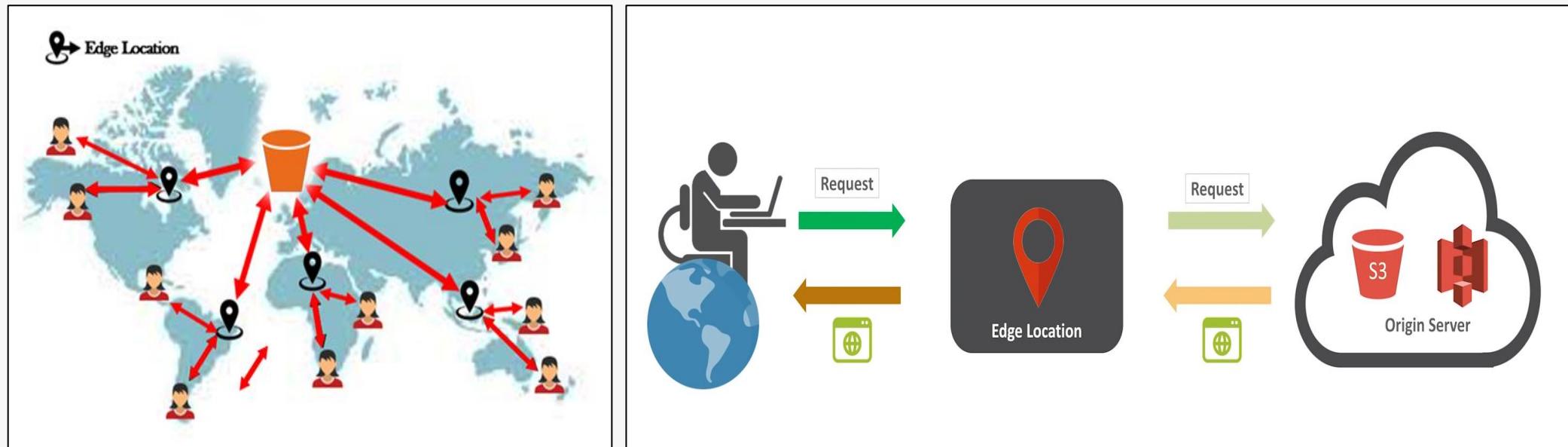
가용 영역

- AZ(가용 영역)는 AWS 리전의 중복 전력, 네트워킹 및 연결이 제공되는 하나 이상의 개별 데이터 센터로 구성
 - 단일 데이터 센터를 사용하는 것보다 더 높은 가용성, 내결함성 및 확장성을 갖고 운영 가능
 - AZ 간의 모든 트래픽은 암호화
 - AZ는 다른 모든 AZ와 수 킬로미터에 상당하는 유의미한 거리를 두고 물리적으로 분리(100km 이내)



엣지 로케이션

- AWS가 CDN 을 제공하기 위해서 만든 서비스인 CloudFront의 캐시 서버
 - CDN(Content Delivery Network)는 콘텐츠(HTML, 이미지, 동영상, 기타파일)을 사용자들이 빠르게 받을 수 있도록 전세계에 곳곳에 위치한 캐시 서버에 복제해주는 서비스
 - 짧은 지연 시간과 높은 처리량을 지원하는 안정적인 네트워크 연결



AWS 서비스와 상호 작용하는 방법 (1/2)

■ 다음 방법으로 AWS 환경 관리 가능

AWS Management Console	<ul style="list-style-type: none">✓ Amazon 서비스 액세스 및 관리를 위한 웹 기반 인터페이스✓ 최근에 사용한 서비스에 빠르게 액세스✓ 이름, 키워드 또는 약어로 서비스 검색 가능✓ 프로세스를 단순화할 수 있는 마법사 및 자동화된 워크플로가 포함✓ 여러 ID가 동시에 AWS 콘솔 모바일 앱에 로그인 가능✓ AWS 콘솔 모바일 애플리케이션을 사용해 리소스 모니터링, 경보 보기, 결제 정보 확인 등 작업을 수행 가능	
AWS 명령줄 인터페이스 (AWS CLI)	<ul style="list-style-type: none">✓ API 요청을 수행 시 시간 절약을 위해 AWS CLI 사용 가능✓ AWS CLI를 사용 시 명령줄에서 직접 여러 AWS 서비스를 제어 가능✓ 스크립트를 통해 서비스 및 애플리케이션이 수행하는 작업을 자동화 가능	
소프트웨어 개발 키트 (SDK)	<ul style="list-style-type: none">✓ 프로그래밍 언어 또는 플랫폼으로 설계된 API를 통해 AWS 서비스를 보다 간편하게 사용✓ SDK를 통해 AWS 서비스를 기준 애플리케이션과 사용 혹은 완전히 새로운 애플리케이션 생성✓ AWS는 지원되는 각 프로그래밍 언어에 대한 설명서와 샘플 코드를 제공✓ 지원되는 프로그래밍 언어 : C++, 자바, .NET 등	

AWS 서비스와 상호 작용하는 방법 (2/2)

AWS Elastic Beanstalk



- ✓ Amazon EC2 기반 환경 프로비저닝을 지원하는 서비스
- ✓ AWS Elastic Beanstalk에 애플리케이션 코드와 원하는 구성을 제공하면 이 정보를 바탕으로 환경 구축
- ✓ 사용자가 코드 및 구성 설정을 제공하면 Elastic Beanstalk이 다음 작업을 수행하는 데 필요한 리소스를 배포
 - 용량 조정
 - 로드 밸런싱
 - 자동 조정
 - 애플리케이션 상태 모니터링

AWS CloudFormation



- ✓ 인프라를 코드로 취급
 - AWS Management Console을 사용해 개별 리소스를 프로비저닝하는 대신 코드를 작성해 환경 구축
 - 리소스를 안전하고 반복 가능한 방식으로 프로비저닝
- ✓ 수작업을 수행하거나 사용자 지정 스크립트를 작성할 필요 없이 인프라 및 애플리케이션을 빈번하게 구축
- ✓ 이 서비스는 스택을 관리 시, 수행 할 적절한 작업을 결정하고 오류를 감지하면 변경 사항을 자동 롤백

- Cf) AWS Outposts :

- 하이브리드 환경을 위해 온프레미스에서 AWS 인프라 및 서비스 실행
- 로컬 시스템과 상호 종속된 애플리케이션 마이그레이션이 필요한 워크로드에 이상적



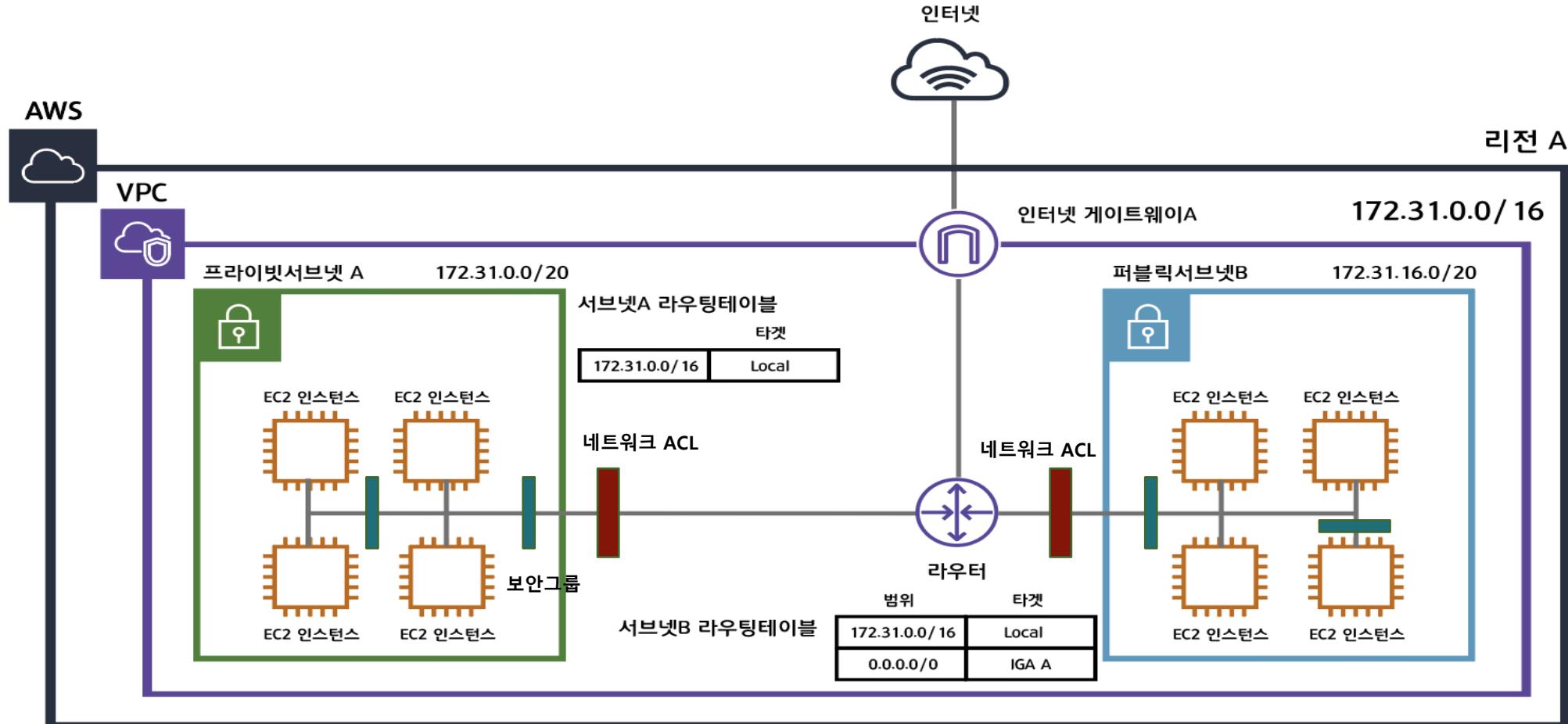
AWS Outposts

Module 4

네트워킹

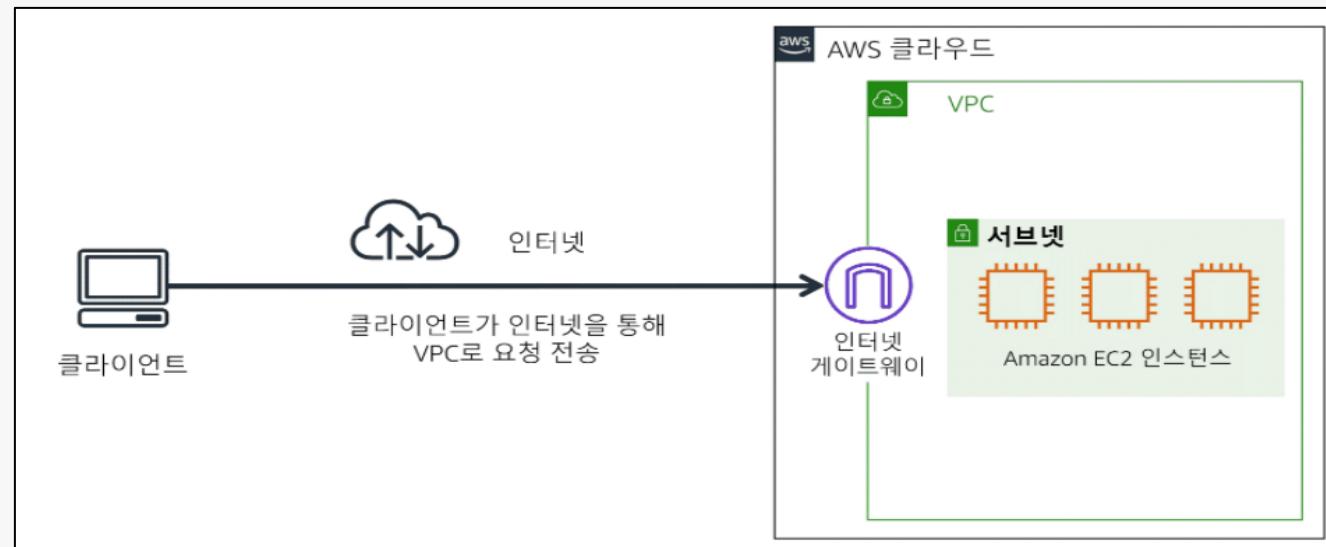
- AWS의 이점 요약
- 온디맨드 제공 및 클라우드 배포의 차이점 설명
- 종량 과금제 요금 모델 요약

Amazon VPC Example



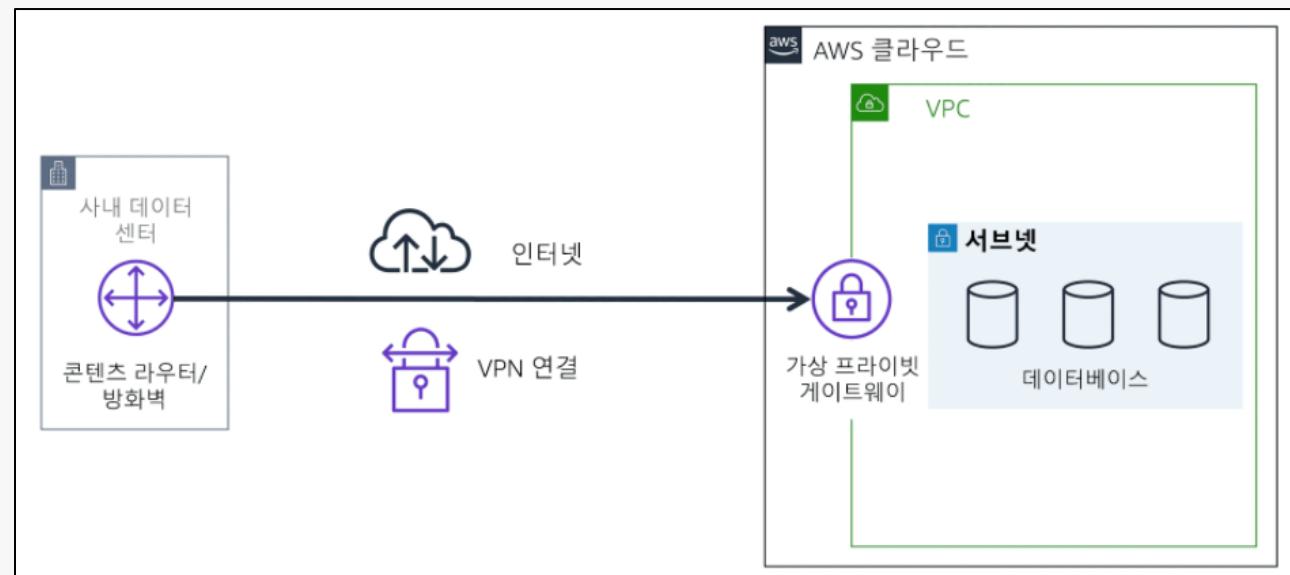
인터넷 게이트웨이

- 인터넷 게이트웨이는 VPC와 인터넷 간의 연결
 - 인터넷의 퍼블릭 트래픽이 VPC에 접근하려면 인터넷 게이트웨이를 VPC에 연결
 - 수평 확장되고 가용성이 높은 중복 VPC 구성 요소
 - IPv4와 IPv6 트래픽 지원
 - 인터넷 라우팅 가능 트래픽에 대한 VPC 라우팅 테이블에 대상 제공
 - 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 NAT(네트워크 주소 변환) 수행



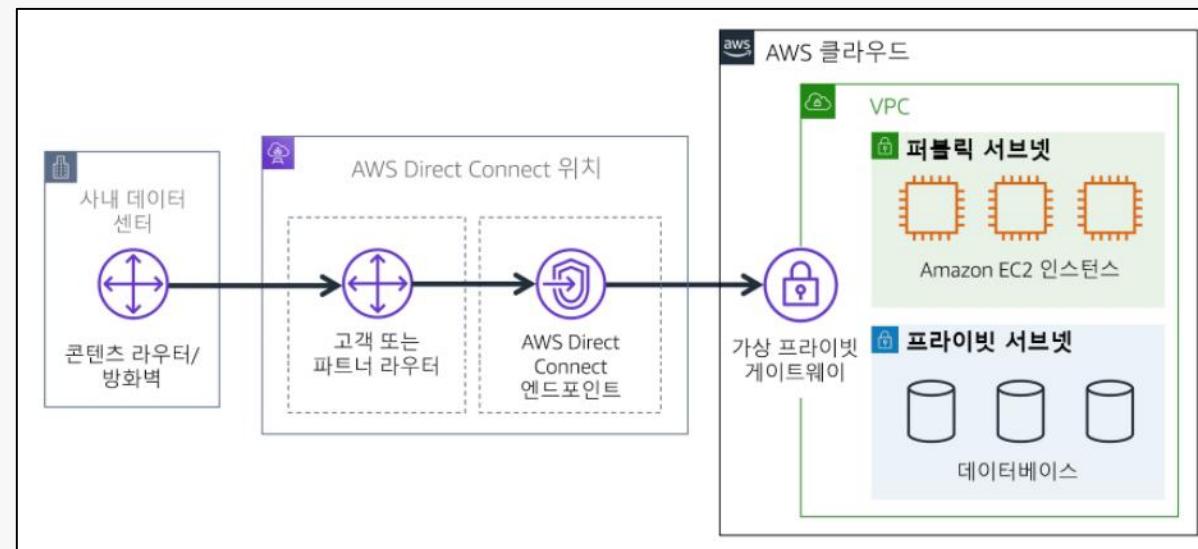
가상 프라이빗 게이트웨이

- 인터넷 VPC 내의 비공개 리소스에 액세스 → 가상 프라이빗 게이트웨이
 - 가상 프라이빗 게이트웨이는 보호된 인터넷 트래픽이 VPC로 들어오도록 허용
 - VPC와 프라이빗 네트워크(예: 온프레미스 데이터 센터 또는 회사 내부 네트워크) 사이의 가상 프라이빗 네트워크(VPN) 연결을 설정 가능



AWS Direct Connect

- 온프레미스에서 AWS로 전용 네트워크 연결을 쉽게 설정할 수 있는 클라우드 서비스
 - AWS와 고객의 데이터 센터, 사무실 또는 코로케이션 환경 간에 프라이빗 연결을 설정
 - 데이터 센터와 VPC 간에 비공개 전용 연결을 설정하는 서비스
 - 일반 인터넷망이나 VPN망에 비해 안정적인 성능을 제공할 수 있으며 보안적으로도 우수
 - 네트워크 비용을 절감하고 네트워크를 통과할 수 있는 대역폭을 늘리는 데 도움
 - 별도의 SLA는 제공하지 않음



서브넷 (Subnet)

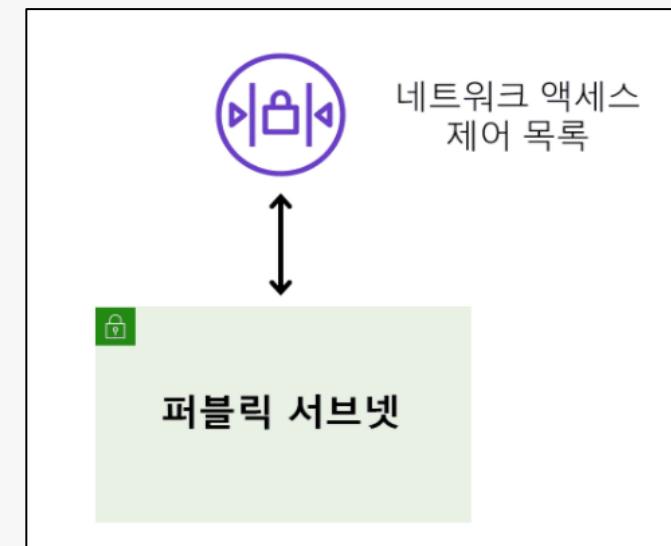
- 서브넷은 보안 또는 운영 요구 사항에 따라 리소스를 그룹화할 수 있는 VPC 내의 한 섹션
 - 퍼블릭 서브넷 : 누구나 액세스할 수 있어야 하는 리소스 포함
 - 프라이빗 서브넷 : 프라이빗 네트워크를 통해서만 액세스할 수 있는 리소스 포함
- VPC 내에서 서브넷은 서로 통신 가능
- VPC의 네트워크 트래픽
 - I. 고객이 AWS App에 데이터를 요청하면, 요청은 패킷으로 전송
 - II. 패킷은 인터넷 게이트웨이를 통해 VPC로 들어감
 - III. 패킷이 서브넷에 IN/OUT 시 권한 체크

✓ 서브넷의 패킷 권한 확인 : 네트워크 ACL(액세스 제어 목록)



네트워크 ACL(액세스 제어 목록)

- 서브넷 수준에서 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽
 - 각 AWS 계정에는 기본 네트워크 ACL이 포함
 - VPC를 구성할 때 계정의 기본 네트워크 ACL을 사용하거나 사용자 지정 네트워크 ACL을 생성 가능
 - 계정의 기본 네트워크 ACL은 기본적으로 모든 인바운드 및 아웃바운드 트래픽을 허용 : 사용자가 규칙 추가 가능
 - 사용자 지정 네트워크 ACL은 사용자가 허용할 트래픽을 지정하는 규칙을 추가 시까지 모든 트래픽을 거부
 - 모든 네트워크 ACL에는 명시적 거부 규칙이 있으며, 패킷이 목록의 다른 모든 규칙과 일치하지 않으면 해당 패킷 거부
- 상태 비저장 패킷 필터링
 - 네트워크 ACL은 상태 비저장 패킷 필터링 수행
 - 서브넷 경계를 통과하는 패킷만 확인
 - 규칙 목록에 따라 패킷 응답을 확인하여 허용 또는 거부 여부를 결정



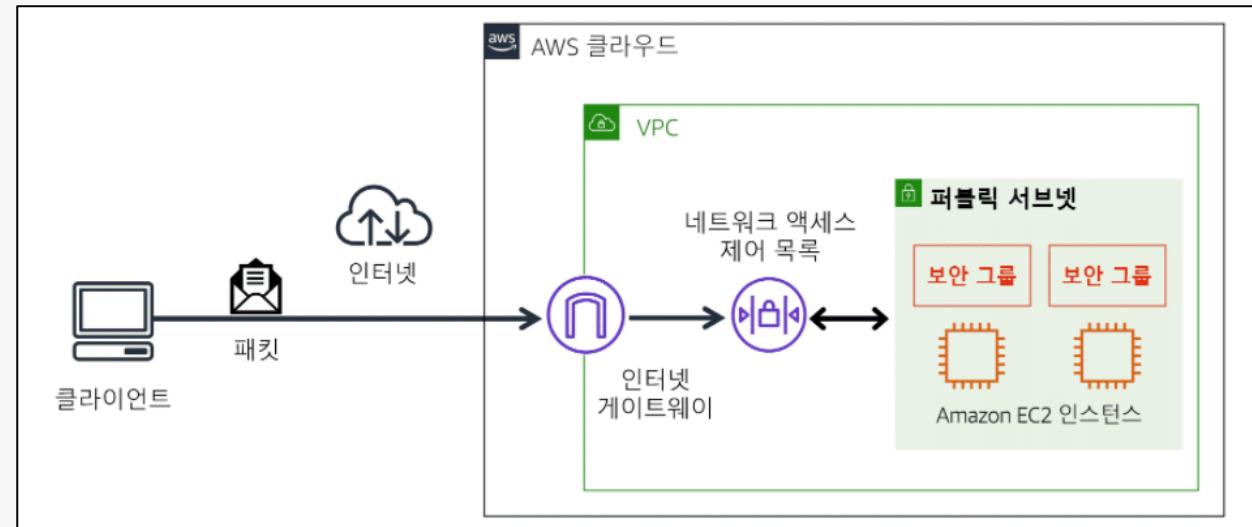
보안 그룹

- 보안 그룹은 Amazon EC2 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽
 - 패킷이 서브넷에 들어간 후에는 서브넷 내의 리소스(예: Amazon EC2 인스턴스)에 대한 권한이 평가 필요
 - 기본적으로 보안 그룹은 모든 인바운드 트래픽을 거부하고 모든 아웃바운드 트래픽 허용
 - 사용자 지정 규칙을 추가하여 허용 또는 거부할 트래픽 구성 가능
 - 서브넷 내에 여러 EC2 인스턴스가 있는 경우 : (1) 동일한 보안 그룹에 연결 OR (2) 인스턴스마다 다른 보안 그룹 사용

- 비저장 패킷 필터링

- 보안 그룹은 상태 저장 패킷 필터링을 수행
- 들어오는 패킷에 대한 이전 결정을 기억
- 인바운드 보안 그룹 규칙에 관계없이

응답이 진행하도록 허용



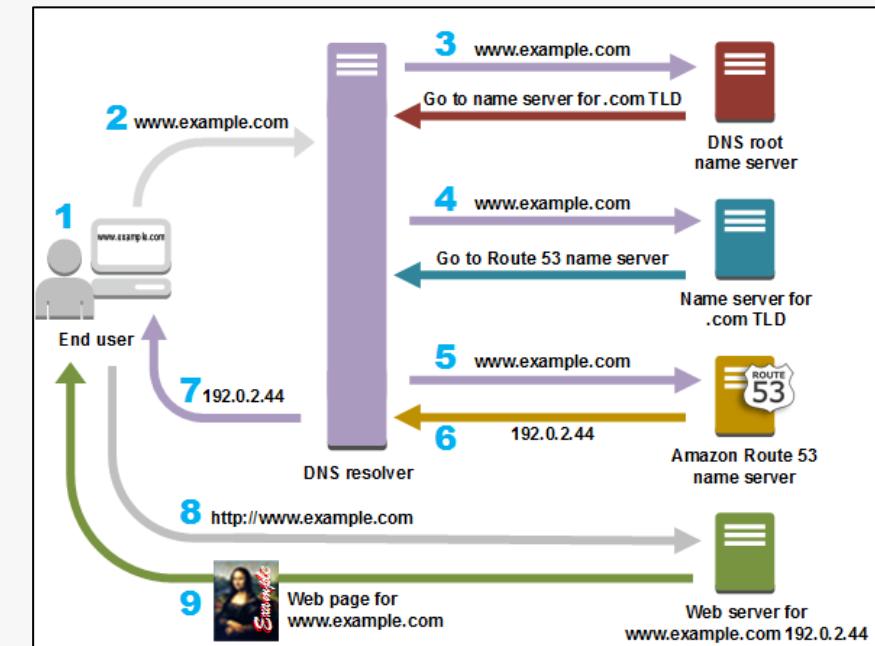
글로벌 네트워킹

▪ Domain Name System(DNS)

- 사람이 읽을 수 있는 도메인 이름(예: www.amazon.com)을 머신이 읽을 수 있는 IP 주소(예: 192.0.2.44)로 변환

▪ Amazon Route 53

- 높은 가용성과 확장성이 뛰어난 클라우드 Domain Name System (DNS) 웹 서비스
- 사용자 요청을 AWS에서 실행되는 인프라에 연결
- 사용자를 AWS 외부의 인프라로 라우팅 가능
- 도메인 이름의 DNS 레코드 관리
 - ✓ Route 53에 직접 새 도메인 이름 등록 가능
- 다른 도메인 등록 대행자가 관리하는 기존 DNS 레코드 전송 가능
 - ✓ 단일 위치에서 모든 도메인 이름 관리



Module 5

스토리지 및 데이터베이스

- 스토리지 및 데이터베이스 개념
- Amazon Elastic Block Store
- Amazon Simple Storage Service
- Amazon Elastic File System
- 스토리지 솔루션
- Amazon Relational Database Service & Amazon DynamoDB

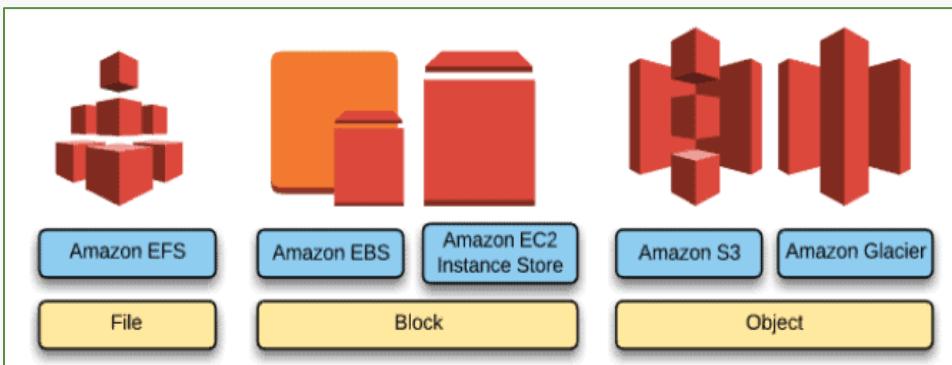
AWS EC2 Storages

▪ Storage

- 컴퓨터에 데이터를 저장하는 저장소 역할을 수행하는 부품 : 컴퓨터의 하드디스크와 동일한 역할
- 스토리지를 서버에 직접 연결하거나 대용량 데이터 저장을 위해 별도의 스토리지용 네트워크 구성 가능
 - ✓ DAS (Direct Attached Storage), NAS (Network Attached Storage), SAN (Storage Area Network)

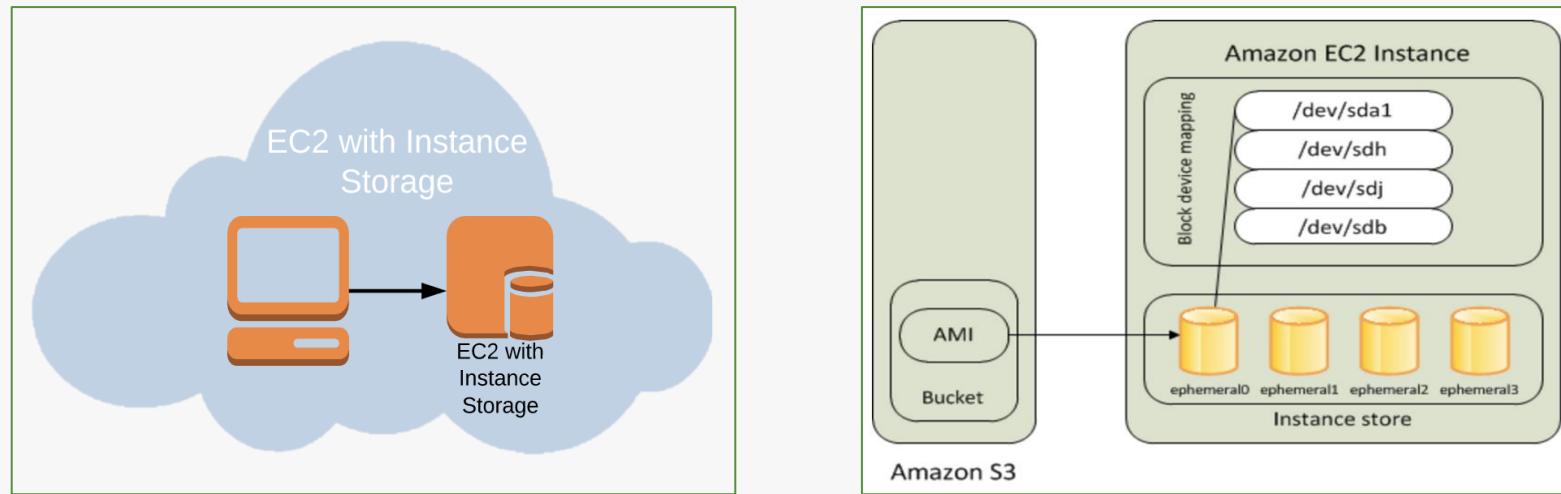
▪ AWS Cloud Storage

- Cloud computing의 중요 구성 요소로 애플리케이션에서 사용하는 정보를 보관
 - ✓ 일정 형태의 data storage architecture가 필요
- AWS에서는 모든 범위의 cloud storage service를 제공하여 application과 archive 규정 준수 요구 사항을 모두 지원
- Object, file, block storage service와 cloud data migration option을 선택해 Cloud IT environment의 기초 설계 가능



Instance Store

- 블록 수준 스토리지 볼륨은 물리적 하드 드라이브처럼 동작
 - 인스턴스 스토어는 물리적으로 EC2 인스턴스의 호스트 컴퓨터에 연결
 - ✓ EBS보다 빠름 : 빠른 속도와 보장된 속도를 요구하는 경우, 소규모 데이터 캐싱에 사용
 - 인스턴스와 수명이 동일한 디스크 스토리지
 - ✓ 인스턴스가 종료되면 인스턴스 스토어의 데이터가 손실
 - ✓ 버퍼, 캐시, 스크래치 데이터 및 기타 임시 컨텐츠와 같이 자주 변경되는 정보의 임시 스토리지
 - ✓ 로드가 분산된 웹 서버 풀과 같은 여러 인스턴스 상에서 복제되는 데이터에 가장 적합



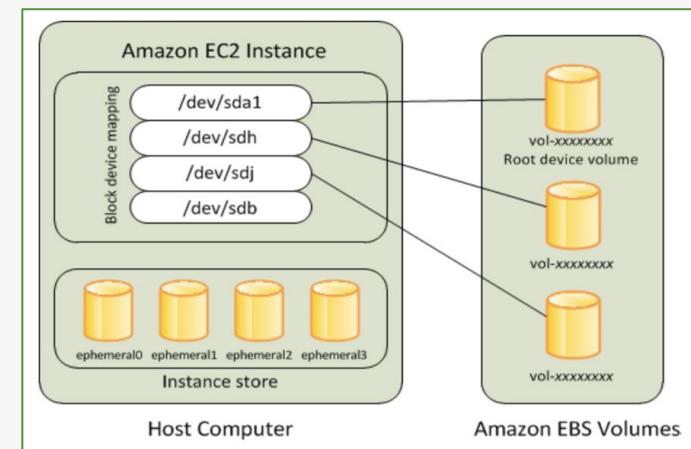
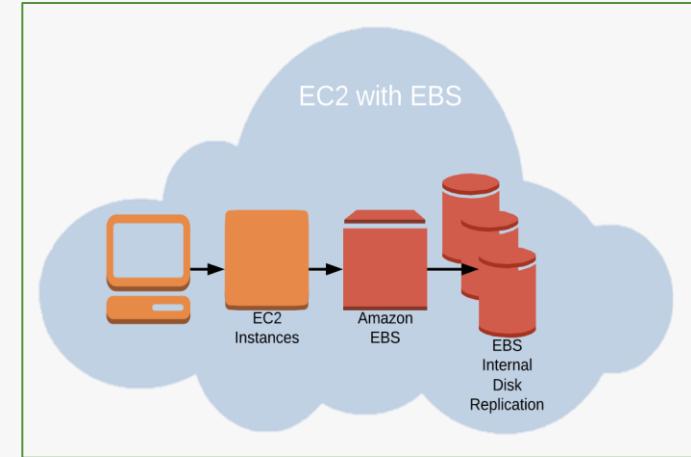
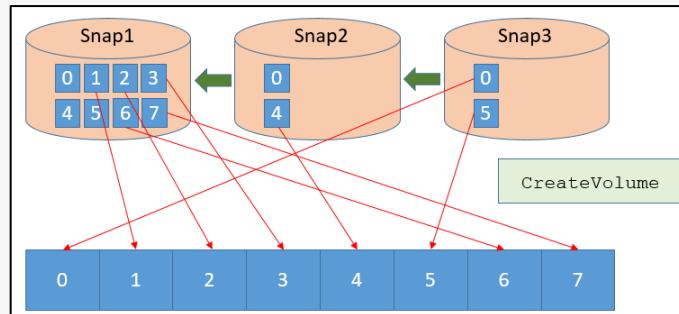
Amazon Elastic Block Store(Amazon EBS)

- Amazon EC2 인스턴스에서 사용할 수 있는 블록 수준 스토리지 볼륨을 제공하는 서비스

- EC2 인스턴스를 중지/종료하더라도 연결된 EBS 볼륨의 모든 데이터를 사용 가능
- EBS 볼륨을 생성하려면 구성(예: 볼륨 크기 및 유형)을 정의하고 볼륨을 프로비저닝
 - ✓ EBS 볼륨을 생성한 다음 볼륨을 Amazon EC2 인스턴스에 연결 가능
- EBS 볼륨은 보존해야 하는 데이터를 위한 것이므로 데이터 백업이 중요
 - ✓ Amazon EBS 스냅샷을 생성하여 EBS 볼륨을 증분 백업

- Amazon EBS 스냅샷

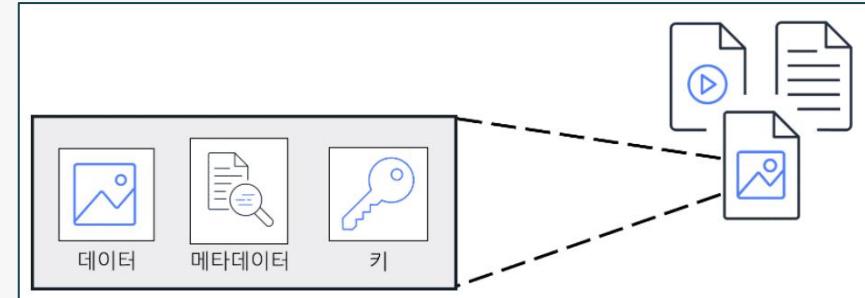
- 증분 백업
 - ✓ 처음 볼륨을 백업하면 모든 데이터가 복사
 - ✓ 이후의 백업에서는 가장 최근의 스냅샷 이후 변경된 데이터 블록만 저장



Amazon Simple Storage Service (Amazon S3)

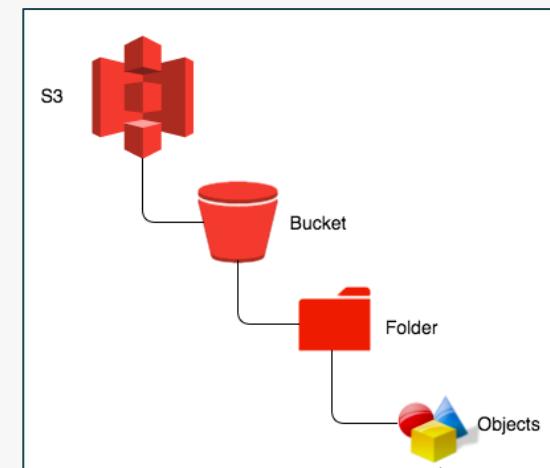
■ 객체 스토리지

- 객체 스토리지에서 각 객체는 데이터, 메타데이터, 키로 구성
 - ✓ 데이터는 이미지, 동영상, 텍스트 문서 또는 기타 유형의 파일
 - ✓ 메타데이터에는 데이터의 내용, 사용 방법, 크기 등에 대한 정보 포함
 - ✓ 객체의 키는 고유한 식별자
- 블록 스토리지에서 파일을 수정하면 변경된 부분만 업데이트
- 객체 스토리지에서 파일을 수정하면 전체 객체가 업데이트



■ Amazon S3

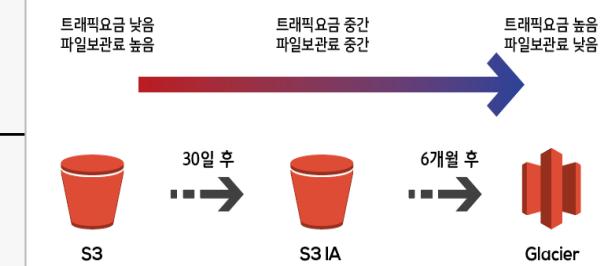
- 객체 수준 스토리지를 제공하는 서비스 : 데이터를 버킷에 객체로 저장
- 이미지, 동영상, 텍스트 파일 등 모든 유형의 파일을 업로드 가능
 - ✓ Amazon S3는 저장 공간을 무제한으로 제공
 - ✓ Amazon S3에 저장할 수 있는 객체의 최대 파일 크기 : 5TB
- 파일 업로드 시, 권한을 설정하여 파일 표시 여부 및 액세스 제어 가능
- Amazon S3 버전 관리 기능을 사용해 시간 경과에 따른 객체 변경사항 추적 가능



Amazon Simple Storage Service (Amazon S3)

- 스토리지 클래스 선택 시 고려 사항 : 데이터 검색 빈도와 요구되는 데이터 가용성

S3 Standard		<ul style="list-style-type: none">✓ 자주 액세스하는 데이터용으로 설계 : 객체에 대한 고가용성 제공✓ 최소 3개의 가용 영역에 데이터를 저장✓ 자주 액세스하지 않는 데이터 및 보관 스토리지를 위한 다른 스토리지 클래스보다 높은 비용
S3 Standard-Infrequent Access (S3 Standard-IA)		<ul style="list-style-type: none">✓ 자주 액세스하지 않지만 고가용성이 요구되는 데이터에 이상적✓ S3 Standard와 비슷하지만 스토리지 가격은 더 저렴하고 검색 가격은 더 높음✓ 최소 3개의 가용 영역에 데이터를 저장
S3 One Zone-Infrequent Access (S3 One Zone-IA)		<ul style="list-style-type: none">✓ 단일 가용 영역에 데이터를 저장 : AZ 장애 발생 시, 데이터를 손쉽게 재현할 수 있는 경우✓ S3 Standard-IA보다 낮은 스토리지 가격 : 스토리지 비용 절감
S3 Intelligent-Tiering		<ul style="list-style-type: none">✓ 액세스 패턴을 알 수 없거나 자주 변화하는 데이터에 이상적✓ 객체당 소량의 월별 모니터링 및 자동화 요금을 부과✓ 30일 연속 객체에 액세스하지 않으면, S3 Standard-IA로 이동
S3 Glacier		<ul style="list-style-type: none">✓ 데이터 보관용으로 설계된 저비용 스토리지✓ 객체를 몇 분에서 몇 시간 이내에 검색
S3 Glacier Deep Archive		<ul style="list-style-type: none">✓ 보관에 이상적인 가장 저렴한 객체 스토리지 클래스✓ 객체를 12시간 이내에 검색



Amazon Elastic File System(Amazon EFS)

- 파일 스토리지에서는 여러 클라이언트가 공유 파일 폴더에 저장된 데이터에 액세스 가능
 - 이 방식에서는 스토리지 서버가 블록 스토리지를 로컬 파일 시스템과 함께 사용하여 파일 구성
 - 클라이언트는 파일 경로를 통해 데이터에 액세스
 - 블록 스토리지 및 객체 스토리지와 비교해, 많은 수의 서비스 및 리소스가 동시에 같은 데이터에 액세스해야 하는 경우 이상적
- AWS 클라우드 서비스 및 온프레미스 리소스와 함께 사용되는 확장 가능한 파일 시스템
 - 파일을 추가 또는 제거하면 Amazon EFS가 자동으로 확장/축소
 - 애플리케이션을 중단하지 않고 온디맨드로 페타바이트 규모로 확장

Amazon EBS	Amazon EFS
<ul style="list-style-type: none">단일 가용 영역에 데이터 저장EC2와 EBS 볼륨이 같은 AZ에 상주해야 함	<ul style="list-style-type: none">리전별 서비스 : 여러 AZ에 걸쳐 데이터 저장중복 스토리지 사용 시, 파일 시스템이 위치한 리전의 모든 AZ에서 접근 가능온프레미스 서버는 AWS Connect를 사용해 접근 가능



S3 vs. EBS vs. EFS

구분		File EFS	Object S3	Block EBS
퍼포먼스	작업별 대기 시간	<ul style="list-style-type: none"> 낮음, 일관됨 	<ul style="list-style-type: none"> 낮음, 여러 요청 탑재 처리, CloudFront와 통합 	<ul style="list-style-type: none"> 가장 낮음, 일관됨
	처리량 크기	<ul style="list-style-type: none"> 초당 GBs 	<ul style="list-style-type: none"> 초당 GBs 	<ul style="list-style-type: none"> 초당 GB
특성	가용성 / 내구성 (availability, durability)	<ul style="list-style-type: none"> 여러 AZ에 중복 저장 	<ul style="list-style-type: none"> 여러 AZ에 중복 저장 	<ul style="list-style-type: none"> 단일 AZ에 중복 저장
	액세스	<ul style="list-style-type: none"> 1개~수천개의 EC2인스턴스 / on-premise 서버 / 여러 AZ에서 동시 접근 	<ul style="list-style-type: none"> 웹을 통한 수백만 개의 연결 	<ul style="list-style-type: none"> 하나의 AZ에 속한 하나의 EC2 인스턴스
사용 케이스				
	사용 케이스	<ul style="list-style-type: none"> 웹 서비스 및 컨텐츠 관리 엔터프라이즈 어플리케이션 홈 디렉토리 데이터베이스 백업 개발자 도구 컨테이너 스토리지 빅데이터 분석 	<ul style="list-style-type: none"> 웹 서비스 및 컨텐츠 관리 미디어 및 엔터테인먼트 백업 빅데이터 분석 데이터 레이크 	<ul style="list-style-type: none"> 부팅 볼륨 트랜잭션 및 NoSQL 데이터베이스 데이터 웨어하우징 및 ETL

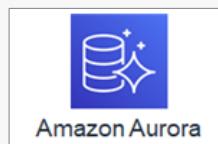
Amazon Relational Database Service(Amazon RDS)

- 관계형 데이터베이스

- 관계형 데이터베이스는 정형 쿼리 언어(SQL)를 사용하여 데이터를 저장하고 쿼리
- 데이터를 쉽게 이해할 수 있고 일관되며 확장 가능한 방식으로 저장

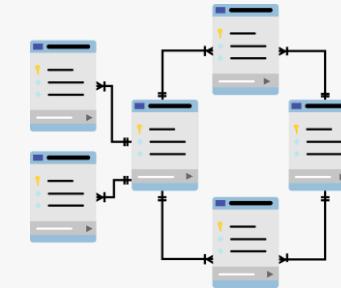
- Amazon RDS 데이터베이스 엔진

- 메모리, 성능 또는 입/출력(I/O)에 최적화된 6개의 데이터베이스 엔진에서 사용 가능



- Amazon Aurora

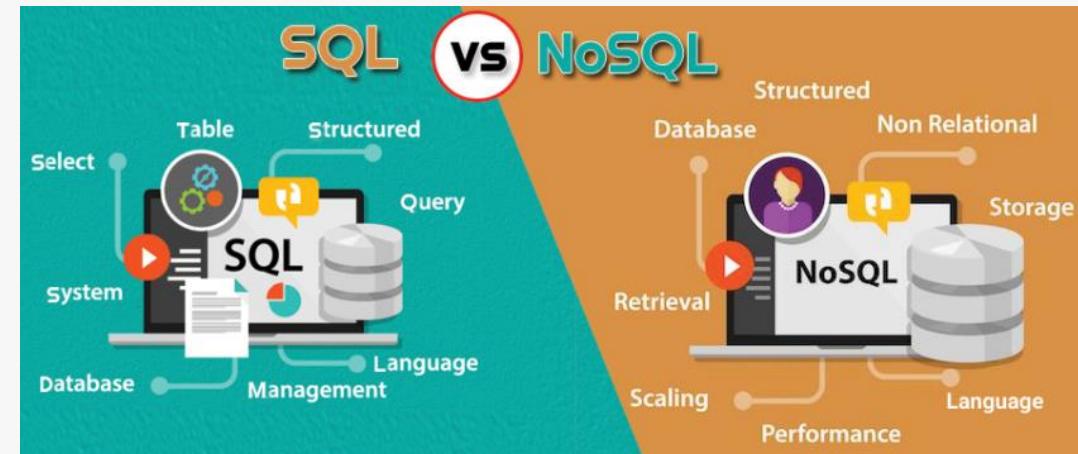
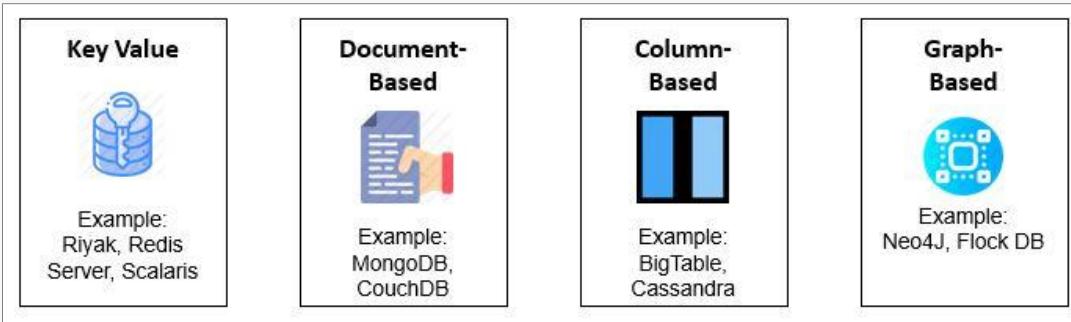
- 엔터프라이즈급 관계형 데이터베이스
 - ✓ 6개의 데이터 복사본을 3개의 가용 영역에 복제하고 지속적으로 Amazon S3에 데이터를 백업
 - ✓ MySQL 및 PostgreSQL 관계형 데이터베이스와 호환
 - ✓ 표준 MySQL 데이터베이스보다 최대 5배 빠르며 표준 PostgreSQL 데이터베이스보다 최대 3배 빠름
 - ✓ 데이터베이스 리소스의 안정성 및 가용성을 유지하면서도 불필요한 입/출력(I/O) 작업을 줄여 데이터베이스 비용 절감



Amazon DynamoDB

■ 비관계형 데이터베이스

- 언제든 테이블의 항목에서 속성을 추가하거나 제거
- 테이블의 모든 항목에 동일한 속성이 있어야 하는 것은 아님



■ Amazon DynamoDB

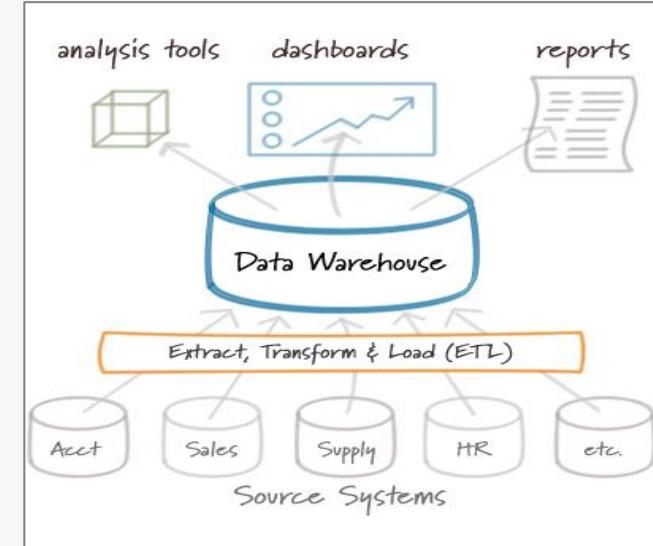
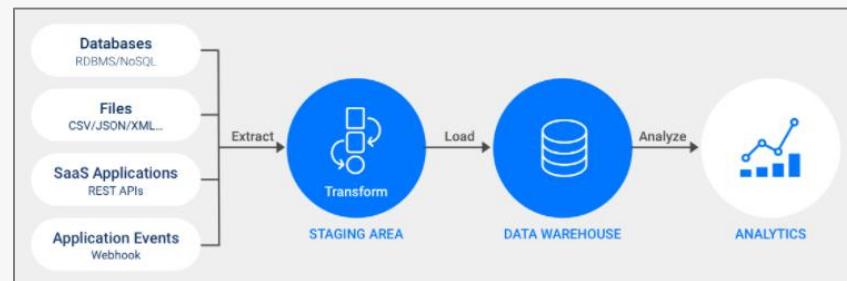
- Amazon DynamoDB는 키-값 데이터베이스 서비스
- 모든 규모에서 한 자릿수 밀리 초의 성능을 제공
- 서비스 : 서버, 소프트웨어를 설치, 유지 관리, 운영 관리 필요 없음
- 자동 조정 : DB 용량에 맞춰 자동으로 크기를 조정하면서도 일관된 성능 유지
 - ✓ 크기를 조정하는 동안에도 고성능을 유지해야 하는 경우에 적합

Amazon Redshift



■ 데이터 웨어하우스(DW)

- 정보에 입각한 의사 결정을 내릴 수 있도록 분석 가능한 정보의 중앙 리포지토리
- ETL(Extraction, Transformation, Loading)
 - ✓ 데이터를 추출하여, 원하는 형태로 변환하고 다른 Database에 적재하는 작업 과정



■ 빅 데이터 분석에 사용할 수 있는 데이터 웨어하우징 서비스

- 여러 원본에서 데이터를 수집하여 데이터 간의 관계 및 추세를 파악하는 데 도움이 되는 기능
- 사용 사례
 - ✓ 비즈니스 인텔리전스
 - ✓ 이벤트에서 운영 분석
 - ✓ 서비스형 데이터
 - ✓ 예측 분석

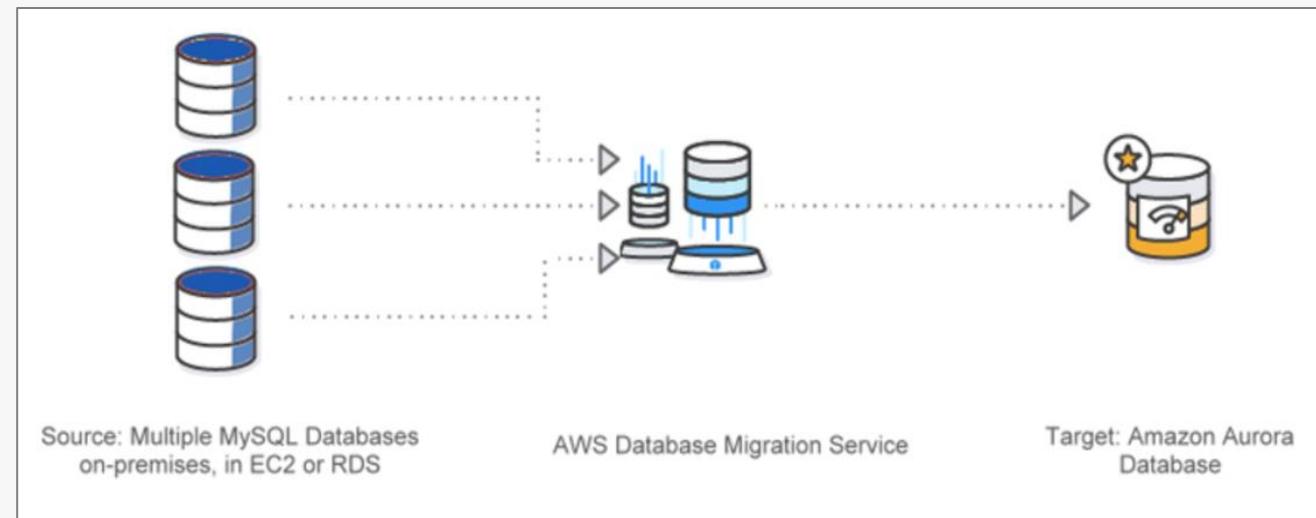


AWS Database Migration Service



AWS Database
Migration Service

- 관계형/비관계형 비관계형 데이터베이스 및 기타 유형의 데이터 저장소를 마이그레이션할 수 있는 서비스
 - 원본 데이터베이스와 대상 데이터베이스 간에 데이터를 이동 – 다른 유형의 데이터베이스
 - ✓ 마이그레이션 동안 원본 데이터베이스가 계속 작동하므로 이를 사용하는 애플리케이션의 가동 중지 시간을 줄임
 - 특징
 - ✓ Simple to Use
 - ✓ Reliable
 - ✓ Low Cost
 - ✓ Fast and Eas Setup
 - ✓ Minimal Downtime
 - ✓ Supports Most Widely Used Databases
 - 사용 사례
 - ✓ 개발 및 테스트 데이터베이스 마이그레이션
 - ✓ 여러 데이터베이스를 단일 데이터베이스로 결합
 - ✓ 연속 복제



추가 데이터베이스 서비스

- 비즈니스 요구 사항에 맞는 올바른 데이터베이스를 선택하고 올바른 스토리지 플랫폼을 선택해야 함

Amazon DocumentDB		✓ MongoDB 워크로드를 지원하는 문서 데이터베이스 서비스
Amazon Neptune		<ul style="list-style-type: none">✓ 그래프 데이터베이스 서비스✓ 추천 엔진, 사기 탐지 같이 고도로 연결된 데이터 세트로 동작하는 애플리케이션의 빌드 및 실행
Amazon Quantum Ledger Database(Amazon QLDB)		<ul style="list-style-type: none">✓ 원장 데이터베이스 서비스✓ Amazon QLDB를 사용해 애플리케이션 데이터에 발생한 모든 변경의 전체 기록 검토 가능
Amazon Managed Blockchain		<ul style="list-style-type: none">✓ 오픈 소스 프레임워크를 사용해 블록체인 네트워크를 생성 및 관리에 사용 가능한 서비스
Amazon ElastiCache		<ul style="list-style-type: none">✓ 자주 사용되는 요청의 읽기 시간 향상을 위해 데이터베이스 위에 캐싱 계층을 추가하는 서비스✓ Redis 및 Memcached 지원
Amazon DynamoDB Accelerator		<ul style="list-style-type: none">✓ Amazon DynamoDB Accelerator(DAX)는 DynamoDB용 인 메모리 캐시✓ 응답 시간을 한 자릿수 밀리초에서 마이크로초까지 향상 가능

Module 6

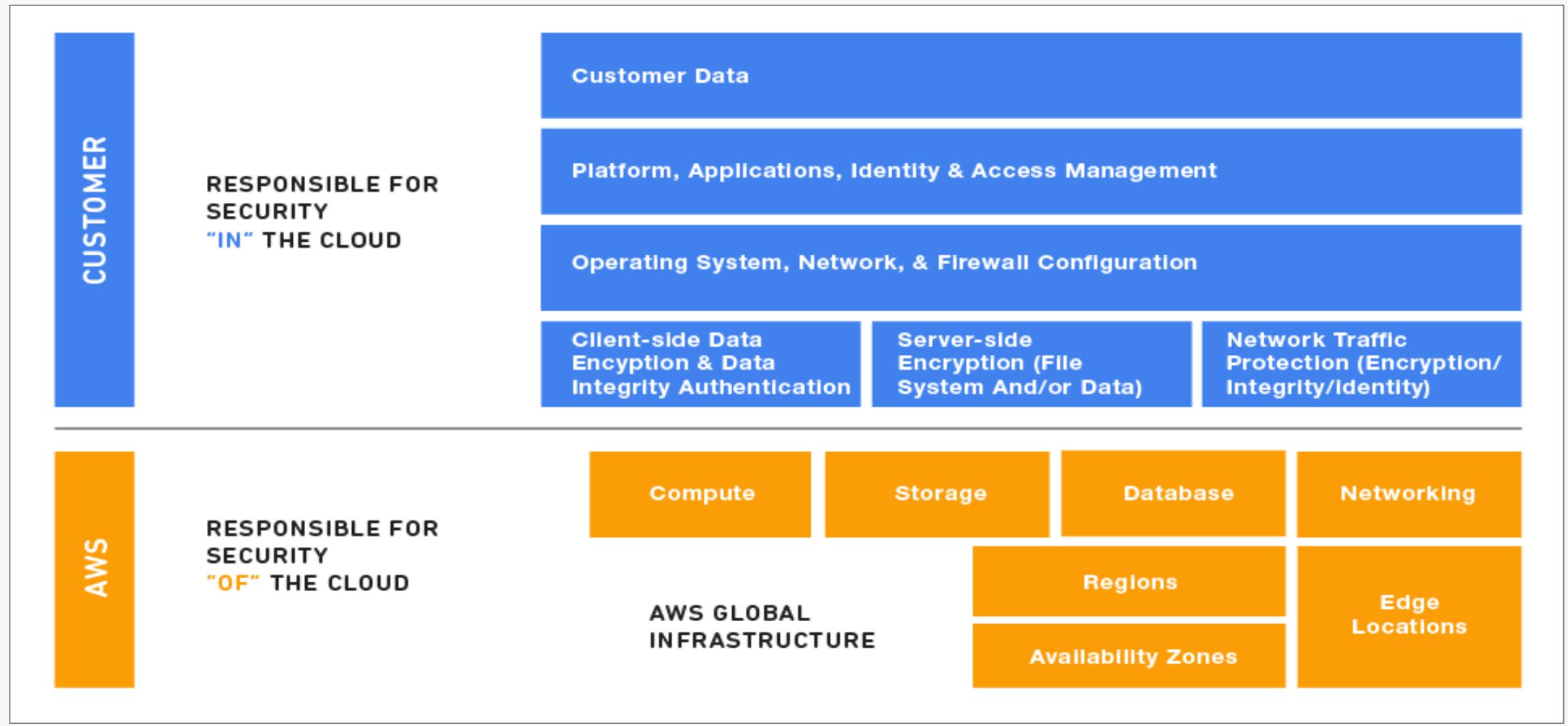
보안

- 공동 책임 모델
- Multi-Factor Authentication
- AWS Identity and Access Management
- 기본 보안 정책과 AWS Organizations
- AWS 사용 시 규정 준수
- AWS 보안 서비스

AWS 공동 책임 모델

- 보안과 규정 준수는 AWS와 고객의 공동 책임
 - AWS 책임 '클라우드의 보안' : AWS 클라우드에서 제공되는 모든 서비스를 실행하는 인프라를 보호할 책임
 - 고객 책임 '클라우드에서의 보안' : 고객 책임은 고객이 선택하는 AWS 클라우드 서비스에 따라 달라짐
- 고객/AWS 공동 책임 모델은 IT 제어까지도 확장
 - AWS 제어 및 규정 준수 설명서를 사용하여 필요에 따라 제어 평가 및 확인 절차를 수행할 있음
 - AWS, AWS 고객 및/또는 양쪽에서 관리하는 제어 항목
 - 상속된 제어 항목 – 고객이 AWS로부터 전적으로 상속받는 제어 항목 :
 - ✓ 물리적 및 환경 제어 항목
 - 공유된 제어 항목 – 인프라 계층과 고객 계층에 모두 적용되지만, 컨텍스트 또는 관점이 완벽하게 구분되는 제어 항목
 - ✓ 패치 관리, 구성 관리, 인지 및 고육
 - 고객 특정 – AWS 서비스에서 배포하는 애플리케이션에 따라 전적으로 고객의 책임인 제어 항목
 - ✓ 고객이 특정 보안 환경 내에서 데이터를 라우팅하거나 영역을 지정 할 수 있는 서비스 및 통신 보호, 영역 보안

AWS 공동 책임 모델



사용자 권한 및 액세스 (1/3)



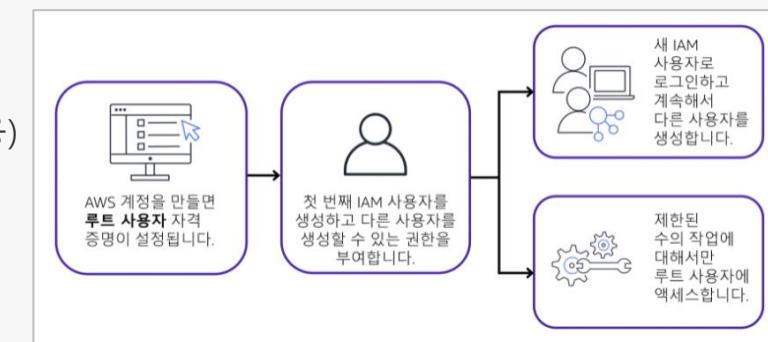
▪ AWS Identity and Access Management(IAM)

- AWS 서비스와 리소스에 대한 액세스를 안전하게 관리 (권한 관리 솔루션)
- IAM은 회사의 고유한 운영 및 보안 요구 사항에 따라 액세스 권한을 구성할 수 있는 유연성 제공
- 이 작업을 수행하기 위해 다음과 같은 IAM 기능을 조합하여 사용
 - ✓ IAM 사용자, 그룹 및 역할
 - ✓ IAM 정책
 - ✓ Multi-Factor Authentication

The screenshot shows the AWS Identity and Access Management (IAM) console. At the top, it says "Identity and Access Management (IAM)". Below that is a navigation bar with "AWS Account" and "AWS Organizations". Under "AWS Account", there are links for "대시보드", "그룹", "사용자", "역할", and "정책". There are also links for "자격 증명 공급자", "계정 설정", and "자격 증명 보고서". A search bar at the bottom right contains the text "IAM 검색".

▪ AWS 계정 루트 사용자

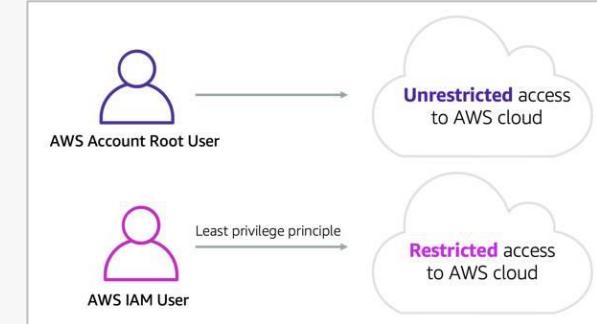
- AWS 계정을 처음 만들면 루트 사용자라고 하는 자격 증명으로 시작
- 루트 사용자는 AWS 계정을 만들 때 사용한 이메일 주소 및 암호로 로그인
 - ✓ 일상 작업에 사용 안됨 (루트 사용자는 AWS Support 플랜 변경 등 제한적인 경우 사용)
 - ✓ 루트 사용자를 사용해 첫 번째 IAM 사용자를 생성
 - ✓ 이 사용자에게 다른 사용자를 생성할 수 있는 권한을 할당



사용자 권한 및 액세스 (2/3)

▪ IAM 사용자

- IAM 사용자는 사용자가 AWS에서 생성하는 자격 증명
 - ✓ 이 사용자는 AWS 서비스 및 리소스와 상호 작용하는 사람 또는 애플리케이션을 나타냄
 - ✓ 이 사용자는 이름과 자격 증명으로 구성
- AWS에서 새 IAM 사용자를 생성하면 해당 사용자와 연결된 권한이 없음
 - ✓ IAM 사용자가 AWS에서 Amazon EC2 인스턴스 시작 등 특정 작업을 수행을 허용하려면 필요한 권한을 부여해야 함
- AWS에 액세스해야 하는 각 사용자마다 개별 IAM 사용자를 생성하는 것이 좋음



▪ IAM 정책

- IAM 정책은 AWS 서비스 및 리소스에 대한 권한을 허용하거나 거부하는 문서
- IAM 정책을 사용하면 사용자가 리소스에 액세스할 수 있는 수준을 사용자 지정 가능
 - ✓ 예) 사용자가 AWS 계정 내의 모든 Amazon S3 버킷에 액세스하거나 특정 버킷에만 액세스하도록 허용
- 권한 부여 시, **최소 권한 보안 원칙** 적용:
 - ✓ 사용자 또는 역할이 해당 작업을 수행하는 데 필요한 것보다 많은 권한을 갖는 것을 방지



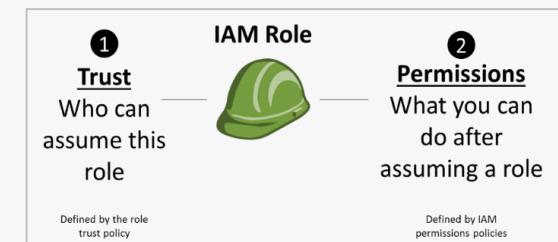
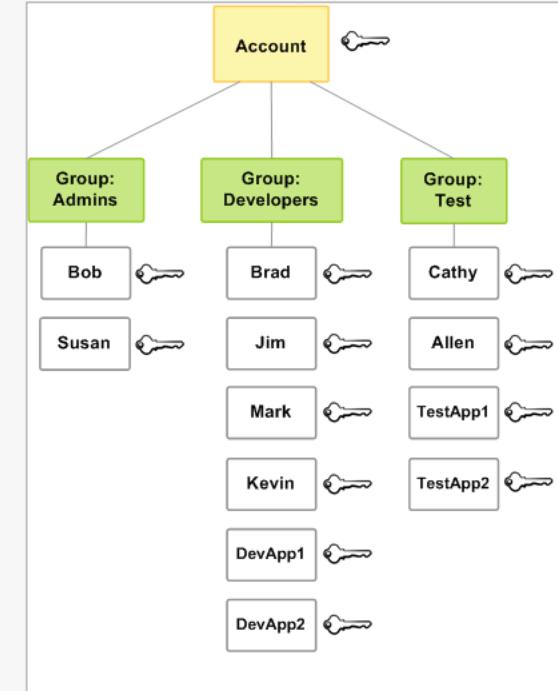
사용자 권한 및 액세스 (3/3)

IAM 그룹

- IAM 그룹은 IAM 사용자의 모음
 - ✓ 한 그룹에 여러 사용자가 포함, 한 사용자가 여러 그룹에 포함
 - ✓ 사용자 그룹은 중첩될 수 없음, 사용자 그룹은 사용자만 포함
 - ✓ 모든 사용자를 자동으로 포함하는 기본 사용자 그룹은 없음
 - ✓ AWS 계정의 IAM 리소스 수와 크기는 제한
- 그룹에 IAM 정책 할당 시, 해당 그룹의 모든 사용자에게 정책에 지정된 권한 부여
 - ✓ 그룹 수준에서 IAM 정책을 할당하면 직원이 직무를 전환하는 경우 권한을 손쉽게 조정 가능

IAM 역할

- IAM 역할은 임시로 권한에 액세스하기 위해 수임할 수 있는 자격 증명
 - ✓ 서비스 또는 리소스에 대한 액세스 권한을 일시적으로 부여해야 하는 상황에 이상적
- 사용자, APP, 서비스가 IAM 역할을 수임하려면, 해당 역할로의 전환 권한을 부여 필요
 - ✓ IAM 역할을 수임한다는 것은 이전 역할에 지정된 모든 권한을 포기하고 새 역할에 지정된 권한을 수임



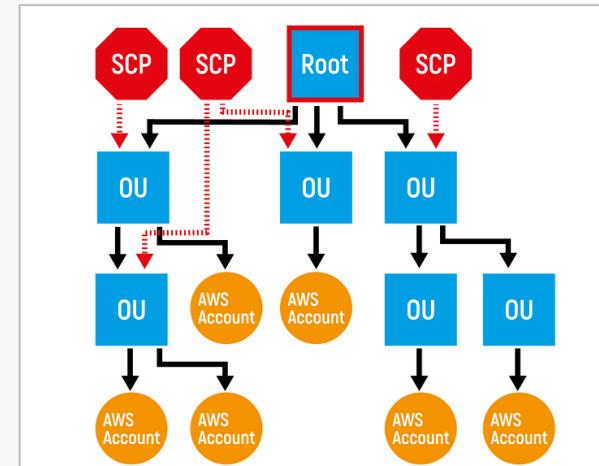
AWS Organizations



- AWS Organizations를 사용해 중앙 위치에서 여러 AWS 계정을 통합하고 관리
 - 조직을 생성하면 AWS Organizations가 조직의 모든 계정에 대한 상위 컨테이너 루트를 자동으로 생성
- 서비스 제어 정책(SCP) - 조직 계정에 대한 권한을 중앙에서 제어
 - 각 계정의 사용자 및 역할이 액세스할 수 있는 AWS 서비스, 리소스 및 개별 API 작업을 제한
- 조직 단위(OU)
 - AWS Organizations에서는 계정을 조직 단위(OU)로 그룹화
 - 비슷한 비즈니스 또는 보안 요구 사항이 있는 계정들을 손쉽게 관리
 - ✓ 개별 계정을 OU로 구성 : 특정 보안 요구사항이 있는 워크로드/애플리케이션을 간편하게 격리

➤ IAM vs. AWS Organizations

- IAM는 개별 계정에서 사용자와 역할에 대한 세분화된 제어를 제공
- AWS Organizations 사용자가 계정이나 계정 그룹에서 사용자와 역할이 할 수 있는 일을 제어하게 함으로써 제어력을 계정 수준까지 확장



규정 준수



■ AWS Artifact

- AWS Artifact는 AWS 보안 및 규정 준수 보고서 및 일부 온라인 계약에 대한 온디맨드 액세스를 제공하는 서비스
- AWS Artifact는 AWS Artifact Agreements 및 AWS Artifact Reports의 두 가지 기본 섹션으로 구성

AWS Artifact Agreements	<ul style="list-style-type: none">✓ AWS 서비스 전체에서 특정 유형의 정보를 사용✓ 개별 계정 및 AWS Organizations 내 모든 계정에 대한 계약을 검토, 수락 및 관리
AWS Artifact Reports	<ul style="list-style-type: none">✓ 특정 규제 표준을 준수하기 위한 책임에 대한 추가 정보가 필요 시, 정보에 액세스하도록 조언✓ 외부 감사 기관이 작성한 규정 준수 보고서를 제공✓ 감사 기관에서 AWS가 다양한 글로벌, 지역별, 산업별 보안 표준 및 규정을 준수했음을 검증✓ AWS Artifact Reports는 릴리스 된 최신 보고서가 반영되어 항상 최신 상태로 유지✓ 감사 또는 규제 기관에 AWS 보안 제어 항목의 증거로서 AWS 감사 아티팩트를 제공

■ 고객 규정 준수 센터

- AWS 규정 준수에 대해 자세히 알아볼 수 있는 리소스 포함
 - ✓ 주요 규정 준수 질문에 대한 AWS 답변
 - ✓ AWS 위험 및 규정 준수 개요
 - ✓ 보안 감사 체크리스트
- 사례를 통해 규제 대상 업종의 기업들이 다양한 규정 준수, 거버넌스 및 감사 과제 해결 방법 확인
 - ✓ 고객 규정 준수 센터에는 감사자 학습 경로가 포함



서비스 거부 공격



■ 서비스 거부(DoS) 공격

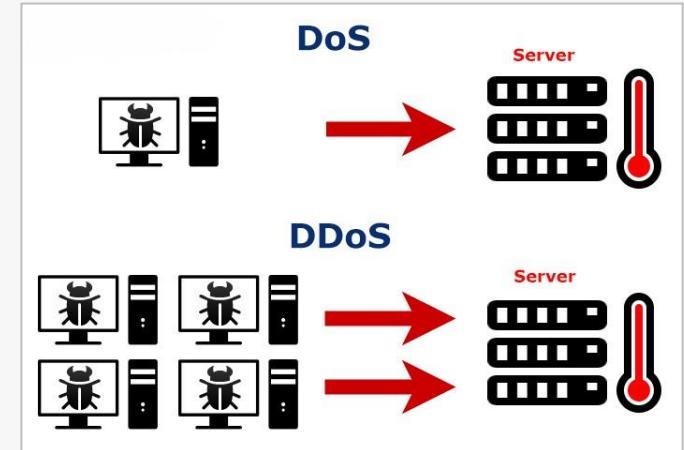
- 특정한 네트워크나 웹 리소스에 합법적인 유저가 접근하지 못하도록 방해
- 사용자들이 웹 사이트 또는 애플리케이션을 이용할 수 없게 만들려는 의도적인 시도

■ 분산 서비스 거부(DDoS) 공격

- 여러 소스를 사용하여 웹 사이트 또는 애플리케이션을 사용할 수 없게 만드는 공격
- 감염된 컴퓨터들('봇')를 사용해 과도한 트래픽을 웹 사이트/애플리케이션으로 전송

■ AWS Shield

- DDoS 공격으로부터 애플리케이션을 보호하는 서비스

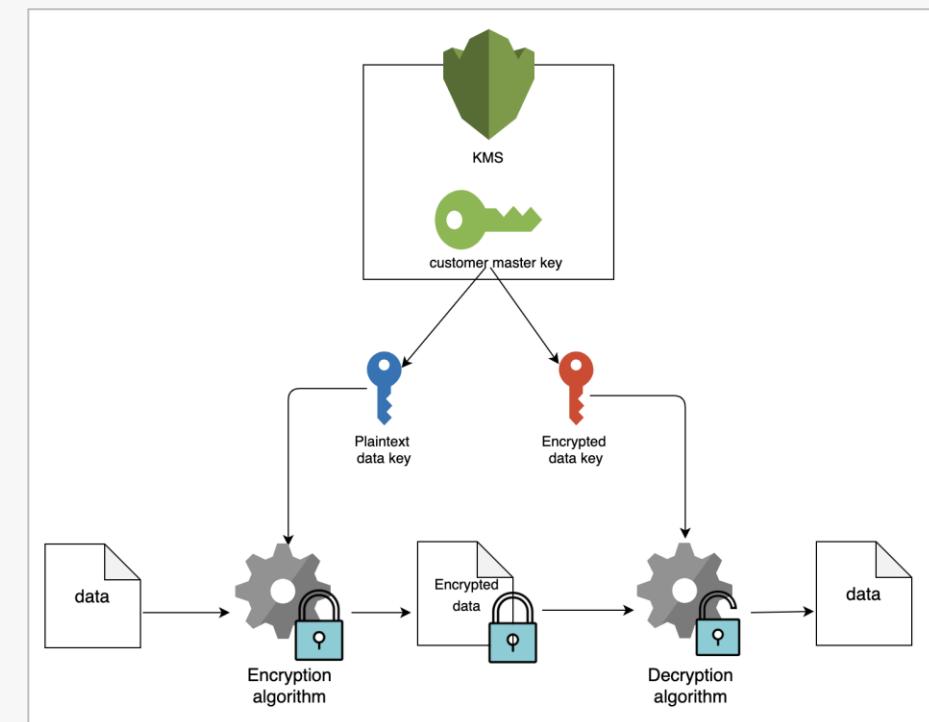


AWS Shield Standard	<ul style="list-style-type: none">✓ 모든 AWS 고객을 자동으로 보호하는 무료 서비스✓ WS 리소스를 가장 자주 발생하는 일반적인 DDoS 공격으로부터 보호✓ 다양한 분석 기법을 사용하여 실시간으로 악성 트래픽을 탐지하고 자동으로 완화✓ SYN flood 및 UDP 공격(3~4계층 DDOS 공격 차단)	
AWS Shield Advanced	<ul style="list-style-type: none">✓ 상세한 공격 진단 및 정교한 DDoS 공격을 탐지하고 완화할 수 있는 기능을 제공하는 유료 서비스✓ Amazon CloudFront, Amazon Route 53, Elastic Load Balancing 같은 서비스와 통합✓ 복잡한 DDOS 공격을 완화하기 위한 사용자 지정 규칙을 작성해 AWS WAF와 통합 가능✓ 7계층 공격 보호 추가	

추가 보안 서비스 (1/4)

▪ AWS Key Management Service(AWS KMS)

- 데이터를 암호화 할 때 사용되는 암호화 Key 를 안전하게 관리하는데 목적을 둔 서비스
- 암호화 키는 데이터 잠금(암호화) 및 잠금 해제(암호 해독)에 사용되는 임의의 숫자 문자열
- AWS KMS를 사용하여 암호화 키를 생성, 관리 및 사용
- 광범위한 서비스 및 애플리케이션에서 키 사용을 제어
- AWS KMS를 사용하면 키에 필요한 액세스 제어를 특정 수준으로 선택
- 키를 관리할 수 있는 IAM 사용자 및 역할을 지정
- 더 이상 사용되지 않도록 일시적으로 키를 비활성화
- 키는 AWS KMS를 벗어나지 않으며, 사용자가 항상 키를 제어 가능

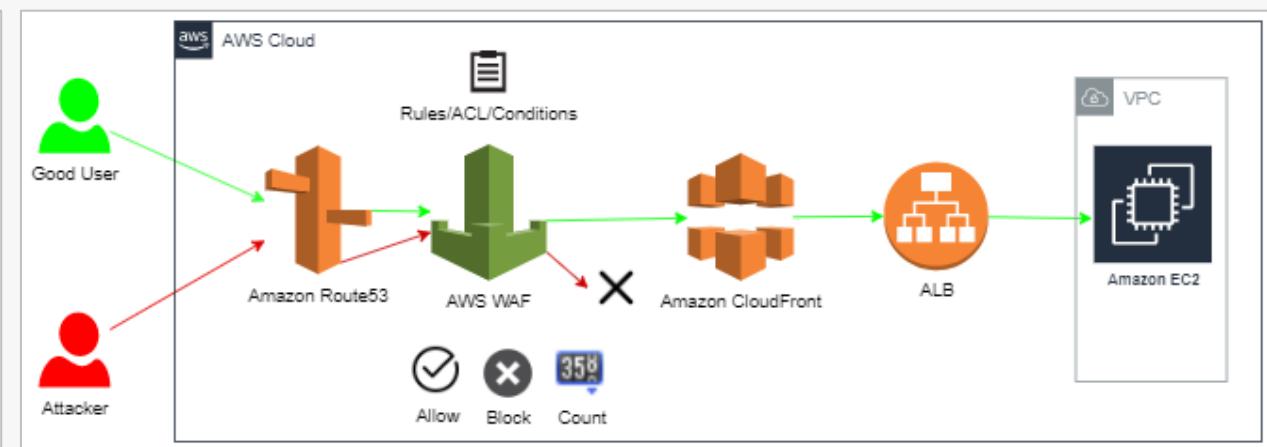
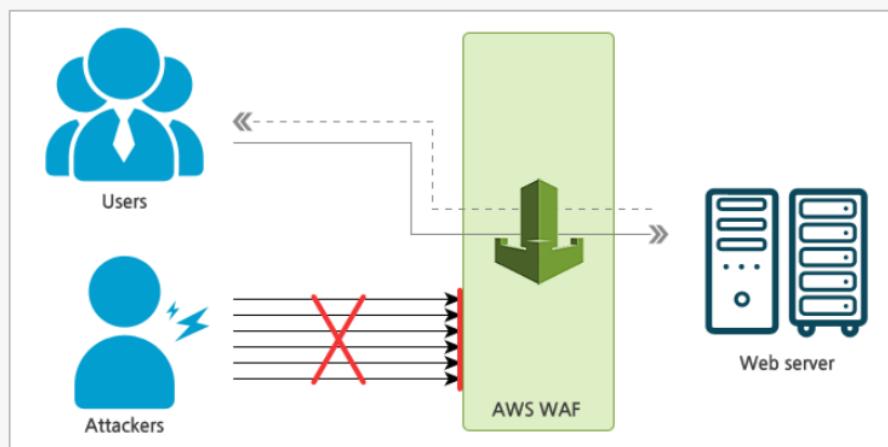


추가 보안 서비스 (2/4)



▪ AWS WAF

- 웹 애플리케이션으로 들어오는 네트워크 요청을 모니터링할 수 있는 웹 애플리케이션 방화벽
 - ✓ 일반적인 웹 취약점으로부터 웹 애플리케이션 보호
 - ✓ 트래픽을 차단하거나 허용
 - ✓ AWS 리소스를 보호하기 위해 웹 ACL(액세스 제어 목록)을 사용
- WS WAF는 Amazon CloudFront 및 Application Load Balancer와 함께 작동
- 원본 IP 주소 패턴이나 지리적 위치에 따라 트래픽 차단
- Lambda함수를 사용하여 알려진 악성 IP 주소 목록 확인 및 HTTP flood 공격 식별



추가 보안 서비스 (3/4)



▪ Amazon Inspector

- Amazon Inspector는 자동화된 보안 평가를 실행하여 애플리케이션의 보안 및 규정 준수를 개선할 수 있는 서비스
- 인스턴스에서 평가를 실행해 네트워크, 파일 시스템, 프로세스 활동을 분석
- 수집한 데이터를 하나 이상의 규칙 패키지와 비교하여 위협과 취약점을 파악
- Amazon Inspector는 평가를 수행한 후에 보안 탐지 결과 목록을 제공
 - ✓ 이 목록은 심각도 수준에 따라 우선 순위가 결정되고 각 보안 문제에 대한 자세한 설명 및 권장 해결 방법이 포함
 - ✓ AWS는 제공된 권장 사항으로 모든 잠재적 보안 문제가 해결됨을 보장하지 않음

Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. [Learn more](#).

Last updated on September 24, 2015 4:12:42 PM (20m ago)

Viewing 1-10 of 24 >

Add/Edit attributes	Severity	Application	Assessment	Rule package	Finding
<input type="checkbox"/>	High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is configured without a password.
<input type="checkbox"/>	High ⓘ	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c46f is vulnerable to a known security issue.
<input type="checkbox"/>	High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity mecha...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Initial app	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found to...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Initial app	PCI DSS 3.0 Readiness	The machine i-aac4c46f was fo...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential security issues fo...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	The machine i-aac4c46f was fo...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues fo...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found to...
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Initial app	PCI DSS 3.0 Readiness	A machine with Instance ID i-a...

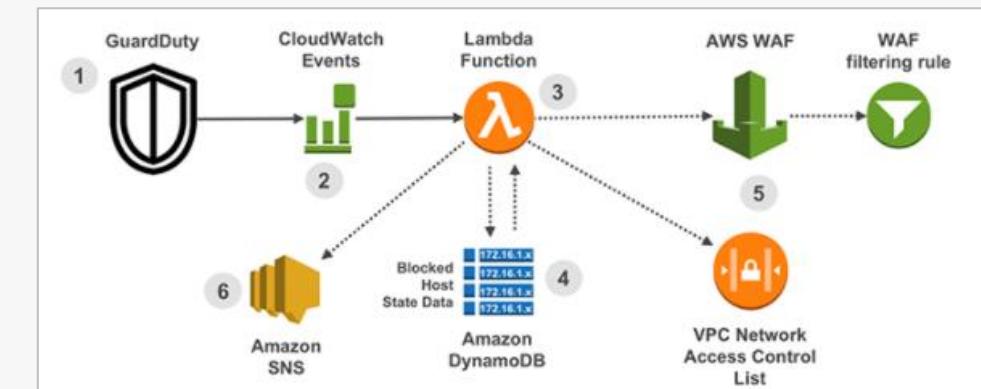
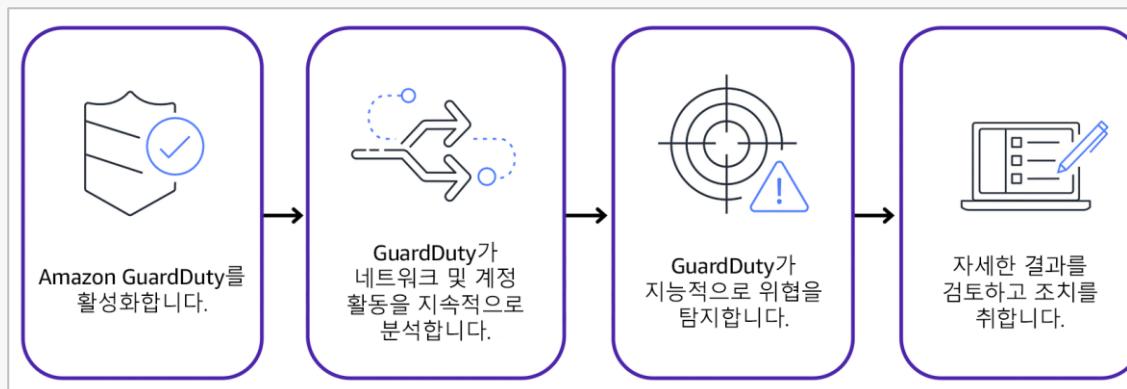


추가 보안 서비스 (4/4)



▪ Amazon GuardDuty

- AWS 인프라 및 리소스에 대한 지능형 위협 탐지 기능을 제공하는 서비스
 - ✓ 이 서비스는 AWS 환경 내의 네트워크 활동 및 계정 동작을 지속적으로 모니터링하여 위협 식별
 - ✓ AWS 계정에서 GuardDuty를 활성화하면 GuardDuty가 네트워크 및 계정 활동을 모니터링하기 시작
- 추가 보안 소프트웨어를 배포하거나 관리할 필요 없음
- GuardDuty가 위협을 탐지한 경우, AWS Management Console에서 위협에 대한 자세한 탐지 결과를 검토
 - ✓ 탐지 결과에는 문제 해결을 위한 권장 단계가 포함
 - ✓ 탐지 결과에 대해 자동으로 문제 해결 단계를 수행하도록 AWS Lambda 함수를 구성 가능



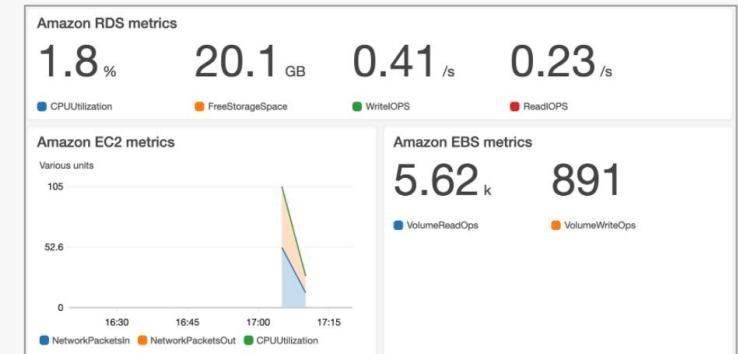
Module 7

모니터링 및 분석

- AWS 환경 모니터링
- Amazon CloudWatch
- AWS CloudTrail
- AWS Trusted Advisor

Amazon CloudWatch

- 다양한 지표를 모니터링 및 관리하고 해당 지표의 데이터를 기반으로 경보 작업을 구성할 수 있는 웹 서비스
 - 지표를 사용하여 리소스의 데이터 포인트 표시
 - ✓ AWS 서비스는 지표를 CloudWatch로 전송
 - ✓ CloudWatch가 이 지표를 사용해 시간에 따른 성능 변화를 보여주는 그래프 자동 생성
- CloudWatch 경보
 - 지표의 값이 미리 정의된 임계치를 상회 또는 하회할 경우 자동으로 작업을 수행하는 경보를 생성
 - 경보를 구성할 때 이 경보가 트리거 될 때마다 알림을 받도록 지정할 수 있음
- CloudWatch 대시보드
 - CloudWatch 대시보드를 사용하면 단일 위치에서 리소스에 대한 모든 지표에 접근
 - ✓ Amazon EC2 인스턴스의 CPU 사용률, Amazon S3 버킷에 대해 실행된 총 요청 수 등
 - 다양한 용도, 애플리케이션/리소스에 따라 별도의 대시보드를 사용자 지정 가능



AWS CloudTrail

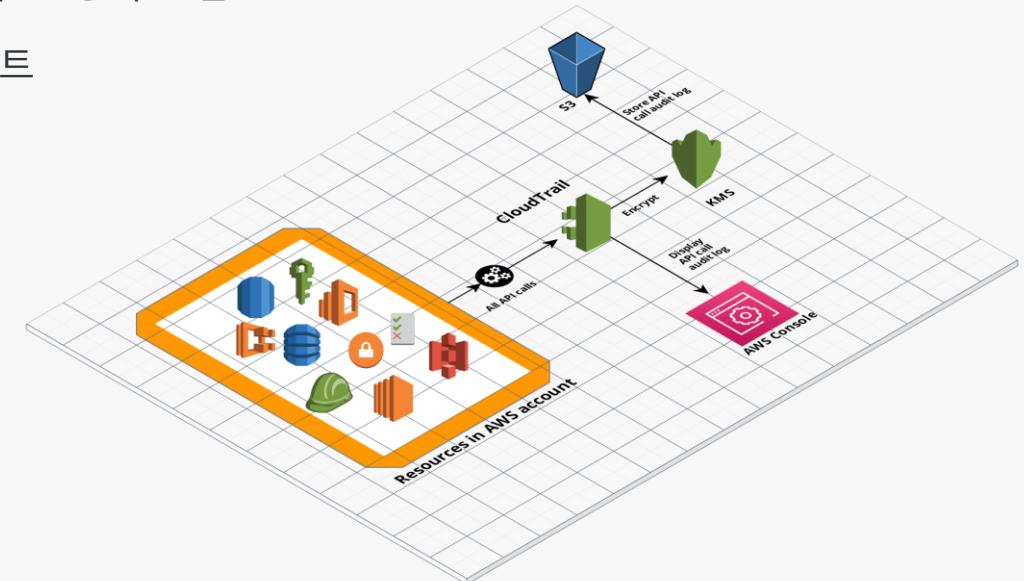


- AWS 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 AWS 서비스
 - CloudTrail은 누군가 남긴 이동 경로(또는 작업 로그)의 '추적'
 - CloudTrail을 사용해 애플리케이션 및 리소스에 대한 사용자 활동 및 API 호출의 전체 내역을 볼 수 있음
 - ✓ API 호출을 사용하여 AWS 리소스를 프로비저닝, 관리 및 구성할 수 있기 때문이다
 - ✓ API 호출이 발생한 날짜 및 시간, 작업을 요청한 사용자, API 호출에 포함된 리소스 유형 등을 지정하여 이벤트 필터링 가능
 - 기록되는 정보 : API 호출자 ID, API 호출 시간, API 호출자의 소스 IP 주소 등이 포함
 - 이벤트는 일반적으로 API 호출 후 15분 이내에 CloudTrail에서 업데이트
- CloudTrail Insights
 - CloudTrail Insights를 활성화 가능
 - ✓ CloudTrail이 AWS 계정에서 비정상적인 API 활동 자동 감지

Insights events 

Insights events are logs of unusual levels of **write** API calls that have occurred in your AWS account over the last 90 days.

Log Insights events Yes No



AWS Trusted Advisor

- AWS 환경을 검사하고 AWS 모범 사례에 따라 실시간 권장 사항을 제시하는 웹 서비스
 - Trusted Advisor는 비용 최적화, 성능, 보안, 내결함성, 서비스 한도라는 5개 범주에서 결과를 AWS 모범 사례와 비교
 - ✓ 각 범주의 검사에 대해 권장 작업 목록을 제공하고 AWS 모범 사례를 자세히 알아볼 수 있는 추가 자료를 제공
 - ✓ AWS Trusted Advisor가 제공하는 권장 사항은 배포의 모든 단계에서 유용
 - 기존 애플리케이션 및 리소스를 지속적으로 개선하는 데 활용
 - 새로운 워크플로를 만들고 새로운 애플리케이션을 개발에 활용
- AWS Trusted Advisor 대시보드
 - 비용 최적화, 성능, 보안, 내결함성, 서비스 한도 범주에서 완료된 검사를 검토



- **녹색** 체크 표시는 문제가 감지되지 않은 항목 수를 나타냅니다.
- **주황색** 삼각형은 권장 조사 항목 수를 나타냅니다.
- **빨간색** 원은 권장 조치 수를 나타냅니다.

Module 8

요금 및 지원

- AWS 요금 및 지원 모델
- AWS 프리티어 설명
- AWS Organizations 및 통합 결제
- AWS 예산, AWS Cost Explorer와 AWS 요금 계산기
- AWS Support 플랜
- AWS Marketplace

AWS 프리 티어

- AWS에서 지정된 기간 동안 비용을 신경 쓸 필요 없이 특정 서비스를 사용 가능
 - 프리 티어를 이용해 100가지가 넘는 제품을 살펴보고 AWS에 구축
- 3 가지 제공 유형

상시 무료		<ul style="list-style-type: none">✓ 여기에 포함되는 제품은 만료되지 않으며 모든 AWS 고객에게 제공<ul style="list-style-type: none">• AWS Lambda에서는 매월 무료 요청 1백만 건과 최대 320만 초의 컴퓨팅 시간 사용• Amazon DynamoDB에서는 매월 25GB의 무료 스토리지 사용
12개월 무료		<ul style="list-style-type: none">✓ WS에 처음 가입한 날로부터 12개월 동안 무료로 제공<ul style="list-style-type: none">• 일정량의 Amazon S3 Standard 스토리지• 월별 Amazon EC2 컴퓨팅 시간 한도• Amazon CloudFront 데이터 전송량
평가판		<ul style="list-style-type: none">✓ 특정 서비스를 활성화한 날짜부터 시작✓ 각 평가판의 기간은 일수 또는 서비스 사용량을 기준으로 다름<ul style="list-style-type: none">• Amazon Inspector는 90일 무료 평가판 제공• Amazon Lightsail은 30일 동안 750시간의 무료 사용 시간 제공

컴퓨팅	스토리지	데이터베이스
프리 티어 Amazon EC2 750시간 플랫폼 클라우드에서 제공되는 크기 조정 가능한 컴퓨팅 파워입니다. 월별 750시간의 Linux, RHEL 또는 SLES	프리 티어 Amazon S3 5GB 표준 스토리지 보안성, 안정성 및 확장성을 갖춘 객체 스토리지 인프라입니다. 표준 스토리지 5GB	프리 티어 Amazon RDS 750시간 플랫폼 db.t2.micro 데이터베이스 사용량(DB 엔진에 적용됨) MySQL, PostgreSQL, MariaDB, Oracle BYOL 또는 SQL Server를 위한 관계형 데이터베이스 서비스입니다.

AWS 요금 개념



- AWS는 종량제 요금으로 다양한 클라우드 컴퓨팅 서비스를 제공

- 실제 사용한 만큼 지불
- 예약하는 경우 비용 감소
- 많이 사용할수록 볼륨 기반 할인

- AWS 요금 계산기

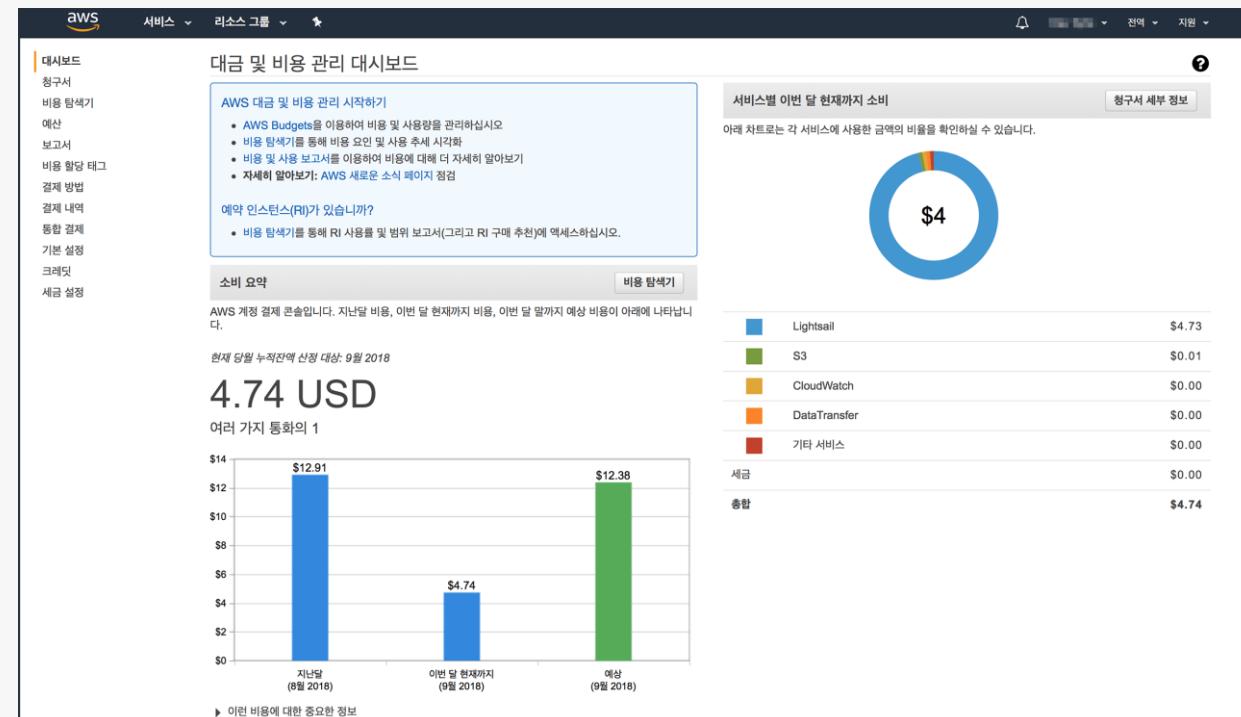
- AWS 서비스를 탐색하고 AWS 기반 사용 사례에 대한 비용을 추정
 - ✓ AWS 비용 추정을 정의된 그룹별로 구성할 수 있습니다.
 - ✓ 그룹은 비용 센터별로 비용 추정을 제공하는 등 회사 조직 구성을 반영
- 회사에서 Amazon EC2 사용에 관심이 있다고 가정
 1. AWS 요금 계산기에 필요한 OS, 메모리, 입/출력(I/O) 요구 사항 등 입력
 2. AWS 요금 계산기에서 AWS 리전 및 EC2 인스턴스 유형별 예상 비용 비교
 3. 사용 사례에 가장 비용 효율적인 AWS 리전 또는 인스턴스 유형 결정

My estimate		Info		Add group		Export	
First 12 months total		949.68 USD					
Upfront		0.00 USD					
Monthly		79.14 USD					
West Coast Servers Region: US West (Oregon)							
Amazon EC2		Action ▾		Add service		Actions ▾	
1 t3.xlarge Linux instance with a consistent workload		Upfront		0.00 USD		Monthly	
Amazon EBS		76.14 USD					
30 GB General Purpose SSD (gp2) with 2x daily snapshots		Upfront		0.00 USD		Monthly	
Group total		Upfront		0.00 USD		Monthly	
79.14 USD							

▼ Pricing strategy		Info		Cost optimized, 1 YR No Upfront	
Pricing model		Contract terms		Monthly	596.52 USD
<input checked="" type="radio"/> Cost optimized		<input type="radio"/> No contract		Monthly	596.52 USD
				Upfront	0.00 USD
		<input checked="" type="radio"/> 1 YR No Upfront		Monthly	543.39 USD
				Upfront	0.00 USD
		<input type="radio"/> On-Demand		Monthly	344.10 USD
				Upfront	2,175.00 USD
		<input type="radio"/> Reserved		Monthly	162.69 USD
				Upfront	4,265.00 USD
		<input type="radio"/> Spot		Monthly	0.00 USD
				Upfront	0.00 USD
		<input type="radio"/> 1 YR Full Upfront		Monthly	371.11 USD
				Upfront	2,500.00 USD
		<input type="radio"/> 1 YR No Upfront - Convertible Reserved Instances		Monthly	162.69 USD
				Upfront	4,905.00 USD
		<input type="radio"/> 1 YR Partial Upfront - Convertible Reserved Instances		Monthly	425.49 USD
				Upfront	0.00 USD
		<input type="radio"/> 5 YR No Upfront		Monthly	425.49 USD
				Upfront	0.00 USD

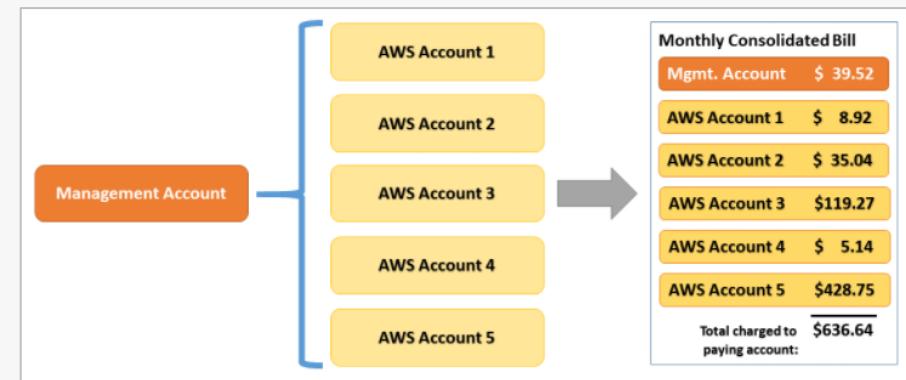
결제 대시보드

- AWS 청구서를 결제하고, 사용량을 모니터링하고, 비용을 분석 및 제어
 - 이번 달 누계 금액을 지난 달과 비교하고 현재 사용량을 기준으로 내달 사용량 예측
 - 서비스별 월 누계 지출 확인
 - 서비스별 프리 티어 사용량 확인
 - Cost Explorer에 액세스해 예산 생성
 - Savings Plans 구매 및 관리
 - AWS 비용 및 사용 보고서 게시



통합 결제

- AWS Organizations는 통합 결제 옵션을 제공
 - 단일 청구서 : 조직의 모든 AWS 계정에 대한 단일 청구서 수령 가능
 - 간편한 추적 : 여러 계정의 요금을 추적하고 비용 및 사용량 데이터 합계를 다운로드
 - ✓ 기본적으로 조직에 허용되는 최대 계정 수는 4개
 - ✓ 필요한 경우 AWS Support에 문의하여 할당량을 확장 가능
 - ✓ 월별 청구서에서 각 계정에서 발생한 항목별 요금을 검토 가능
 - 단일 월별 청구서의 편의성은 유지하면서도 조직의 계정에 대한 투명성을 높임
 - 사용량 결합 : 조직의 계정 전체에서 대량 할인 요금, Savings Plans 및 예약 인스턴스 공유
 - 추가 요금 없음— 추가 비용 없이 통합 결제 제공



AWS Budget



■ AWS 예산 기능

- 예산 작성 및 관리
- 필터를 사용하여 예산 구체화
- 예산에 알림 추가(사용자 지정 알림을 설정)

■ AWS 예산 대시보드

- 예산을 생성하고, 추적하고, 검사할 수 있는 허브
- 예산에 대한 추가 세부 정보 확인
- 월/분기/연 수준으로 예산 생성,
 - ✓ 시작/종료 날짜 사용자 지정 가능
- 예산을 AWS 서비스, 계정, 태그 등 여러 측면의 연결 비용 추적

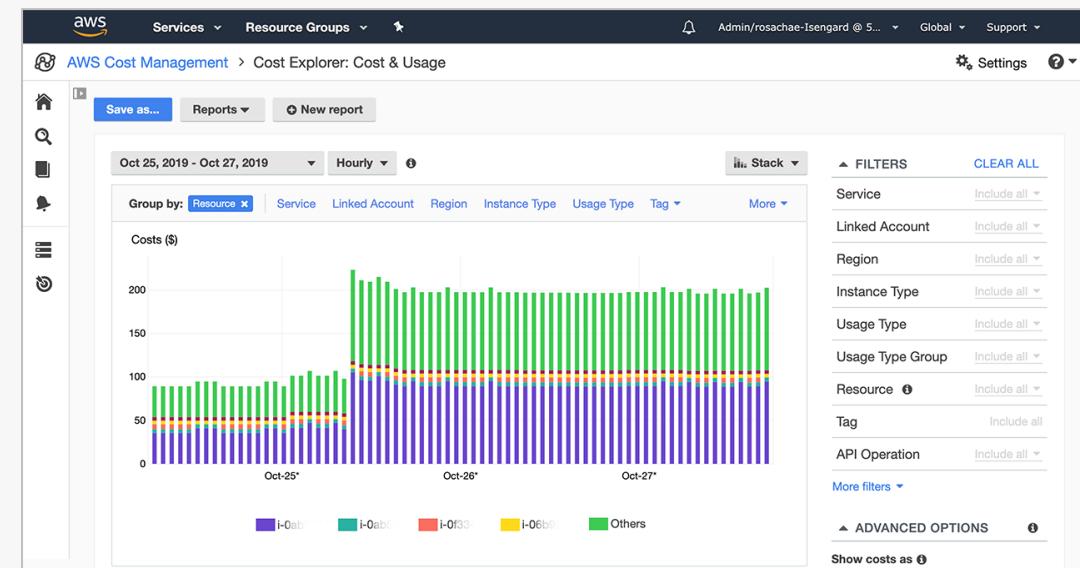
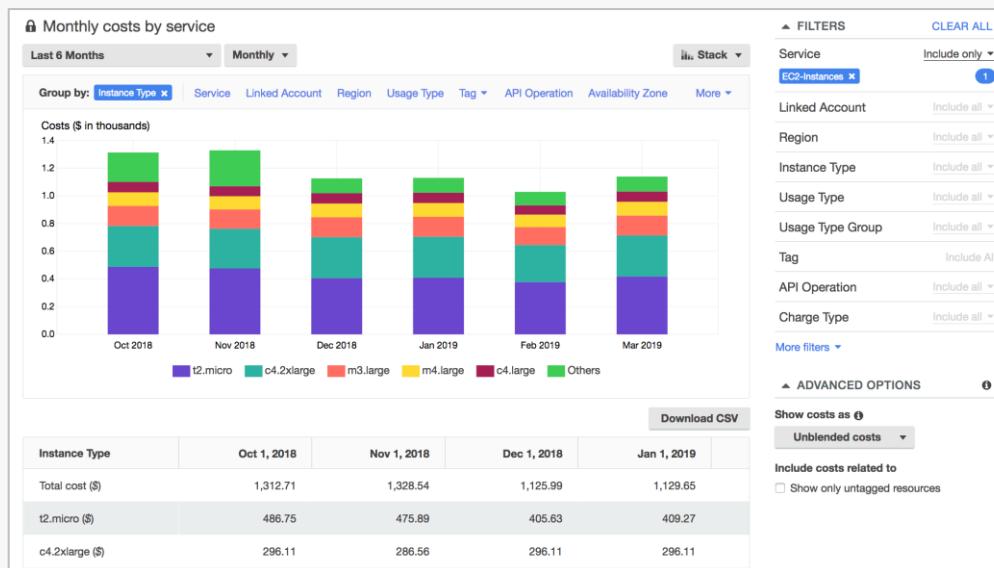
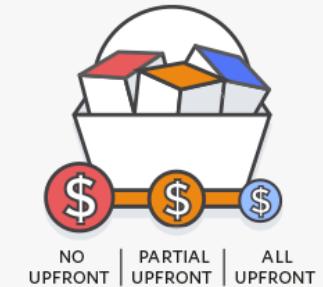
The screenshot shows the AWS Budgets service interface. On the left, there's a navigation menu with options like Dashboard, Bills, Cost Explorer, Budgets (which is highlighted with a red box), Reports, Cost Allocation Tags, Payment Methods, Payment History, Consolidated Billing, Preferences, Credits, and Tax Settings. The main area is titled 'AWS Budgets' and contains a message: 'You currently have no budgets. AWS Budgets lets you quickly create custom budgets that will automatically alert you when your AWS costs or usage exceed, or are forecasted to exceed, the thresholds you set.' Below this message are three cards: 'Create and manage budgets' (with a database icon), 'Refine your budget using filters' (with a user profile icon), and 'Add notifications to your budget' (with a computer monitor icon). A red box surrounds the 'Create a budget' button at the top right.

The screenshot shows the AWS Budgets service interface with the 'All budgets' tab selected. It displays a table of seven budgets, each with columns for Budget name, Budget type, Current, Budgeted, Forecasted, Current vs. budgeted, and Forecasted vs. budgeted. The budgets listed are: Project Nemo Cost Budget (Cost, \$43.90, \$45.00, \$56.33, 97.55%, 125.17%), Eastern US Regional Budget (Cost, \$85.21, \$100.00, \$125.28, 85.21%, 125.28%), Total Monthly Cost Budget (Cost, \$141.50, \$175.00, \$187.00, 80.86%, 106.86%), Total EC2 Cost Budget (Cost, \$136.90, \$200.00, \$195.21, 68.45%, 97.61%), S3 Usage Budget (Usage, 3,601 Requests, 5,500 Requests, 4,675.75 Requests, 65.47%, 85.01%), Monthly DataTransfer Usage Budget (Usage, 2.26 GB, 4 GB, 3.07 GB, 57.05%, 76.63%), and Quarterly Budget (Cost, \$133.10, \$550.00, \$516.10, 24.2%, 93.84%). A red box surrounds the 'Create budget' button at the top right.

All budgets (7)	Cost budgets (5)	Usage budgets (2)	Reservation budgets (0)			
Project Nemo Cost Budget	Cost	\$43.90	\$45.00	\$56.33	97.55%	125.17%
Eastern US Regional Budget	Cost	\$85.21	\$100.00	\$125.28	85.21%	125.28%
Total Monthly Cost Budget	Cost	\$141.50	\$175.00	\$187.00	80.86%	106.86%
Total EC2 Cost Budget	Cost	\$136.90	\$200.00	\$195.21	68.45%	97.61%
S3 Usage Budget	Usage	3,601 Requests	5,500 Requests	4,675.75 Requests	65.47%	85.01%
Monthly DataTransfer Usage Budget	Usage	2.26 GB	4 GB	3.07 GB	57.05%	76.63%
Quarterly Budget	Cost	\$133.10	\$550.00	\$516.10	24.2%	93.84%

AWS Cost Explorer

- 시간 경과에 따라 AWS 비용 및 사용량을 시각화, 이해, 관리할 수 있는 도구
 - 발생 비용 기준 상위 5개 AWS 서비스의 비용 및 사용량에 대한 기본 보고서가 포함
 - 사용자 지정 필터 및 그룹을 적용해 데이터 분석 가능
 - 시간 경과에 따른 AWS 비용 분석을 통해 향후 비용 및 예산 수립에 대한 정보에 입각한 결정 가능



AWS Support Plan

- AWS 서비스를 효율적으로 사용하는 데 도움이 되는 네 가지 Support 플랜을 제공
 - Basic : 무료 제공, 백서 설명서 및 지원 커뮤니티 액세스 포함, AWS Personal Health Dashboard 사용
 - Developer, Business 및 Enterprise Support : 월 단위 비용

- 기술 지원 관리자(TAM)

- TAM이 AWS 측 주 연락 창구
- 권장 사항, 아키텍처 검토 제공
- AWS 서비스 전문 지식 제공
 - ✓ 서비스 통합
 - ✓ 솔루션 설계 지원 등



Technical Support
We're here to help.

Features	Basic Current plan	Developer	Business	Enterprise
Customer service and communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best practices	Access to 7 core Trusted Advisor checks	Access to 7 core Trusted Advisor checks	Access to all Trusted Advisor checks	Access to all Trusted Advisor checks
Health status and Notifications	Access to Personal Health Dashboard	Access to Personal Health Dashboard	Access to Personal Health Dashboard & Health APIs	Access to Personal Health Dashboard & Health APIs
Technical support		Business hours** access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat, and phone	24x7 access to Cloud Support Engineers via email, chat, and phone
Who can open cases		One primary contact/ Unlimited cases	Unlimited contacts/ Unlimited cases (IAM supported)	Unlimited contacts/ Unlimited cases (IAM supported)
Case severity/Response times*		General guidance: < 24 hours System impaired: < 12 hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours

AWS Marketplace



- Independent Software Vendor(ISV)의 소프트웨어 리스팅 수천 개가 포함된 디지털 카탈로그
 - AWS에서 실행되는 소프트웨어를 검색하고 평가하고 구매
 - 각 리스팅에 대해 요금 옵션, 사용 가능한 지원 및 다른 AWS 고객의 리뷰 등 자세한 정보에 액세스
 - 산업 및 사용 사례별로 소프트웨어 솔루션을 탐색
- AWS Marketplace 범주
 - 각 범주에서 하위 범주의 상품 리스팅을 탐색하여 검색 범위를 좁힐 수 있음

Find AWS Marketplace products that meet your needs.

Categories Vendors Pricing Plans Delivery Methods

All categories All vendors All pricing plans All delivery methods

Over 10,000 results Clear selection View results

Popular Categories

 Operating Systems	 Security	 Networking	 Storage	 Data Products
 Data Analytics	 Dev Ops	 Machine Learning	 View all categories	

Module 9

マイグレーション

- AWS 클라우드 마이그레이션
- AWS Cloud Adoption Framework
- 클라우드 마이그레이션 전략의 6가지 핵심 요소
- AWS 데이터 마이그레이션 솔루션: AWS Snowcone, AWS Snowball, AWS Snowmobile
- AWS 제공 혁신 솔루션

Cloud Adoption Framework

- AWS CAF는 지침을 6가지 초점 영역(관점)으로 구성 : 각 관점은 별개의 책임을 해결
 - 계획 프로세스는 조직 전체에서 적합한 인물들이 앞으로의 변화에 대비할 수 있도록 함

비즈니스 관점	비즈니스 기능	<ul style="list-style-type: none">✓ IT가 비즈니스 요구 사항을 반영하고 IT 투자가 주요 비즈니스 결과와 연계되도록 보장✓ 클라우드 채택을 위한 강력한 비즈니스 사례를 설정하고 클라우드 채택 이니셔티브의 우선 순위를 지정<ul style="list-style-type: none">• 비즈니스 전략 및 목표가 IT 전략 및 목표에 부합하는지 확인	<ul style="list-style-type: none">• 비즈니스 관리자• 재무 관리자, 예산 소유자• 전략 이해당사자
인력 관점		<ul style="list-style-type: none">✓ 클라우드 채택을 성공하기 위한 조직 전반의 변화 관리 전략 개발 지원✓ 조직 구조 및 역할, 새로운 기술 및 프로세스 요구 사항을 평가하고 격차 파악<ul style="list-style-type: none">• 이를 통해 교육, 인력 배치 및 조직 변화의 우선 순위를 지정	<ul style="list-style-type: none">• 인사 관리• 인력 배치• 인력 관리자
거버넌스 관점		<ul style="list-style-type: none">✓ IT 전략이 비즈니스 전략에 부합하도록 조정하는 기술 및 프로세스에 중점✓ 클라우드에서 비즈니스 거버넌스를 보장에 필요한 직원 기술 및 프로세스를 업데이트하는 방법 이해<ul style="list-style-type: none">• 클라우드 투자를 관리하고 측정하여 비즈니스 성과를 평가	<ul style="list-style-type: none">• 최고 정보 책임자(CIO)• 프로그램/포트폴리오 관리자• 엔터프라이즈 아키텍트• 비즈니스 분석가
플랫폼 관점	기술 역량 중점	<ul style="list-style-type: none">✓ 클라우드를 기반의 새 솔루션을 구현하고 온프레미스 워크로드를 클라우드로 마이그레이션하기 위한 원칙과 패턴 포함✓ 다양한 아키텍처 모델을 사용하여 IT 시스템의 구조와 그 관계를 이해하고 전달	<ul style="list-style-type: none">• 최고 기술 책임자(CTO)• IT 관리자• 솔루션 아키텍트
보안 관점		<ul style="list-style-type: none">✓ 조직이 가시성, 감사 가능성, 제어 및 민첩성에 대한 보안 목표를 충족하도록 보장✓ AWS CAF를 사용하여 조직의 요구 사항에 맞춰 보안 제어의 선택 및 구현 구성	<ul style="list-style-type: none">• 최고 정보 보안 책임자(CISO)• IT 보안 관리자/분석가
운영 관점		<ul style="list-style-type: none">✓ 비즈니스 이해당사자와 합의된 수준까지 IT 워크로드를 구현, 실행, 사용, 운영 및 복구하는 데 도움✓ 일별, 분기별 및 연간으로 비즈니스를 수행하는 방법을 정의✓ 이해당사자가 현재 운영 절차를 정의하고 성공적인 클라우드 채택 구현에 필요한 프로세스 변경 및 교육을 파악	<ul style="list-style-type: none">• IT 운영 관리자• IT 지원 관리자

マイグ레이션 전략



- 애플리케이션을 클라우드로 마이그레이션할 때 구현할 수 있는 가장 일반적인 6가지 마이그레이션 전략

리호스팅(Rehosting)	<ul style="list-style-type: none">✓ 리프트 앤 시프트(lift-and-shift)✓ 애플리케이션을 변경 없이 이전✓ 마이그레이션을 신속하게 하여 비즈니스 사례를 충족하기 원하는 대규모 레거시 마이그레이션의 시나리오
리플랫포밍(Replatforming)	<ul style="list-style-type: none">✓ 리프트 앤 시프트 및 수정(lift, tinker, and shift)✓ 실질적인 이점을 실현하기 위해 몇 가지 클라우드 최적화 수행✓ 최적화는 애플리케이션의 핵심 아키텍처를 변경하지 않고 달성
리팩터링(Refactoring)/ 아키텍처 재설계(Re-architecting)	<ul style="list-style-type: none">✓ 클라우드 네이티브 기능을 사용하여 애플리케이션을 설계하고 개발하는 방식을 재구성<ul style="list-style-type: none">• 기존 환경의 애플리케이션에서 구현이 어려운 기능 추가/ 확장 또는 성능 개선이 필요할 때
재구매(Repurchasing)	<ul style="list-style-type: none">✓ 기존 라이선스를 Software-as-a-Service 모델로 전환
유지(Retaining)	<ul style="list-style-type: none">✓ 비즈니스에 중요한 애플리케이션을 소스 환경에 유지<ul style="list-style-type: none">• 마이그레이션하려면 대규모 리팩토링이 필요한 애플리케이션• 연기할 수 있는 워크로드
폐기(Retiring)	<ul style="list-style-type: none">✓ 더 이상 필요하지 않은 애플리케이션을 제거하는 프로세스

AWS Snow 패밀리 멤버



- AWS와 고객 간에 최대 엑사바이트 규모의 데이터를 물리적으로 이동할 수 있는 물리적 디바이스 모음
 - AWS Snow 패밀리는 AWS Snowcone, AWS Snowball 및 AWS Snowmobile로 구성
 - ✓ 각각 다른 용량 포인트를 제공하며 대부분 내장 컴퓨팅 기능을 포함
 - ✓ AWS는 Snow 패밀리 디바이스를 소유 및 관리하고 AWS 보안, 모니터링, 스토리지 관리 및 컴퓨팅 기능과 통합

Snowball	Snowball Edge	Snowmobile
<ul style="list-style-type: none">✓ 작고 견고하며 안전한 옛지 컴퓨팅 및 데이터 전송 디바이스- CPU 2개, 4GB 메모리- 8TB의 가용 스토리지- 10G 네트워크- 엔드 투 엔드 암호화- 방진, 방수	<ul style="list-style-type: none">✓ Snowball Edge Storage Optimized 디바이스<ul style="list-style-type: none">- 대규모 데이터 마이그레이션 및 반복 전송 워크플로와 큰 용량이 필요한 로컬 컴퓨팅- 40개 vCPU, 80GB 메모리- 80TB HDD, 1TB SATA SSD✓ Snowball Edge Compute Optimized<ul style="list-style-type: none">- 기계 학습, 풀 모션 비디오 분석, 분석 및 로컬 컴퓨팅 스택을 위한 강력한 컴퓨팅 리소스- 52개 vCPU, 208GB 메모리 등- 42TB HDD, 7.68TB SATA SSD	<ul style="list-style-type: none">✓ 대용량 데이터를 AWS로 이동하는 데 사용하는 엑사바이트 규모의 데이터 전송 서비스✓ 세미 트레일러 트럭으로 견인되는 45피트 길이의 견고한 운반 컨테이너인 Snowmobile 1대당 최대 100페타바이트의 데이터를 전송- GPS 트래킹- 알람 모니터링- 24/7 가동

AWS 서비스를 통한 혁신

- AWS 서비스를 사용하는 방식을 살펴볼 때는 원하는 결과에 집중하는 것이 중요
- 다음 상태를 명확하게 설명할 수 있어 함
 - 현재 상태
 - 원하는 상태
 - 해결하려는 문제
- 클라우드 여정을 지속하면서 탐색할 수 있는 몇 가지 경로

서비스 애플리케이션	인공 지능	기계 학습
<ul style="list-style-type: none">✓ AWS Lambda는 서비스 애플리케이션을 실행하는 데 사용할 수 있는 서비스✓ 서비스 애플리케이션을 사용하여 아키텍처를 구축하면 개발자는 서버를 관리하고 운영하는 대신 핵심 제품에 집중   	<ul style="list-style-type: none">✓ AWS는 인공 지능(AI)을 기반으로 하는 다양한 서비스를 제공✓ Amazon Transcribe : 음성을 텍스트로 변환✓ Amazon Comprehend : 텍스트 패턴 검색✓ Amazon Fraud Detector : 잠재적인 온라인 사기 행위를 식별✓ Amazon Lex : 음성 및 텍스트 챗봇 빌드    	<ul style="list-style-type: none">✓ 기존의 기계 학습(ML) 개발은 복잡, 고비용, 오랜 시간 및 오류 발생✓ AWS는 ML 모델을 신속하게 빌드, 훈련, 배포에 사용할 수 있는 SageMaker를 제공✓ ML을 사용해 데이터를 분석하고, 복잡한 문제를 해결하고, 아직 발생하기 전에 결과를 예측 가능    

Module 10

클라우드로의 여정

- AWS Well-Architected 프레임워크
- AWS Well-Architected 5가지 핵심 요소
- 클라우드 컴퓨팅의 6가지 이점

AWS Well-Architected 프레임워크

- AWS에서 안정적, 안전하며 효율적이며, 비용 효율적인 시스템을 설계하고 운영하는 방법
- 모범 사례 및 설계 원칙에 따라 아키텍처를 지속적으로 측정하고 개선할 영역을 파악
- 5가지 핵심 원칙

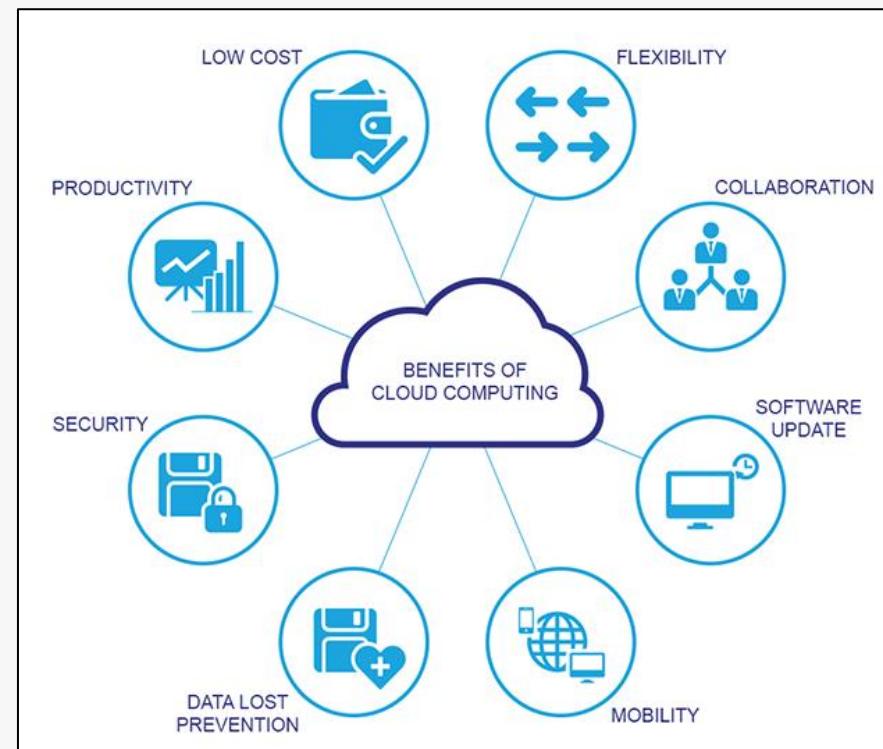


운영 우수성		<ul style="list-style-type: none">✓ 시스템을 실행/모니터링하여 비즈니스 가치를 제공하고 지원 프로세스 및 절차를 지속적으로 개선하는 능력✓ 코드로 작업 수행, 문서에 주석 추가, 실패 예측, 되돌릴 수 있는 소규모 변경을 자주 수행
보안성		<ul style="list-style-type: none">✓ 위험 평가 및 완화 전략을 통해 비즈니스 가치를 제공하는 동시에 정보, 시스템, 자산을 보호하는 능력<ul style="list-style-type: none">• 가능한 한 보안 모범 사례를 자동화• 모든 계층에 보안을 적용• 전송 중/저장 시 데이터를 보호
안정성		<ul style="list-style-type: none">✓ 복구 절차 테스트, 전체 시스템 가용성을 높이기 위한 수평 확장, 장애 발생 시 자동 복구가 포함<ul style="list-style-type: none">• 인프라 또는 서비스 중단으로부터 복구• 컴퓨팅 리소스를 동적으로 확보하여 수요를 충족• 잘못된 구성 또는 일시적인 네트워크 문제와 같은 중단 완화
성능 효율성		<ul style="list-style-type: none">✓ 리소스를 효율적으로 사용하고 시스템 요구사항을 만족시키고 수요 변화와 기술 진화에 따라 효율성을 유지하는 능력✓ 실험 빈도 증가, 서비스 아키텍처 사용, 몇 분 만에 전 세계 배포가 가능 시스템 설계 등이 포함
비용 최적화		<ul style="list-style-type: none">✓ 가장 낮은 가격으로 비즈니스 가치를 제공하도록 시스템을 실행하는 능력✓ 소비 모델 채택, 비용 분석 및 귀속, 관리형 서비스를 사용하여 소유 비용 절감이 포함

클라우드 컴퓨팅

❖ 클라우드 컴퓨팅의 이점

- **선행 비용을 가변 비용으로 대체**
 - ✓ 사용하는 컴퓨팅 리소스에 대해서만 비용을 지불
- **데이터 센터 운영 및 유지 관리에 비용 투자 불필요**
 - ✓ 인프라 작업에 신경을 덜 쓰고 애플리케이션과 고객에 집중
- **용량 추정 불필요**
 - ✓ 필요한 용량만 사용 가능, 수요에 따라 용량을 확장 또는 축소 가능
- **규모의 경제**
 - ✓ 인프라를 소유할 때보다 가변 비용이 낮아짐
- **속도 및 민첩성 향상**
 - ✓ 몇 분 만에 새로운 리소스에 액세스 가능 → 유연성 증가
- **몇 분 만에 전 세계에 배포 가능**
 - ✓ 신속한 배포 및 짧은 지연 시간 제공



thank
you

