aws re/start

AWS 공동 책임 모델

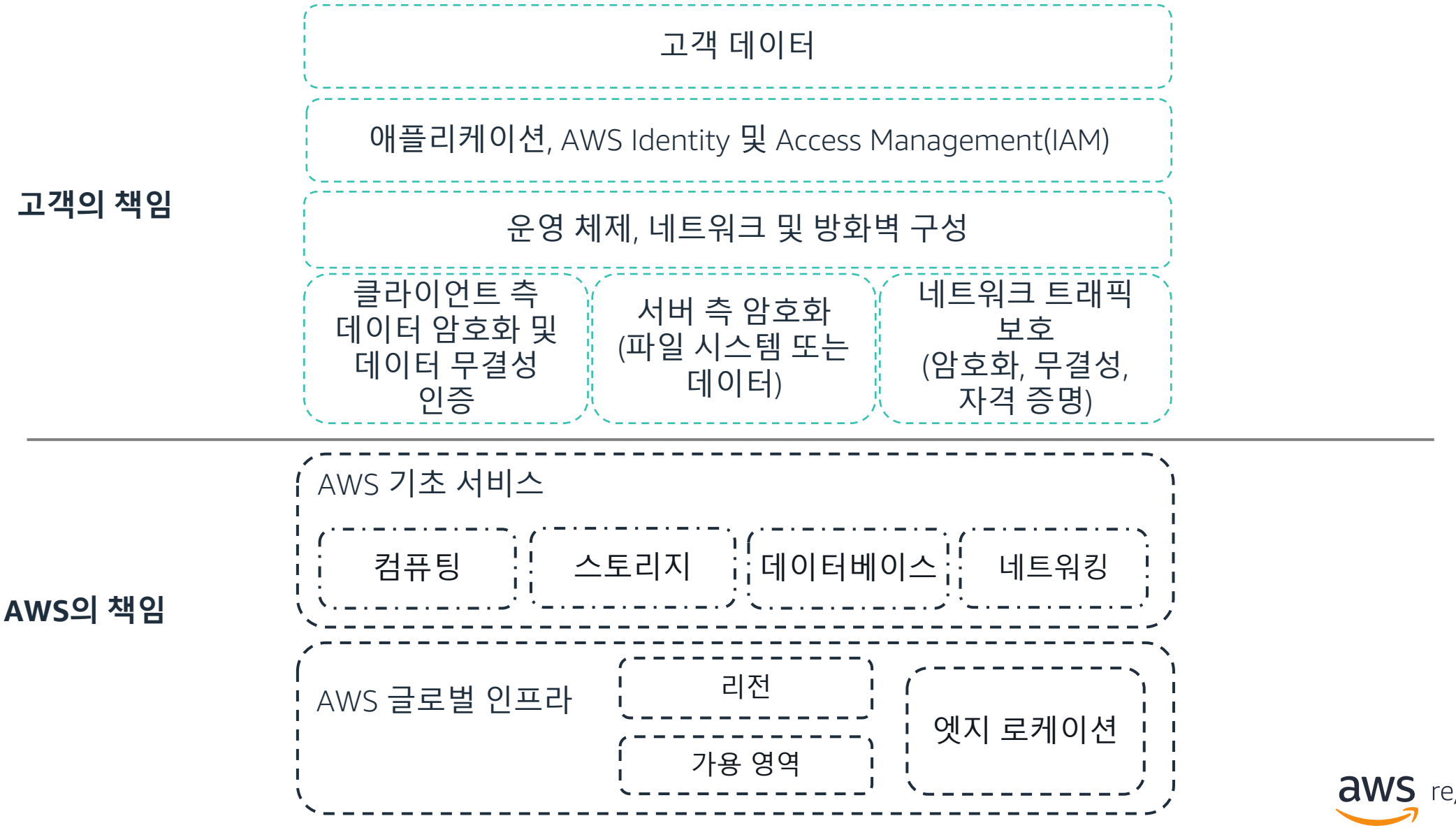
학습 내용

강의의 핵심

학습 내용은 다음과 같습니다.

- AWS Cloud 보안 및 공동 책임 모델 설명
- AWS와 고객의 보안 책임을 구별

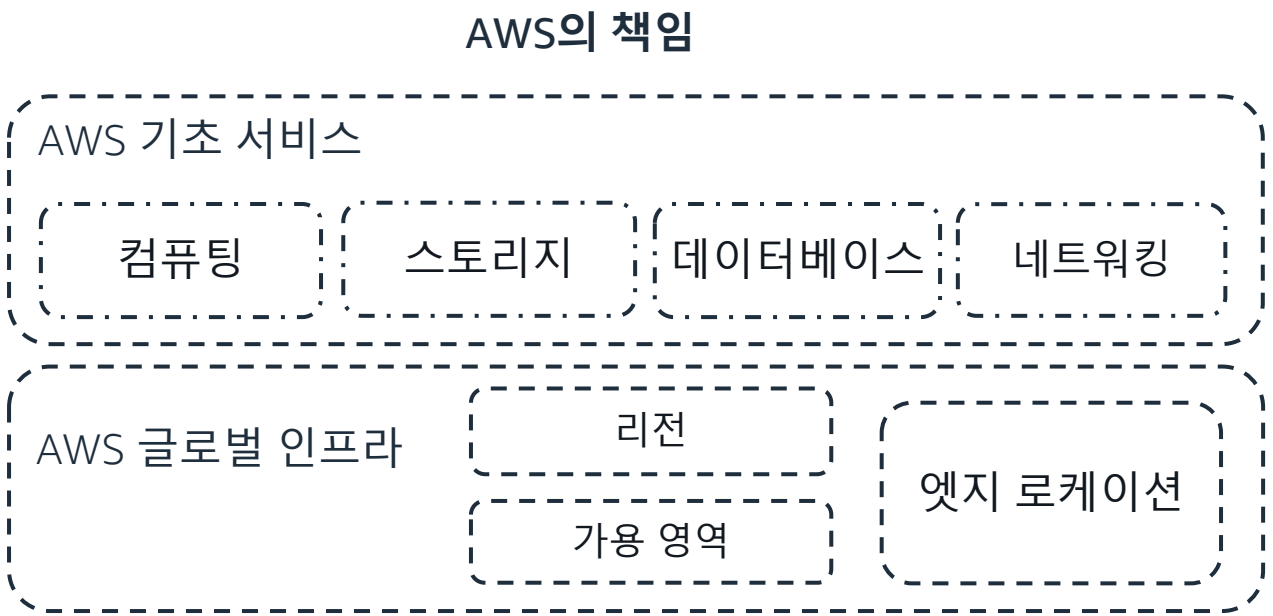
공동 책임 모델



AWS 보안 책임: 클라우드 **자체의** 보안

클라우드 자체의 보안

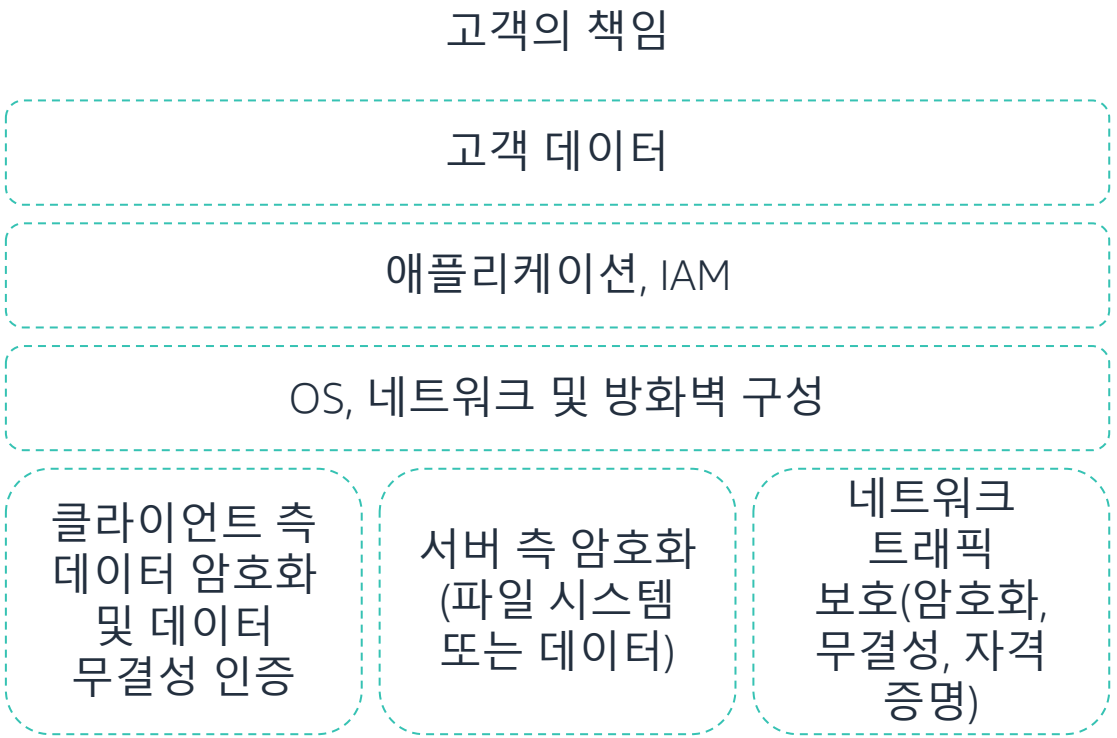
- 데이터 센터의 물리적 보안 -
  - 필요 기반의 통제된 출입 관리
- 하드웨어 및 소프트웨어 인프라 -
  - 스토리지 폐기, 호스트 운영 체제(OS) 액세스 로깅 및 감사
- 네트워크 인프라 -
  - 침입 탐지
- 가상화 인프라 -
  - 인스턴스 격리



사용자 보안 책임: 클라우드 **내부** 보안

클라우드 내부의 보안

- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 OS
  - 패치 적용, 유지 관리 등
- 애플리케이션
  - 암호, 역할 기반 액세스 등
- 보안 그룹 구성
- OS 또는 호스트 기반 방화벽
  - 침입 탐지 또는 차단 시스템 등
- 네트워크 구성
- 계정 관리
  - 각 사용자에 대한 로그인 및 권한 설정



aws re/start

서비스 특성 및 보안 책임

고객이 관리하는 서비스의 예

Amazon EC2

Amazon Elastic Block Store (Amazon EBS)

Amazon Virtual Private Cloud (Amazon VPC)

서비스형 인프라(IaaS)

- 고객은 네트워킹 및 스토리지 설정을 보다 유연하게 구성할 수 있음
- 고객은 보안의 더 많은 측면을 관리해야 함
- 고객이 액세스 제어를 구성

AWS에서 관리하는 서비스의 예

AWS Lambda

Amazon Relational Database Service (Amazon RDS)

AWS Elastic Beanstalk

서비스형 플랫폼(PaaS)

- 고객이 기본 인프라를 관리할 필요가 없음
- 운영 체제, 데이터베이스 패치 적용, 방화벽 구성 및 재해 복구(DR)를 AWS가 처리
- 고객은 코드 또는 데이터 관리에 집중할 수 있음

서비스 특성 및 보안 책임(계속)

SaaS의 예


AWS Trusted Advisor


AWS Shield


Amazon Chime

서비스형 소프트웨어(SaaS)

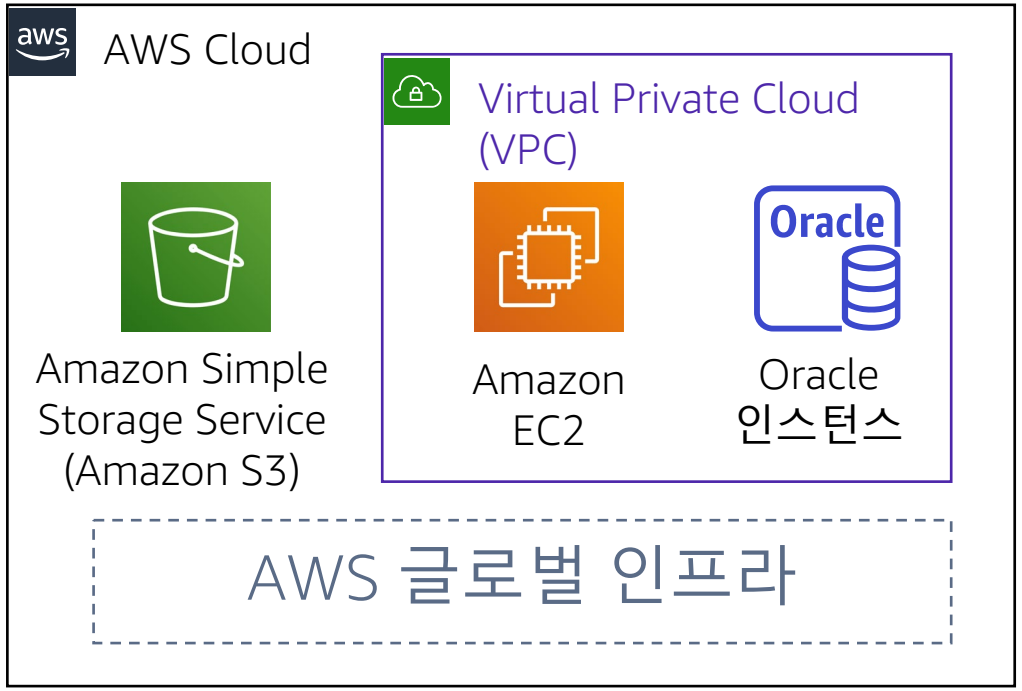
- 중앙에서 소프트웨어를 호스팅
- 구독 모델 또는 종량제 기준으로 라이선스 부여
- 일반적으로 웹 브라우저, 모바일 앱 또는 애플리케이션 프로그래밍 인터페이스(API)를 통해 서비스에 액세스
- 고객은 서비스를 지원하는 인프라를 관리할 필요가 없음

활동: AWS 공동 책임 모델

aws re/start

활동 시나리오

다음 배포에서 책임은 AWS와 고객 중 누구에게 있나요?



1. EC2 인스턴스의 운영 체제에 대한 업그레이드 및 패치
   - **답**: 고객
2. 데이터 센터의 물리적 보안
   - **답**: AWS
3. 가상화 인프라
   - **답**: AWS
4. Amazon EC2 보안 그룹 설정
   - **답**: 고객
5. EC2 인스턴스에서 실행되는 애플리케이션의 구성
   - **답**: 고객
6. Oracle 인스턴스가 Amazon RDS 인스턴스로 실행되는 경우 Oracle 업그레이드 또는 패치
   - **답**: AWS
7. Oracle이 EC2 인스턴스에서 실행되는 경우 Oracle 업그레이드 또는 패치
   - **답**: 고객
8. S3 버킷 액세스 구성
   - **답**: 고객

핵심 요점

- AWS와 고객은 보안 책임을 공유
  - AWS는 클라우드 **자체의** 보안을 담당
  - 고객은 클라우드 **내부의** 보안을 담당
- **AWS**는 하드웨어, 소프트웨어, 네트워킹 및 시설 등 AWS Cloud 서비스에서 실행되는인프라의 보호를 담당
- 서비스형 인프라(IaaS)로 분류되는 서비스의 경우 고객은 필요한 보안 구성 및 관리 작업 수행을 담당
  - 예: 게스트 OS 업데이트 및 보안 패치, 방화벽, 보안 그룹 구성