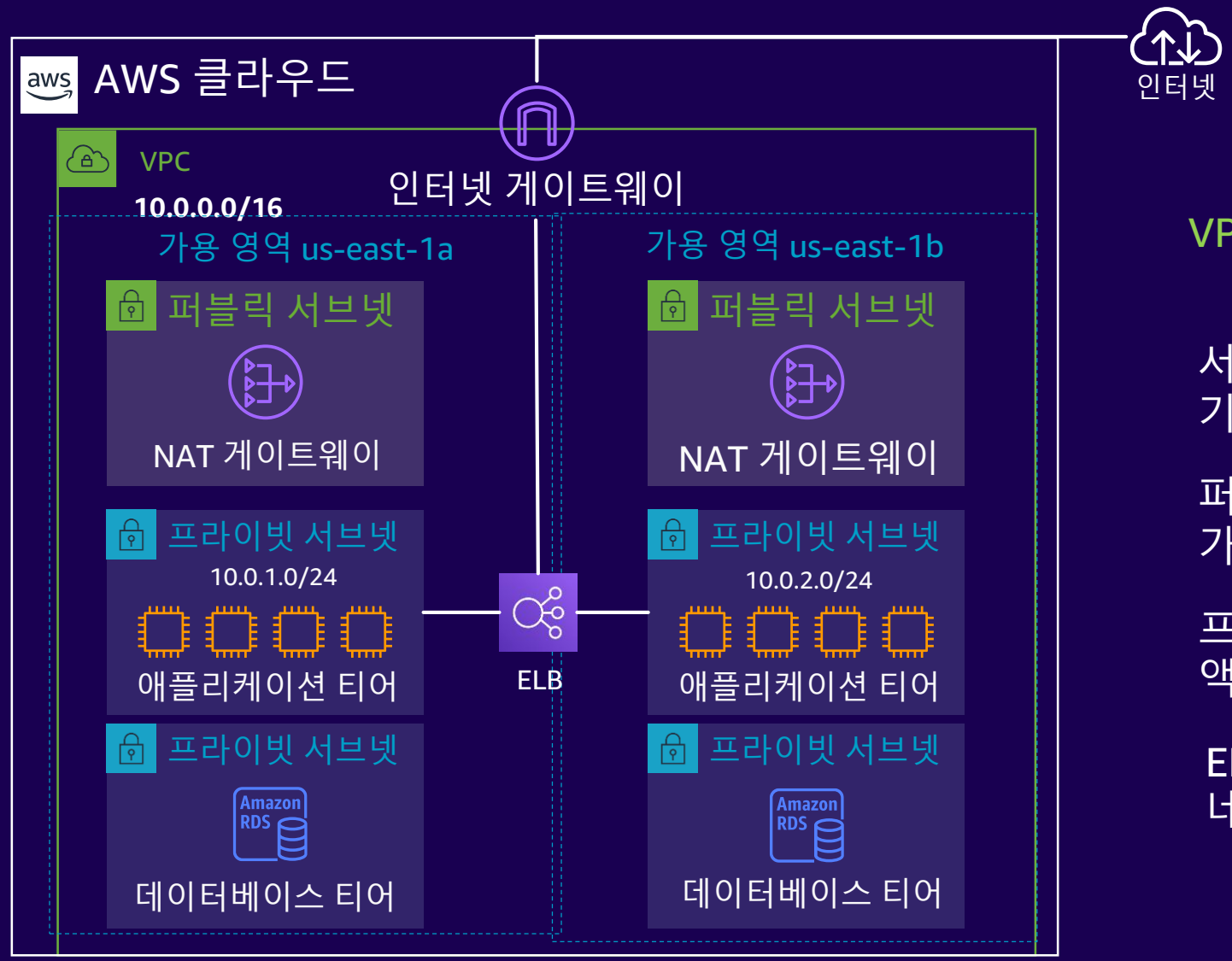
네트워킹

엄혜주
테크니컬 트레이너. AWS

Amazon Virtual Private Cloud(Amazon VPC)



VPC: AWS Cloud의 개인 네트워크 공간

서브넷: 워크로드를 네트워크에서 격리하는 기능 제공

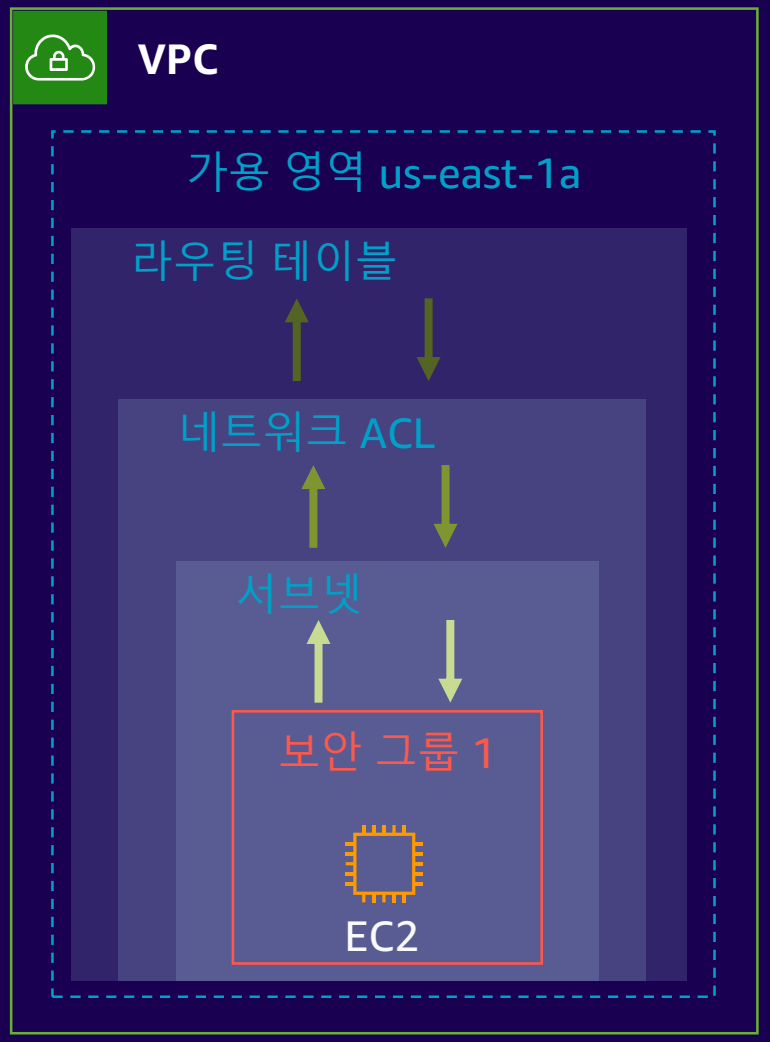
퍼블릭 서브넷: 공용 인터넷에서 직접 액세스 가능

프라이빗 서브넷: 공용 인터넷에서 직접 액세스할 수 없음

ELB: 로드 밸런서가 수신되는 애플리케이션 네트워크 트래픽을 분산시킴

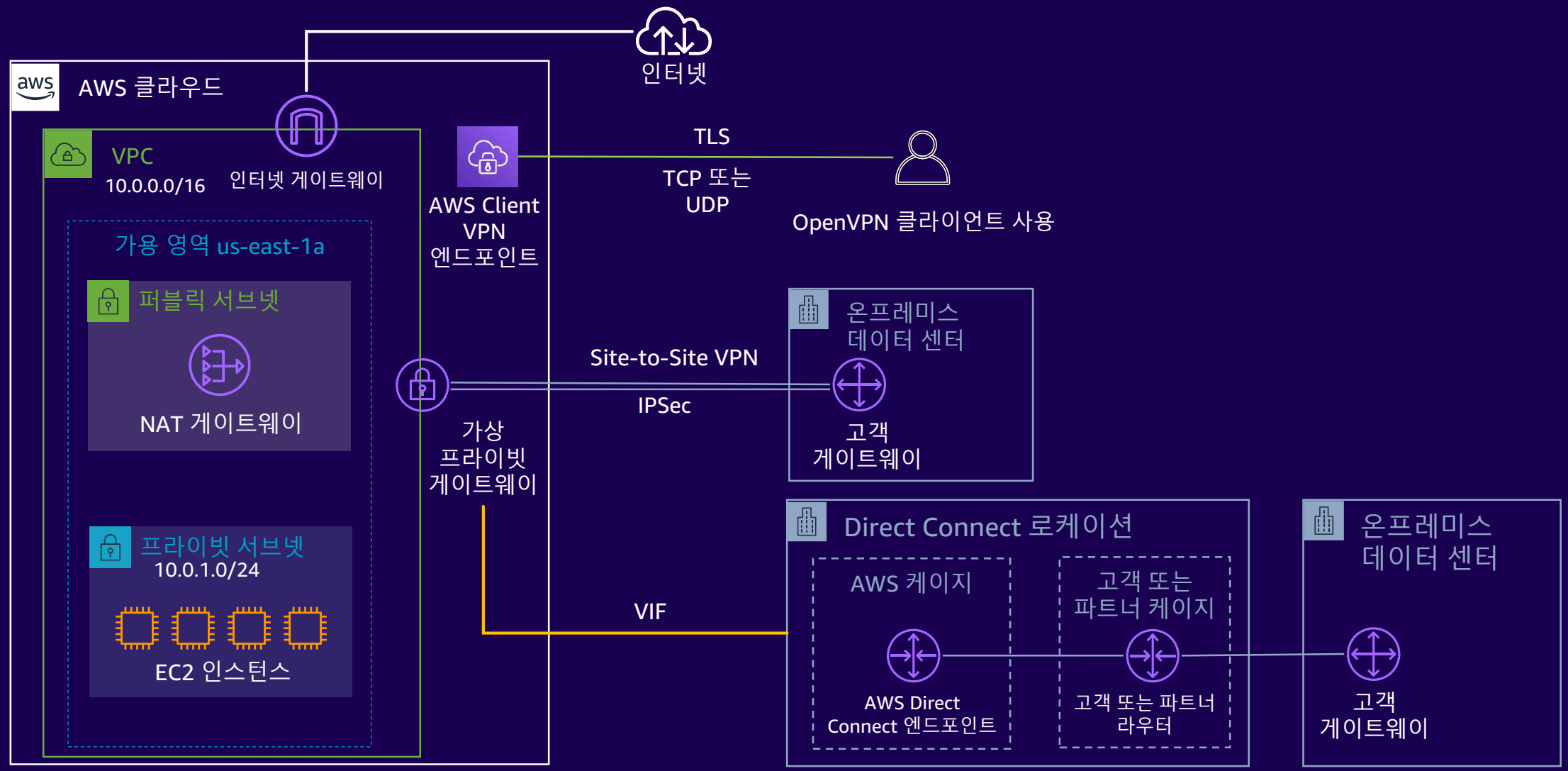
ELB Demo.mp4 (2m 30s)

인프라 보안



- **라우팅 테이블**
  - 네트워크 트래픽이 전달되는 위치를 결정하는 데 사용되는 경로라는 규칙 집합 포함
  - 라우팅 테이블은 VPC, 게이트웨이 및 서브넷과 연결 가능
- **네트워크 액세스 제어 목록(네트워크 ACL)**
  - 서브넷과 주고받는 트래픽 허용 또는 거부
  - 서브넷 수준에서 2차 방어 계층으로 보안 강화
- **보안 그룹**
  - 네트워크 인터페이스(인스턴스) 수준에서 수신 및 발신되는 트래픽을 허용하기 위해 사용
  - 일반적으로 애플리케이션 개발자가 관리함

인프라와 연결



지식 확인

다음 중 VPC의 네트워크 방어 계층은 무엇인가?(3개 선택)

A. Amazon Machine Images(AMI)
B. 네트워크 액세스 제어 목록(서브넷 수준)
C. 보안 그룹(인스턴스 수준)
D. S3 수명 주기 정책
E. VPC 라우팅 테이블

지식 확인

다음 중 VPC의 네트워크 방어 계층은 무엇인가?(3개 선택)

~~A. Amazon Machine Images(AMI)~~

B. 네트워크 액세스 제어 목록(서브넷 수준)

C. 보안 그룹(인스턴스 수준)

~~D. S3 수명 주기 정책~~

E. VPC 라우팅 테이블

정답: B, C, E

핵심 사항

Amazon VPC는 다음을 제공합니다.

- 애플리케이션 시작을 위한 논리적으로 격리된 네트워크
- 배포를 보호하는 보안 그룹, 네트워크 ACL 및 라우팅 테이블

고객이 AWS에 연결하는 주요 방법은 세 가지입니다.

- Client VPN
- Site-to-Site VPN
- Direct Connect

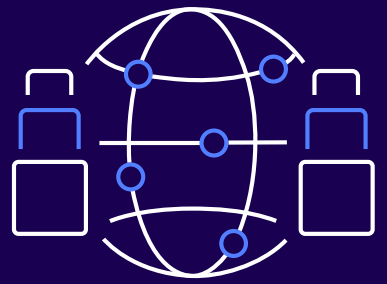
보안

보안이 최우선

보안 위주
설계

지속적인
모니터링

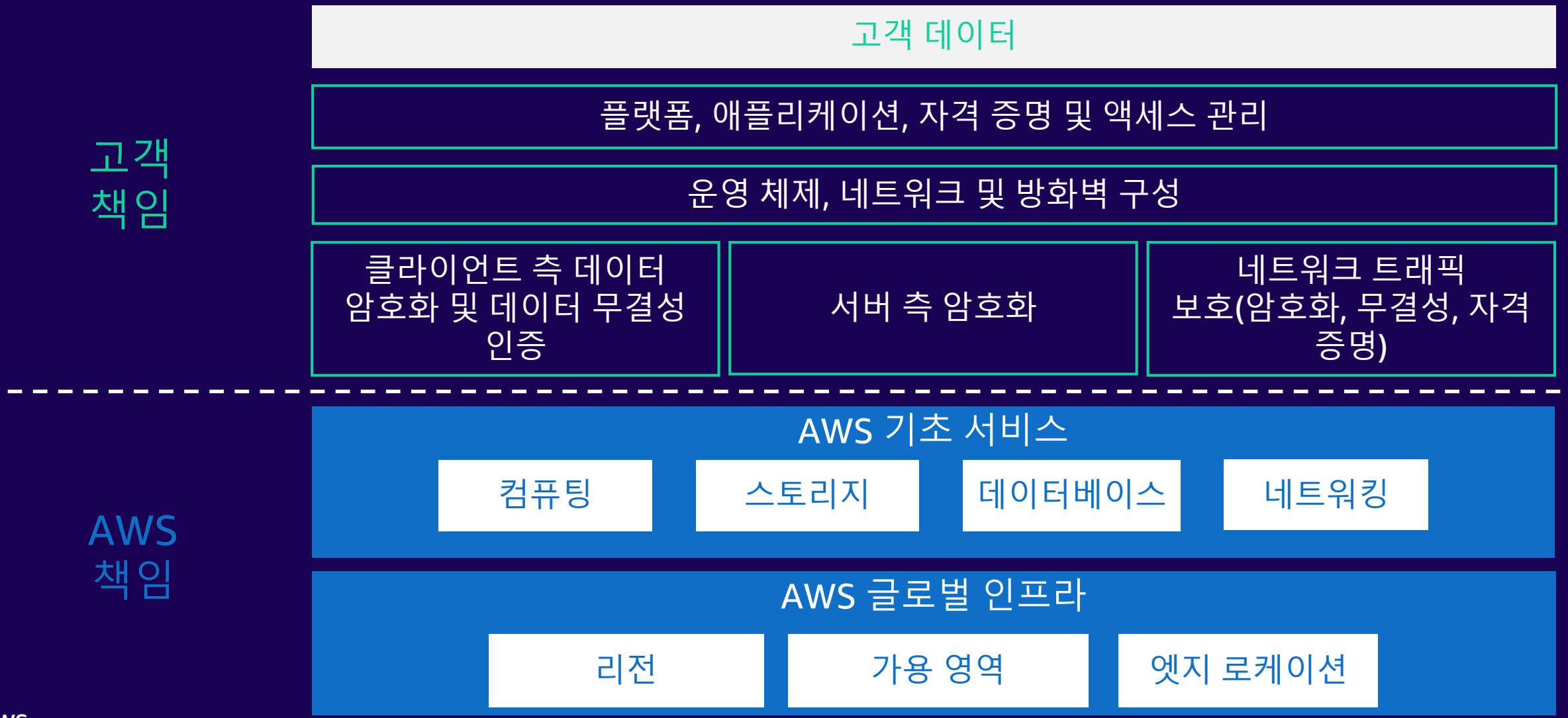
높은
자동화 수준



높은
가용성

많은
인증

공동 책임 모델



AWS Identity and Access Management(IAM)

AWS 리소스에 대한 액세스를 안전하게 제어

- 사용자, 그룹 또는 역할에 세분화된 권한 할당
- AWS 계정에 대한 임시 액세스 공유
- 회사 네트워크의 사용자 연동 또는 인터넷 자격 증명 공급자와 연동

IAM 구성 요소

서비스 제어

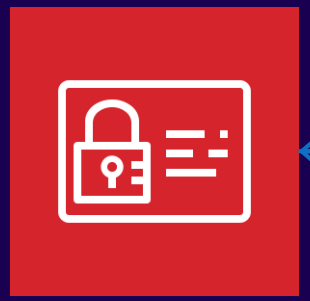
사용자
AWS와 상호 작용하는 사람 또는 애플리케이션

그룹
동일한 권한을 가진 사용자 집단

역할
엔터티가 보유할 수 있는 임시 권한

권한

정책



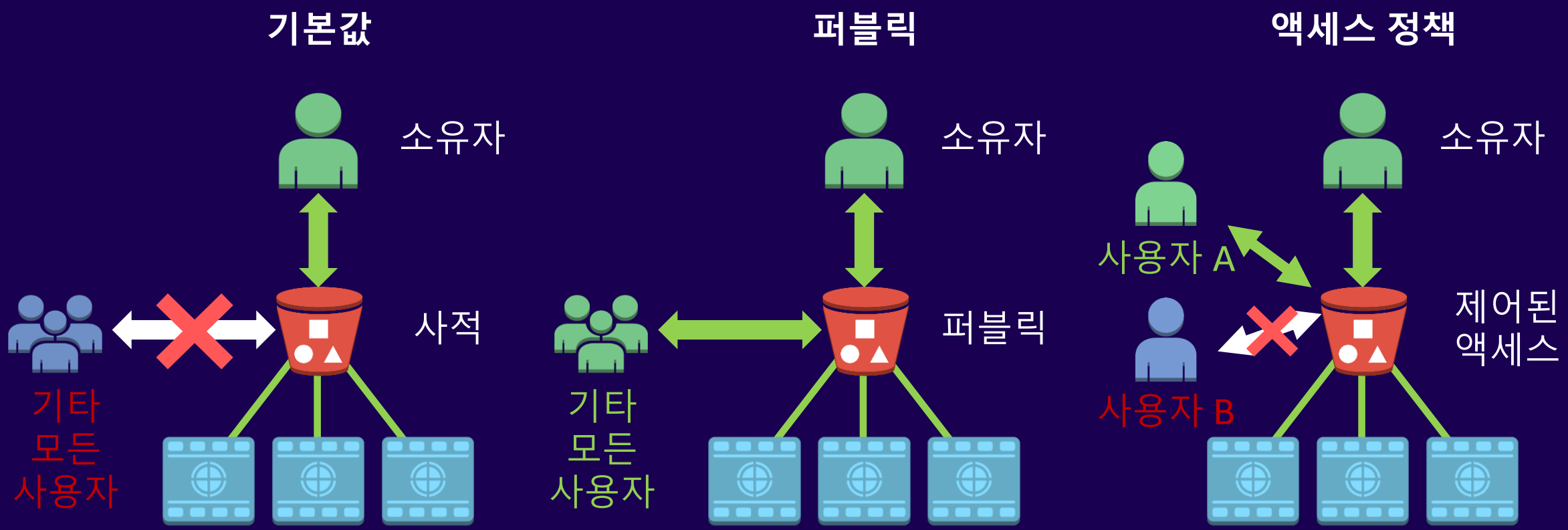
IAM

권한을 정의하여 사용자가 액세스할 수 있는 AWS 리소스 제어

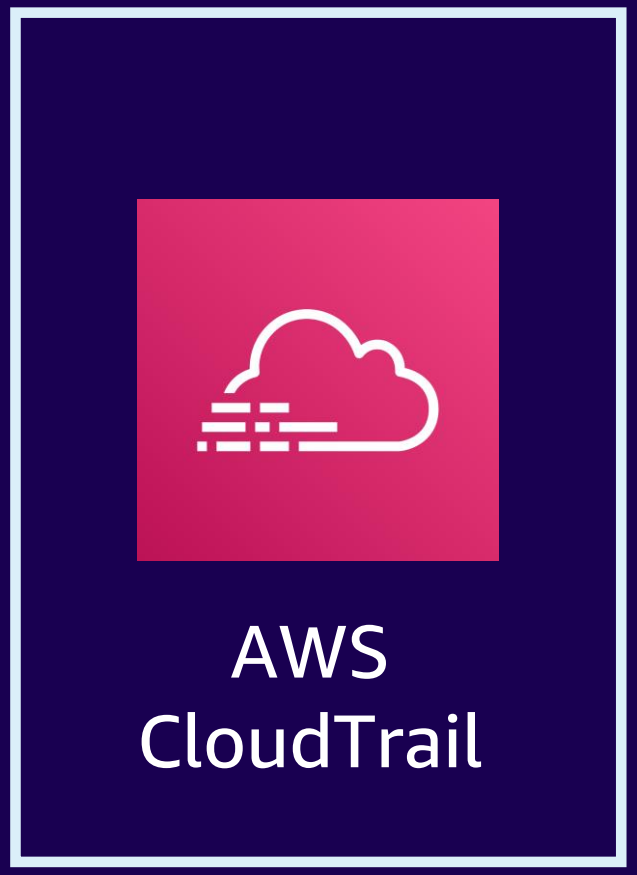
자격 증명 및 액세스 제어 기준 충족 지원
- 인증
- 권한 부여

Amazon S3 액세스 제어: 일반

일부 서비스는 S3 버킷 정책과 같은 리소스 기반 정책을 지원합니다.



AWS CloudTrail



AWS 계정의 사용자 활동 및 API 사용 추적

- 지속적으로 사용자 활동을 모니터링하고 API 호출을 기록
- 규정 준수 감사, 보안 분석, 문제 해결에 유용
- 로그 파일은 Amazon S3 버킷으로 전송됨

API 보안 관련 정보

AWS Trusted Advisor란 무엇입니까?

비용 절감, 성능 향상 및 보안 개선에 도움이 되는 방법을 안내하는 서비스

$7,516.87
잠재적 월별 절감액

지식 확인

다음 중 AWS IAM의 구성 요소인 것은 무엇인가?

A. 그룹 - 동일한 권한을 가진 사용자 집단
B. 버킷 - 저장된 객체를 담는 컨테이너
C. 사용자 - AWS와 상호 작용하는 사람 또는 애플리케이션
D. 인스턴스 - 가상 서버로 실행되는 AMI의 복사본
E. 정책 - 하나 이상의 권한으로 구성된 공식 스테이트먼트

지식 확인

다음 중 AWS IAM의 구성 요소인 것은 무엇인가?

A. 그룹 - 동일한 권한을 가진 사용자 집단

~~B. 버킷 – 저장된 객체를 담는 컨테이너~~

C. 사용자 - AWS와 상호 작용하는 사람 또는 애플리케이션

~~D. 인스턴스 – 가상 서버로 실행되는 AMI의 복사본~~

E. 정책 - 하나 이상의 권한으로 구성된 공식 스테이트먼트

정답: A, C, E

핵심 사항

- 보안은 모두의 책임
  - 클라우드 내 보안/클라우드의 보안
- IAM을 통해 사용자는 AWS 리소스에 대한 액세스 제어 가능
  - 사용자, 그룹 및 역할에 정책 적용
- S3 버킷을 만들면 버킷이 기본적으로 PRIVATE으로 설정
- CloudTrail은 AWS에서 API 호출을 기록
  - 누가, 무엇을, 언제, 어디서
- AWS Trusted Advisor가 권장 사항 제안
  - 비용 절감, 성능 향상 및 보안 개선에 기여