



Module 5 - AWS security

🕒 Created At	@Dec 28, 2020 6:08 PM
👤 Person	👤 하 상엽
☰ Tags	
🕒 Updated At	@Dec 29, 2020 10:18 AM
👤 마지막 수정	👤 송 용석
📅 발표일	@Dec 29, 2020
👤 발표자	👤 하 상엽
🗳 분류	스터디
👤 작성자	👤 하 상엽
👤 참석 인원	
☰ 태그	AWS Cloud Practitioner Essentials
☰ 프로젝트	

AWS Security

AWS는 높은 가용성과 신뢰성을 제공하며, 확장 가능한 클라우드 컴퓨팅 플랫폼을 제공하며, 이를 통해 고객들이 다양한 애플리케이션을 실행할 수 있는 수단을 제공한다.

AWS Security는 시스템과 데이터의 기밀성, 무결성 가용성을 지키는 것을 최우선으로 한다.

데이터를 안전하게 유지

기존 데이터 센터의 자본 지출 및 운영 간접비 없이 높은 보안이 보장되도록 설계된 복원력 있는 인프라를 얻을 수 있다.

- 복원력이 뛰어난 인프라
- 철저한 보안
- 강력한 조치

지속적인 개선

고객의견을 반복적으로 통합하여 대혁신, 지속적인 발전을 이루고 있다. (아래의 서비스를 무료 혹은 낮은 가격에 제공)

- Identity and Access Management
- 로깅 및 모니터링
- 암호화 및 키 관리
- 네트워크 세그먼트 분리 및 표준 DDoS 보호

필요한 것에 대한 지불

고급 보안 서비스를 통해 새롭게 등장하는 위협에 즉시 능동적으로 대처하는 동시에, 사용하는 만큼만 지불하여 비용을 절감할 수 있음. 자체 인프라 관리에 비해 초기 비용이 없고 운영 간접비를 줄이면서 조직의 성장에 따라 필요한 보안을 선택할 수 있음

- 고급 보안 서비스
- 실시간으로 발생하는 위협 해결
- 더 저렴한 운영 비용으로 요구 사항 충족 (조직의 성장에 따라 필요한 보안을 취사 선택)

규정 준수 요구 사항 충족

적절한 보안 환경은 규정을 준수하는 환경. 규정된 워크로드를 AWS 클라우드로 마이그레이션하면 다양한 거버넌스 지원 기능을 사용하여 보다 높은 수준의 보안을 구현할 수 있음 (클라우드 기반의 거버넌스 또한 더욱 효율적인 관리, 보안 제어 및 중앙 자동화를 통해서 시작 비용의 절감, 손쉬운 운영, 향상된 민첩성을 제공

- 추가 감독
- 보안 통제
- 중앙 자동화

AWS 책임 공유 모델

AWS가 실행하는 많은 보안관리를 상속, 유지 관리해야하는 보안 관리의의 수를 줄일 수 있음

특정 보안 보장 요구 사항을 유지하고 실행하는 데 소요되는 비용을 줄이는 동시에, 자체 규정 준수 및 인증 프로그램이 강화됨

- AWS 보안 제어 기능 상속
- 제어 기능의 계층화

보안 제품 및 기능

고객이 보안 목표를 달성할 수 있도록 수많은 도구 및 기능을 제공, 온프레미스 환경 내에서 배포하는 익숙한 관리와 호환

네트워크 보안, 구성 관리, 액세스 제어 및 데이터 보안 전반에 걸친 보안 특정 도구 및 기능을 제공

모니터링 및 로깅 도구를 제공하므로 사용자 환경에서 발생하는 상황을 완벽하게 파악

- AWS 및 파트너가 액세스
- 모니터링 및 로깅에 사용

네트워크 보안

프라이빗 네트워크를 만들 수 있는 내장 방화벽, 인스턴스 및 서브넷에 대한 네트워크 액세스 제어, 모든 서비스에 걸친 전송 계층 보안을 통한 전송 중 암호화, 사무실 또는 오프레미스 환경에서 프라이빗 또는 전용 연결을 지원하는 연결 옵션, Auto Scaling 또는 콘텐츠 제공 전략의 일부인 DDoS 완화 기술이 포함

- 기본 제공 방화벽
- 전송 중 암호화
- 비공개 / 전용 연결
- DDoS 완화

인벤토리 및 구성과 관리

리소스의 생성 및 폐기를 유지하는 배포 도구, AWS 리소스를 식별한 후 시간 경과에 따라 해당 리소스의 변경 사항을 추적하고 관리하는 인벤토리 및 구성 관리 도구, Amazon EC2 인스턴스에 대해 미리 구성된 표준 강화 가상 머신(VM)을 생성하는 템플릿 정의 및 관리 도구가 포함

- 배포 도구
- 인벤토리 및 구성 도구
- 템플릿 정의 및 관리 도구

데이터 암호화

클라우드에 저장되어 있는 데이터의 보안 계층을 제공하여 확장 가능하고 효율적인 암호화 기능을 지원

스토리지와 데이터베이스 서비스에서 사용가능한 데이터 암호화 기능이 포함

- 암호화 기능
- 키 관리 옵션 (AWS Key Management Service)
- 하드웨어 기반 암호화 키 스토리지 옵션 (AWS HSM)

액세스 제어 및 관리

암호화 및 데이터 보호 기능을 AWS 환경에서 개발 또는 배포하는 모든 서비스와 통합할 수 있도록 API를 제공

서비스의 사용자 액세스 정책을 정의하고, 실시하고, 관리할 수 있는 기능을 지원

- Identify and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- 기업 디렉터와의 통합 및 연동
- Amazon Cognito
- AWS SSO

모니터링 및 로깅

AWS 환경의 현재 상태를 알 수 있도록 다양한 도구와 기능을 지원

API 호출에 대한 깊은 가시성(누가, 무엇을, 언제, 어디에서 호출했는지 등)

로그 집계 및 옵션, 조사 및 규정 준수 보고의 간소화, 특정 이벤트가 발생하거나 임계값을 초과할 경우의 경고 알림이 포함

- API에 호출에 대한 심층적인 가시성
- 로그 집계 및 옵션
- 알림 제공

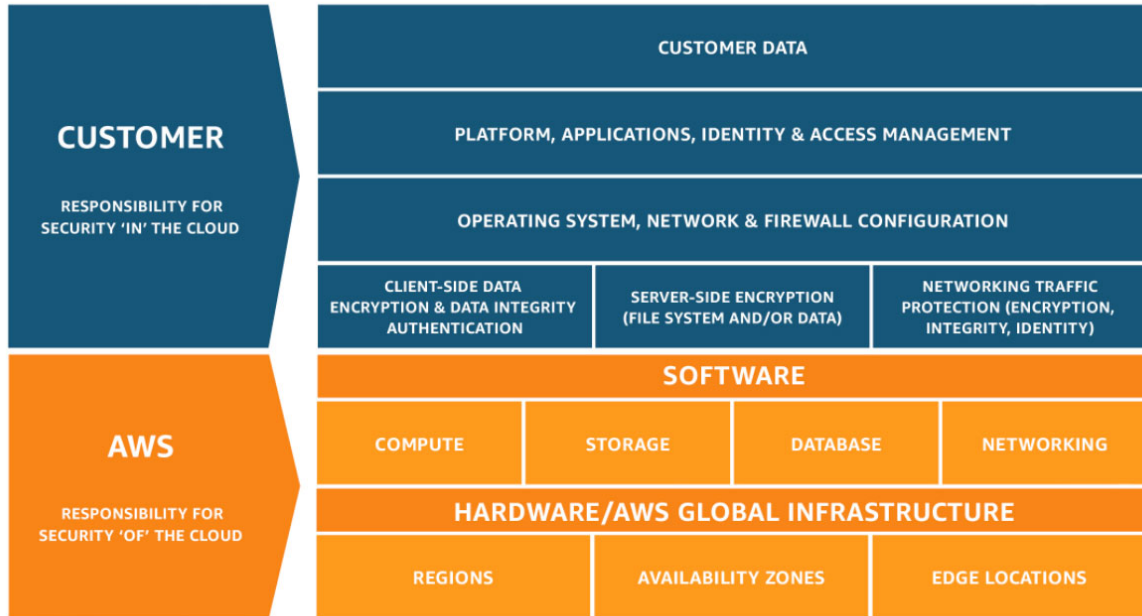
AWS Marketplace

멀웨어 방지 프로그램, 웹 애플리케이션 방화벽, 침입 방지 등 온프레미스 환경과 기존 제어 솔루션에 전혀 뒤지지 않을 뿐만 아니라 원활한 통합도 가능한 수많은 업계 최고 파트너 제품을 제공

- AWS 고객에게 SW를 마케팅/판매할 수 있는 공인 파트너
- AWS에서 실행할 수 있는 온라인 소프트웨어 스토어

공동 책임 모델

보안과 규정 준수는 AWS와 고객의 공동 책임



AWS 책임 '클라우드의 보안'

AWS는 AWS 클라우드에서 제공되는 모든 서비스를 실행하는 인프라를 보호할 책임을 가짐

- 하드웨어
- 소프트웨어
- 네트워킹 및 시설

고객 책임 '클라우드에서의 보안'

고객이 선택하는 AWS 클라우드 서비스에 따라 차이가 있음

EC2

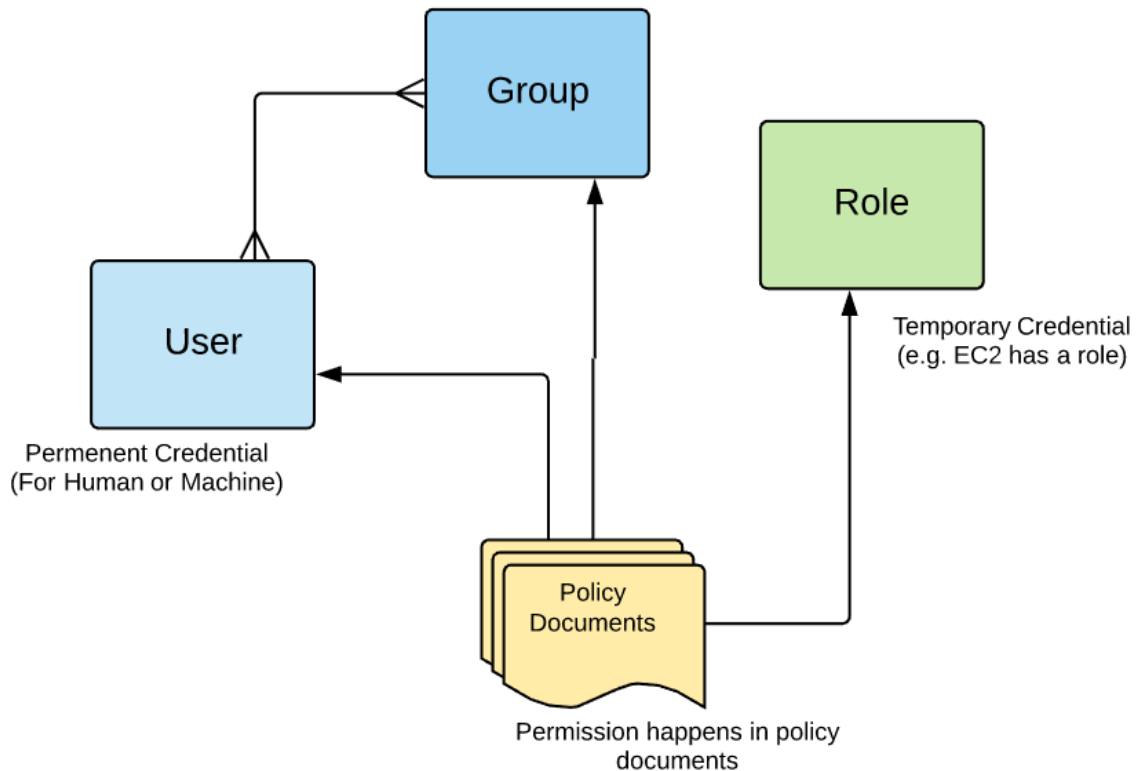
- 인스턴스에 설치한 모든 애플리케이션 소프트웨어 또는 유틸리티의 관리
- 인스턴스별로 AWS에서 제공한 방화벽(보안 그룹이라고 부름)의 구성 관리에 대한 책임이 있습니다.

S3, Amazon DynamoDB

- 데이터 관리(암호화 옵션 포함), 자산 분류, 적절한 허가를 부여하는 IAM 도구 사용

IAM(Identity and Access Management)

AWS 권한 작동 방식 이해



User

- 영구적 명명된 운영자 (사람 or 기계)

Group

- User와 N:M 관계

Role

- 일시적 운영자 (사람 or 기계)

Policy Documents

- JSON File
- User, Group, Role과 직접 연결 될 수 있다.

AWS의 모든 것은 API 이다. 또한 모든 API는 Policy Documents를 통해서 실행되게 된다. 모든 인증은 Policy Documents를 통해서 권한으로 변경되는 과정을 거친다. 따라서 해당 정책 파일을 수정하는 것으로 이미 인가된 사용자의 요청도 막을 수 있다. 또한 모든 API 요청에 대한 성공 및 거부 사실은 CloudTrail에 기록된다.

Amazon Inspector

AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는데 도움 되는 자동 보안 평가 서비스

이점

애플리케이션 보안 문제 파악

- 애플리케이션이 배포되기 이전 또는 프로덕션 환경에서 실행되는 동안 보안 취약성 뿐만 아니라 보안 모범 사례와의 차이점을 파악 할 수 있음

DEVOPS에서 보안을 통합

- DevOps 프로세스에 바로 구축하여 취약성 평가를 분산 및 자동화하고, 보안 평가가 개발 프로세스의 필수 요소가 되도록 개발 및 운영 팀을 지원

개발 민첩성 향상

- 보안 평가를 자동화하고 취약성을 사전에 파악함으로써 개발 및 배포 동안 보안 문제가 발생할 위험을 낮춰줌

보안 표준 적용

- 표준 및 모범 사례를 정의하고, 해당 표준을 준수하는지 검증할 수 있음

Amazon Shield

AWS에서 실행되는 애플리케이션을 보호하는 DDoS보호 서비스

DDoS(Distributed Denial of Service attack) 분산 서비스 거부 공격

악성코드에 감염된 좀비PC를 활용, 특정 시간대 공격명령을 실행하여 공격 대상 컴퓨터에 동시 접속요청을 함으로써 시스템을 마비시키는 방식의 사이버 공격

이점

원활한 통합 및 배포

- 일반적인 네트워크 및 전송 계층 DDoS 공격으로 부터 자동 보호
- 탄력적 IP, ELB, CloudFront, Accelerator의 Advanced Shield를 활성화 하는 것 만으로도 높은 수준의 보호를 실현

관리형 보호 및 공격 가시성

- 리소스별 탐지를 제공하며 정교하거나 더 큰 규모의 공격에는 고급 완화 및 라우팅 기술을 사용
- AWS CloudWatch 지표 및 공격 진단을 통해 모든 DDoS 인시던트에 대한 가시성 및 분석 정보를 제공

사용자 지정 가능한 보호

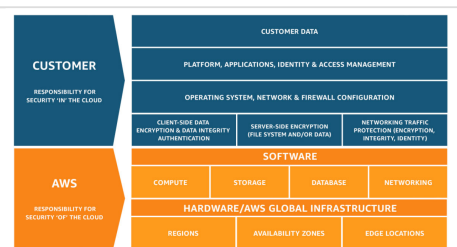
- 인프라 보호를 위한 리소스를 유연하게 설정 할 수 있음
- WAF로 사용자 지정된 규칙을 작성하여 정교한 애플리케이션 계층의 공격 완화 가능

비용 효율

- AWS Shield Standard 추가 비용없이 자동 활성화
- Advanced(WAF, Firewall Manager를 추가 비용 없이 제공)
- DDoS 공격으로 인한 사용량 증가 시 "조정 시 DDoS 요금 보호" 적용

References

https://d1.awsstatic.com/security-center/Shared_Responsibility_Model_V2.59d1eccec334b366627e9295b304202faf7b899b.jpg



How To Create Admin User In AWS - MyDatahack


After you create an AWS account, the best practice is to lock away the root account credential (which you used to create the account) and never use it to do your daily tasks. Instead

👁 <https://www.mydatahack.com/how-to-create-admin-user-in-aws/>



Amazon Inspector - Amazon Web Services(AWS)


AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동 보안 평가 서비스 Amazon Inspector는 AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는데 도움이 되는 자동 보

 <https://aws.amazon.com/ko/inspector/>



AWS Shield - Amazon Web Services(AWS)


AWS Shield는 AWS에서 실행되는 애플리케이션을 보호하는 디도스(DDoS) 보호 서비스입니다. AWS Shield는 애플리케이션 가동 중지 및 지연 시간을 최소화하는 상시 탐지 및 자동 인라인 통합을 제공하

 <https://aws.amazon.com/ko/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>



AWS IAM: IAM Policy 알아보기 (이론편)

모든 법률의 가장 기본이 되는 여섯 가지 법률을 일컬어 육법(六法)이라고 합니다. 육법에는 헌법, 민법, 형법, 상법, 형사소송법, 민사소송법 등이 있습니다. 이 육법은 다른 특별한 법률과 하위 법령의 기반이 되어

 <https://musma.github.io/2019/11/05/about-aws-iam-policy.html>

