AWS_210804

*AWS lAM

-AWS IAM은 클라우드 인프라에서의 신분 및 접속 관리 (IAM, Identity and Access Management) 서비스.

-사용자와 사용자 그룹이 보안이 유지된 상태에서 AWS 리소스에 접근할 수 있도록 도와줌.

-IAM을 이용하면 특정 유저가 어떤 서비스를 사용할지 정할 수 있고, 해당 유저에게 어떤 권한을 부여할지도 정할 수 있고

-매우 간단하게 AWS 리소스에 대한 신분 인증 및 접근 권한 관리를 수행가능.

이처럼 IAM을 이용하면 업무 감사, 사용자 로그 분석, 지속적 모니터링, 계정별 리뷰 등이 가능.

*IAM의 신분 인증(Authentication)

유저 및 접근 권한 관리

-클라우드 유저를 생성하고 액세스 키, 패스워드, 멀티팩터 인증 등 보안 수단 관리가능.

-유저의 접근 허용 관리, 유저가 수행할 수 있는 작업의 세부적인 통제가능.

그룹화된 유저 및 접근 권한 관리

협업을 위해 그룹화된 유저(federated users)관리.

그룹화를 이용해서 AWS 리소스에 접근할 수 있는 싱글 사인온(SSO) 방식으로 기업 디렉터리에 접근가능.

AWS는 보안 추가 마크업 언어인 SAML 방식 지원.

MS 액티브 디렉터리(Active Directory)를 위한 AWS 디렉터리 서비스 (Directory Service) 등 비 SAML 방식도 지원.

*권한 부여

-IAM을 이용시 클라우드 내에서 사용자의 행동을 세부적으로 관리가능. 즉, 이를 통해 '최소한의 권한 부여(Authorization) 및 책임의 분리'라는 보안 컨셉을 구현.

-AWS에서는 IAM 정책(policies) 방식으로 권한을 부여하는데, JSON으로 작성된, 하나 혹은 그 이상의 접근 승인 규칙포함. 유저, 그룹, 롤 등 어떤 IAM 엔티티에도 적용이 가능하며,유저 또는 그룹이 할 수 있는 행동, 접근 가능한 리소스의 종류, 실행 결과 등 클라우드에서 일어나는 거의 모든 권한부여 업무정의가능.

-IAM 정책을 이용하면 IAM 엔티티에 대한 세부적인 통제하고, 다수의 엔티티에 한 번에 정책 적용하는것도 가능함. 또 회사의 개발자에게 아마존 RDS에 대한 리드 온리 접근권한을 부여하려는 경우, RDSRO라는 정책을 생성해 모든 개발자에게도 적용가능. (간단해짐.)

*감사

-AWS는 클라우드 업무 감사(Auditing)를 위한 도구 제공.
-AWS 클라우드트레일(CloudTrail)은 계정에서 일어나는 일을 기록하고, 이에 대한 로그 파일을 아마존 S3 버킷에 저장.
-콘솔, CLI 등을 이용해 로그 파일에 접근할 수 있고, Splunk, SumoLogic, AlertLogic, Loggly, DataDog 등 널리 사용되는 분석 도구로 로그 데이터 분석도 가능.

*보안 자격 정보의 유형

-AWS 생태계에서는 다양한 유형의 보안 자격 정보(Security Credentials)가 사용.
-보안 자격 정보는 사용자가 어떤 방식으로 AWS 리 소스에 접근하느냐에 따라 달라짐.
-AWS는 위의 보안 자격 정보 외에도 임시 보안 자격 정보(Temporary Security Credentials)제공
-AWS 리소스에 대한 접근 권한을 부여하기 위해 임 시 보안 자격 정보를 제공하는 경우에는 AWS 시큐리티 토큰 서비스(AWS STS, Security Token Service)사용가능.

*유저

-AWS에 로그인할 때도 AWS에 로그인할 수 있는 유저 Users 라는 신분필요.
-IAM에서 유저란 AWS 생태계에 존재하는 사용자 또는 서비스를 가리키는 유일무이한 개체(entity). 사용자는 이들 개체를 통해 AWS와 상호작용하고 일상의 업무를 수행.
-IAM 유저는 유저네임과 보안 자격 정보를 지님. 어드민 등이 명시적으로 접근 권한을 승인해주지 않는 한 아무런 리소스에도 접근불가.
-또 특정 개발자가 데이터베이스 작업을 해야 하는 경우, 어드민은 RDS에 대한 리드 온리(읽기전용) 권한부여가능.
-IAM으로 처음 생성된 유저는 보안 자격 증명 또한 지니고 있지 않으므로 어드민 은 이들 유저에게 적합한 보안 자격 증명을 부여해야 함.

*그룹

-IAM 그룹(Groups)은 유닉스 운영체제의 그룹과 유사한 개념.

-그룹은 다수의 역할과 권한으로 구성되고 IAM을 이용해서 승인함.
-그룹에 추가된 유저는 그룹에 정의된 역할과 권한을 상속 ㅁ 그룹에 다수의 유저 추가 가능.
-하나의 유저가 다수의 그룹에 포함될 수 있음 (단, 하나의 그룹을 다른 그룹에 추가할 수는 없으며, 그룹에는 오직 유저만 추가 가능.)
-AWS 계정의 모든 유저를 포함한 기본 그룹이 자동으로 생성되지는 않으며, 그룹을 생성해서 모든 유저를 추가가능.)

*IAM 권한의 계층(Hierarchy of Privileges)

-AWS 유저를 권한의 계층으로 구분할 필요가 있는 경우 아래와 같이 가장 권한 이 높은 유저를 맨 앞에 놓고 가장 권한이 낮은 유저를 맨 뒤에 놓는 순서로. ㅁ AWS 루트 유저 또는 계정 소유자 모든 서비스와 리소스에 대한 무제한의 접근 권한 보유 ㅁ AWS IAM 유저 제한된 권한 보유. 그룹과 유저 정책에 의해 제한 받음 ㅁ 임시 보안 자격 정보 보유자 신분 확인 후 접근이 제한되고, 토큰 생성 등에 대한 정책으로 추가 제한 됨

*IAM 활용 베스트 프랙티스

-AWS 계정 생성 직후 계정 소유자이자 관리자를 IAM 유저를 생성해 어드민 권한을 부여하고 루트 유저 계정은 안전하게 감춤.
-강력한 패스워드 정책을 수립하고, 90 일이 경과한 패스워드는 폐기.
-패스워드에는 최소 하나의 대문자, 소문자, 기호문자, 숫자가 포함되도록 하고, 최소 8자에서 10자 이 상이 되어야함.
-서로 다른 계정 간의 접근 권한 부여 시, 계정 내에서의 접근 권한 부여 시, 그룹 유저에게 접근 권한부 여 시 항상 IAM 롤을 사용.
-롤을 이용하면 보안자격 정보를 공유하거나 장기 보안 정보를 저장할 필요가 없어지며 누가 어떤 소 스에 접근할 수 있는지 파악가능.
-AWS 생태계에서 감사의 중요성은 매우 크므로 모든 리전에서 AWS CloudTrail의 로그 파일 검증기능을 활성화시키는 것이 좋음.
-또한 아마존 S3에 저장된 CloudTrail 로그 데이터를 안전하게 관리하는 일 또한 중요.

*AWS 보안 규정 프로그램

-AWS 보안 규정 프로그램(Compliance Program)은 고객으로 하여금 AWS 클라우드 내에서 보안 유지 및 데이터 보호가 어떻게 이뤄지는지 잘 이해할 수 있도록 해줌.
이 프로그램은 AWS 클라우드 인프라 위에 마련돼 있으며, 보안 규정에 따른 책임이 효과적으로 공유됨.

-고객은 AWS 보안 통제 환경에서 좀 더 쉽고 효과적으로 보안 규정 프로그램을 수립 및 운영가능.
-AWS가 고객에게 제공하는 IT 인프라는 검증된 보안 기법과 다양한 IT 보안 표준을 제공.
-AWS 플랫폼이 제공하는 유연성과 통제성은 고객으로 하여금 다음과 같이 다양한 산업 표준안에 부합하는 보안 솔루션을 제공가능.

*AWS 공유 책임 모델

기업이 자신의 컴퓨터 시스템과 데이터를 클라우드로 이전하면, 보안 책임은 기업, 클라우드 서비스 제공자가 분담하는데, AWS는 클라우드 환경을 구성하는 인프라에 대한 보안을 책임지고, 기업은 클라우드에 저장한 것, 혹은 클라우드에 연결한 것에 대한 보안을 책임지게 됨. 이와 같은 보안 책임의 공유 모델(Shared Responsibility Model)은 다양한 측면 에서 기업의 운영 부담을, 추가적인 비용 부담이나 노력 없이 기업의 기본적인 보안수준을 개선가능하다는 장점. AWS 준수하는 공유 보안 책임 모델에는 AWS가 책임지는 부분과 AWS의 고객 인 기업이 책임을 지는 부분이 명확히 구분되어있음.

*보안에 대한 AWS측의 책임

데이터 센터에 대한 물리적 보안

-아마존이 운영하는 데이터 센터의 물리적 보안은 물론, 이에 접근하는 아마존 임직원의 로그 데이터, 감사 데이터를 관리하고 있으며, 데이터 센터 곳곳에 대한 비디오 감시, 첨단의 화재 감지 및 진화를 갖춤.
-데이터 센터는 전력 상황을 고려해서 중복 구현 방식으로 설계됐으며, 갑작스런 정전 사태에 대비하기 위해 무정전 전원장치(UPS, Uninterruptable Power Supply)를 보유하고 있고, 태풍, 장마 등 각종 자연재해에도 대비.
-AWS 데이터 센터 내부는 작업자의 업무에 따라 접근 가능 구역이 세분화돼 있으며, 물리적으로 접근 할 때는 논리적 접근 권한을 차단하고, 데이터 센터를 방문하는 임직원은 AWS 콘솔을 통한 접근을 할 수 없음.

아마존 EC2 보안

-AWS는 루트 유저를 위한 운영 체제 호스팅에 대한 보안 책임이 있음.
-AWS 호스팅 영역에 접근하려는 기업 고객의 어드민은 미리 접근 권한을 얻은 뒤, 반드시 멀티팩터 인 증 방식으로 로그인해야 하며, 로그인 이후의 모든 행동은 로그 및 감사 데이터로 기록됨.
-게스트 OS에서 실행되는 가상 인스턴스는 AWS 고객이 운영하므로 계정, 서비스, 애플리케이션 등 모 든 부문에 대한 루트 접근 권한 및 어드민 수준의 통제 권한이 제공.

-AWS는 고객의 인스턴스 또는 게스트 OS에 대한 접근 권한은 갖고 있지 않으며, 이에 대한 로그 데이 터 또한 기록X

-또한 아마존 EC2는 완벽한 방화벽 솔루션을 제공하며, 시큐리티 그룹에서 인스턴스로 유입되는 모든 접근을 기본적으로 거부하는 인바운드 방화벽도 제공.

-시큐리티 그룹을 이용해서 방화벽의 환경을 설정할 수 있고, 동일한 물리적 서버에서 실행되는 다수의 인스턴스는 Xen 하이퍼바이저에 의해 각각 격리.

*보안에 대한 AWS측의 책임

네트워크 보안

-AWS는 네트워크 인프라에 대한 책임을 지며, 세심한 모니터링 및 관리 역량을 바탕으로 글로벌 최고 수준의 네트워크를 운영 중.

-AWS의 네트워크 디바이스는 중복 구현 원칙에 따라 설계되며, 방화벽, 내부 및 외부 커뮤니케이션에 대한 모니터링 및 통제 시스템을 운영 중.

환경설정 관리

-환경설정 관리는 모든 변경 사항의 인증, 로그, 테스트, 승인, 문서화 업무를 관리.

-또 AWS는 이메일 또는 서비스 헬스 대시보드를 통해 서비스에 미칠 수 있는 잠재적인 요소를 알려주고, 고객과 소통.

고가용성 데이터 센터

-AWS는 모든 데이터 센터가 언제나 고가용성을 유지하도록 하는 책임이 있음.

-모든 데이터 센터는 항상 가동 상태를 유지해야 하고, 고객에게 언제든 서비스를 제공해야함.

-결국 모든 AZ가 항상 가동 상태를 유지하고 있어야 하는데, 모든 AZ는 중복 구현 컨셉으로 설계되어, 장애 대응 능력을 보유.

디스크 관리

-AWS는 고객 소유 디스크 관리라는 측면에서(멀티 테넌시 환경이지만) 다른 사용자의 디스크 공간 또 는 데이터 영역을 볼 수 없도록 관리중.

-고객의 서버 인스턴스는 물리적 장치를 통해 접근할 수 없으며, 가상의 디스크 형태로 존재.

-디스크 가상화 레이어는 고객에 의해 각 블록 스토리지 생성 시마다 자동으로 리셋되며, 이전에 기록 됐던 내용은 모두 삭제됨.

-고객은 자신이 AWS의 어떤 서비스를 사용하느냐에 따라 책임 범위와 책임 이행의 방법이 달라짐.

네트워크 환경설정

-VPC는 클라우드에서 개별 기업만을 위한 데이터 센터를 운영할 수 있도록 해주지만, VPC의 보안 환 경설정 책임은 고객부담.

-AWS는 개별 기업의 VPC에 접근할 수 없고, 그 속에서 실행되는 요소에 대한 통제력도 없으므로 VPC가 안전한 환경에서 실행될 수 있도록 해야함.

서비스 환경설정

-고객은 서비스 환경설정 면에서 자신의 서버에 누가, 어떤 소프트웨어를 설치하는지 알고 있어야 하고, 자신의 인프라에 어떤 변경 사항이 적용됐는지도 잘 파악해야함.

자격 인증 및 계정 관리

-고객은 AWS 유저와 애플리케이션 유저의 자격 인증과 계정 관리에 대한 책임있음.

-고객이 IaaS 외에도 AWS의 컨테이너 서비스와 같은 PaaS를 사용하는 경우, 예를 들어 RDS에서 데이 터베이스를 호스팅하거나 Redshift에서 데이터 웨어하우스를 실행하는 경우, DynamoDB에서 NoSQL 데이터베이스를 실행하는 경우, AWS는 운영체제 호스팅, 운영체제 방화벽 관리, 인스턴스 론 칭 및 유지보수, 게스트 OS 또는 데이터베이스 패칭, 데이터베이스 복제 등 모든 업무를 관장.

-고객은 AWS 계정의 보안 자격 정보를 보호하고 개별 유저 계정을 IAM을 통해 관리해 다수의 유저가 자신의 보안 자격 정보를 관리할 수 있도록 하고, 권한의 한계를 명확히 해야 하며 RDS의 서비스에 포함된 데이터의 관리 책임을 짐.

-고객은 PaaS 외에도 AWS의 추상적 서비스(abstract services)로도 부르는 SaaS를 사용할 수 있는데, AWS에서 대표적인 SaaS는 S3. 암호화를 비롯한 제반 관리 업무는 AWS가 맡음. SaaS의 경우 고객의 보안 환경설정 작업량은 사용하는 서비스와 데이터의 용도에 따라 달라짐.

실습하기 1. IAM 유저, 그룹, 롤 생성하기

실습하기 2. 아마존 EC2 접근을 위한 IAM 롤