IAM 소개 및 최소 권한 원칙

AWS Identity and Access Management 기본 개념

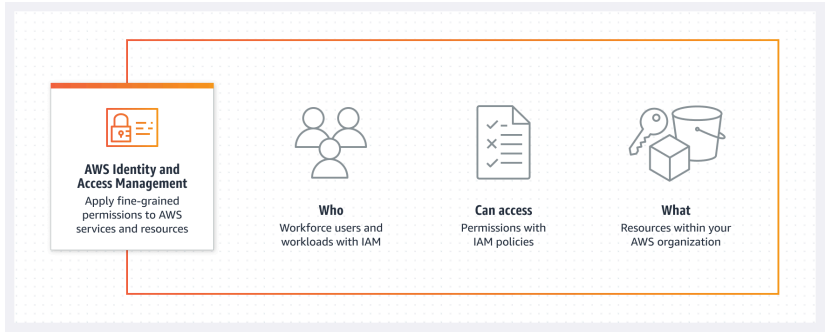
IAM이란?

IAM (Identity and Access Management)
AWS 리소스에 대한 접근을 안전하게 제어하는 서비스

- **인증 (Authentication)**: "당신은 누구인가?"
  - 사용자의 신원을 확인
- **권한 부여 (Authorization)**: "무엇을 할 수 있는가?"
  - 인증된 사용자가 수행할 수 있는 작업을 결정

IAM의 역할

AWS 계정 내 **누가 어떤 리소스**에 접근할 수 있는지 세밀하게 제어



IAM 기본 개념

세 가지 핵심 요소:

1. **사용자 (Users)**
2. **역할 (Roles)**
3. **정책 (Policies)**

사용자 (Users)

IAM 사용자는 AWS 서비스와 상호작용하는 **사람** 또는 **애플리케이션**

- 각 사용자는 고유한 자격 증명을 가짐
  - 비밀번호
  - 액세스 키
- 사용자별로 개별 권한 설정 가능
- 콘솔 로그인 또는 프로그래밍 방식 접근에 사용

⚠️ 사용자 관리 주의사항

절대 하지 말아야 할 것

하나의 IAM 사용자 계정을 여러 사람이 공유하지 마세요

올바른 방법

각 사용자는 **개별 IAM 사용자**를 가져야 합니다

역할 (Roles)

IAM 역할은 **특정 권한을 가진 임시 자격 증명**

사용자와 달리 영구적인 자격 증명이 없음

- AWS 서비스(EC2, Lambda)가 다른 리소스에 접근할 때
- 외부 사용자에게 임시 접근 권한을 부여할 때
- 역할을 "맡으면(assume)" 임시 자격 증명을 받음

💡 역할 활용 팁

EC2에서 S3 접근이 필요할 때

❌ 액세스 키를 인스턴스에 저장

✅ **IAM 역할을 인스턴스에 연결**

정책 (Policies)

IAM 정책은 **JSON 형식의 권한 문서**

누가, 어떤 리소스에, 어떤 작업을 할 수 있는지 정의

```
{
  "Effect": "Allow",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
}
```

정책의 핵심 요소

요소	설명	예시
Effect	허용 또는 거부	`Allow`, `Deny`
Action	수행할 수 있는 작업	`s3:GetObject`
Resource	작업 대상 리소스	`arn:aws:s3:::my-bucket/*`

정책 유형

유형	설명
AWS 관리형 정책	AWS가 생성하고 관리하는 사전 정의된 정책
고객 관리형 정책	사용자가 직접 생성하고 관리하는 정책
인라인 정책	특정 사용자/그룹/역할에 직접 포함된 정책

최소 권한 원칙

Principle of Least Privilege

사용자나 서비스에게 **업무 수행에 필요한 최소한의 권한**만 부여하는 보안 원칙

🤔 자주 받는 질문

"왜 모든 권한을 한 번에 받을 수 없나요?"

비개발직군에서 AWS 접근을 요청할 때 자주 받는 질문입니다

- 비즈니스 분석
- 데이터 사이언티스트
- 마케팅

이유 1: 보안 위험

- 계정이 유출되면 **모든 리소스**가 위험에 노출
- 실수로 중요한 리소스를 삭제하거나 변경할 수 있음
- **비용이 급증**하는 리소스를 생성할 수 있음

이유 2: 규정 준수

- 많은 보안 규정에서 최소 권한 원칙을 요구
  - ISO 27001
  - SOC 2
- 감사 시 과도한 권한은 **지적 사항**이 됨

실제 사례

사례 1

S3 버킷 **읽기만** 필요한데 Administrator 권한을 받으면
→ 실수로 버킷을 **삭제**할 수 있음

사례 2

특정 EC2 인스턴스만 관리하면 되는데 모든 EC2 권한을 받으면
→ **다른 팀의 인스턴스**도 영향받을 수 있음

모범 사례

원칙	설명
필요한 권한만 요청	업무에 필요한 최소한의 권한만 요청
권한 검토 주기 설정	정기적으로 부여된 권한이 여전히 필요한지 검토
그룹 활용	비슷한 역할의 사용자들은 그룹으로 관리
임시 권한 활용	일시적인 작업은 역할을 통한 임시 권한 사용

요약

1. **IAM**은 AWS 리소스 접근을 제어하는 서비스
    - 인증 + 권한 부여
2. **IAM 기본 개념**
    - 사용자(Users): 개인/애플리케이션의 고유 자격 증명
    - 역할(Roles): 임시 자격 증명을 제공하는 권한 세트
    - 정책(Policies): JSON 형식의 권한 정의 문서
3. **최소 권한 원칙**: 필요한 최소한의 권한만 부여

다음 세션 예고

IAM Identity Center

중앙 집중식 접근 관리와 SSO(Single Sign-On)에 대해 알아봅니다

질문 있으신가요?