IAM Identity Center 활용

중앙 집중식 접근 관리와 SSO

IAM Identity Center란?

AWS IAM Identity Center (구 AWS SSO)

여러 AWS 계정과 애플리케이션에 대한 접근을 **중앙에서 관리**하는 서비스

- 한 번의 로그인으로 여러 계정 접근
- 사용자와 그룹을 중앙에서 관리
- 권한 세트로 일관된 권한 부여

중앙 집중식 접근 관리

기존 방식의 문제점

- 각 AWS 계정마다 별도의 IAM 사용자 생성
- 계정별로 비밀번호/액세스 키 관리
- 퇴사자 발생 시 모든 계정에서 삭제 필요

IAM Identity Center 방식

- **하나의 ID**로 모든 계정 접근
- 중앙에서 사용자 추가/삭제
- 권한 변경도 한 곳에서 관리

SSO (Single Sign-On)

SSO란?

한 번의 인증으로 여러 시스템에 접근하는 방식

SSO의 장점

장점	설명
편의성	여러 비밀번호를 기억할 필요 없음
보안 강화	하나의 강력한 인증만 관리
관리 효율성	계정 생성/삭제가 한 곳에서 처리
감사 용이성	모든 접근 로그가 중앙에 기록

로그인 방법

1. AWS Access Portal 접속

회사 전용 포털 URL로 접속

```
https://your-company.awsapps.com/start
```

2. 자격 증명 입력

- 회사 이메일/ID
- 비밀번호
- MFA 인증 (필수)

로그인 후 화면

접근 가능한 **AWS 계정** 목록이 표시됨

각 계정에서 사용 가능한 **역할** 선택 가능

권한 세트 (Permission Sets)

권한 세트란?

AWS 계정에서 사용자가 가질 수 있는 **권한의 묶음**

- AWS 관리형 정책 기반
- 커스텀 정책 추가 가능
- 여러 계정에 동일하게 적용

권한 세트 예시

권한 세트	용도	포함 권한
ViewOnlyAccess	읽기 전용	모든 리소스 조회
PowerUserAccess	개발자용	IAM 외 모든 서비스
AdministratorAccess	관리자용	전체 권한
Billing	비용 관리	비용 조회/관리

멀티 계정 설정

왜 여러 계정을 사용하나요?

- **환경 분리**: 개발/스테이징/프로덕션
- **비용 분리**: 프로젝트별 비용 추적
- **보안 격리**: 장애 영향 범위 최소화
- **규정 준수**: 민감 데이터 격리

멀티 계정 구조 예시

```
Management Account (관리 계정)
├── Development Account (개발)
├── Staging Account (스테이징)
├── Production Account (프로덕션)
└── Security Account (보안/로깅)
```

IAM Identity Center에서 **한 번에 모든 계정** 관리 가능

MFA 설정

IAM Identity Center의 MFA

- 로그인 시 **필수** MFA 요구 가능
- 가상 MFA 앱 지원 (Google Authenticator 등)
- 하드웨어 토큰 지원

설정 위치

IAM Identity Center → 설정 → 인증 → MFA

MFA 정책 옵션

옵션	설명
매번 로그인 시	모든 로그인에 MFA 요구
컨텍스트 기반	새 디바이스/위치에서만 요구
사용자 선택	사용자가 직접 설정

권장: 매번 로그인 시 MFA 요구

요약

1. **IAM Identity Center**는 여러 AWS 계정을 중앙에서 관리하는 서비스
2. **SSO**로 한 번의 로그인으로 모든 계정에 접근
3. **권한 세트**로 일관된 권한 정책 적용
4. **멀티 계정** 환경에서 효율적인 접근 관리
5. **MFA** 필수 설정으로 보안 강화

다음 세션 예고

AWS CLI와 단기 자격 증명

IAM Identity Center를 활용한 안전한 CLI 사용 방법을 알아봅니다

질문 있으신가요?