AWS CLI와 단기 자격 증명

IAM Identity Center를 활용한 안전한 CLI 사용

© 2025 내부 교육 자료

AWS CLI란?

AWS Command Line Interface

터미널에서 AWS 서비스를 제어하는 도구

```
# S3 버킷 목록 조회
aws s3 ls

# EC2 인스턴스 목록 조회
aws ec2 describe-instances
```

© 2025 내부 교육 자료

CLI 사용이 필요한 경우

- 스크립트를 통한 **자동화**
- 반복 작업의 **효율화**
- CI/CD 파이프라인 연동
- 콘솔에서 지원하지 않는 고급 기능

© 2025 내부 교육 자료

장기 자격 증명 vs 단기 자격 증명

장기 자격 증명

- Access Key ID + Secret Access Key
- **만료 없음** (직접 삭제 전까지 유효)
- `~/.aws/credentials` 에 저장

단기 자격 증명

- 임시 Access Key + Session Token
- **자동 만료** (보통 1-12시간)
- 매번 새로 발급

© 2025 내부 교육 자료

⚠️ 장기 자격 증명의 위험성

유출 시 피해

- 키가 유출되면 **즉시 악용** 가능
- GitHub에 실수로 커밋하는 경우 많음
- 채굴 봇이 자동으로 탐지하여 악용

실제 사례

- GitHub에 올린 지 **5분 만에** 수천 달러 비용 발생
- 퇴사자가 가져간 키로 리소스 접근

© 2025 내부 교육 자료

단기 자격 증명의 장점

장점	설명
자동 만료	유출되어도 시간이 지나면 무효화
추적 가능	세션별로 누가 발급받았는지 기록
권한 제한	발급 시 권한 범위 지정 가능
MFA 연동	MFA 인증 후에만 발급

© 2025 내부 교육 자료

STS 토큰

AWS Security Token Service (STS)

임시 자격 증명을 발급하는 서비스

```
{
  "AccessKeyId": "ASIA...",
  "SecretAccessKey": "wJalr...",
  "SessionToken": "FwoGZX...",
  "Expiration": "2025-02-15T18:00:00Z"
}
```

SessionToken 포함 → 단기 자격 증명

© 2025 내부 교육 자료

AWS CLI 설정 방법

IAM Identity Center 연동

```
# SSO 설정 시작
aws configure sso

# 필요한 정보 입력
SSO session name: my-sso
SSO start URL: https://your-company.awsapps.com/start
SSO region: ap-northeast-2
SSO registration scopes: sso:account:access
```

© 2025 내부 교육 자료

SSO 로그인 과정

```
# SSO 로그인
aws sso login --profile my-profile

# 브라우저가 열리고 인증 진행
# MFA 입력 후 승인

# 완료 후 CLI 사용 가능
aws s3 ls --profile my-profile
```

© 2025 내부 교육 자료

프로필 설정

~/.aws/config 파일

```
[profile dev]
sso_session = my-sso
sso_account_id = 123456789012
sso_role_name = PowerUserAccess
region = ap-northeast-2

[profile prod]
sso_session = my-sso
sso_account_id = 987654321098
sso_role_name = ViewOnlyAccess
region = ap-northeast-2
```

© 2025 내부 교육 자료

프로필 활용

```
# 개발 계정에서 작업
aws s3 ls --profile dev

# 프로덕션 계정 조회 (읽기 전용)
aws ec2 describe-instances --profile prod

# 기본 프로필 설정
export AWS_PROFILE=dev
aws s3 ls  # --profile 없이 사용
```

© 2025 내부 교육 자료

로컬 개발 모범 사례

✅ 해야 할 것

- IAM Identity Center + SSO 사용
- 프로필로 계정/역할 구분
- 세션 만료 시 재로그인

❌ 하지 말아야 할 것

- 장기 Access Key 사용
- 코드에 자격 증명 하드코딩
- 자격 증명 파일 Git 커밋

© 2025 내부 교육 자료

자격 증명 우선순위

AWS CLI가 자격 증명을 찾는 순서:

1. **환경 변수** (`AWS_ACCESS_KEY_ID`)
2. **프로필** (`~/.aws/credentials`)
3. **IAM 역할** (EC2/Lambda 등)
4. **컨테이너 자격 증명** (ECS)

로컬 개발: **프로필(SSO)** 사용 권장

© 2025 내부 교육 자료

요약

1. **장기 자격 증명**은 보안 위험이 높음
    - 유출 시 즉시 악용 가능
2. **단기 자격 증명**으로 보안 강화
    - 자동 만료, MFA 연동
3. **IAM Identity Center + SSO**로 CLI 설정
    - 프로필로 여러 계정 관리
4. **절대** 코드에 자격 증명 하드코딩 금지

© 2025 내부 교육 자료

다음 세션 예고

AWS 계정 vs IAM

AWS 계정과 IAM의 차이점, 그리고 멀티 계정 전략을 알아봅니다

© 2025 내부 교육 자료

질문 있으신가요?

© 2025 내부 교육 자료