04_IAM & CLI

IAM

- Identity and Access Management
- IAM은 Global 서비스이다. (리전을 선택할 수 없음)
- Root 계정은 최초 계정 생성 시에만 사용할 것을 권장한다.
- Group에는 오직 User만 포함될 수 있고, 다른 Group이 포함될 수 없다.
- User는 여러 그룹에 속할 수도, 또는 아무 그룹에 속하지 않을 수도 있다.
- **최소 권한의 원칙**을 따른다.
  - 필요한 권한이 생길 때마다 부여한다.
- AWS에서는 비밀번호 정책을 직접 설정할 수 있다.

Policies (정책)

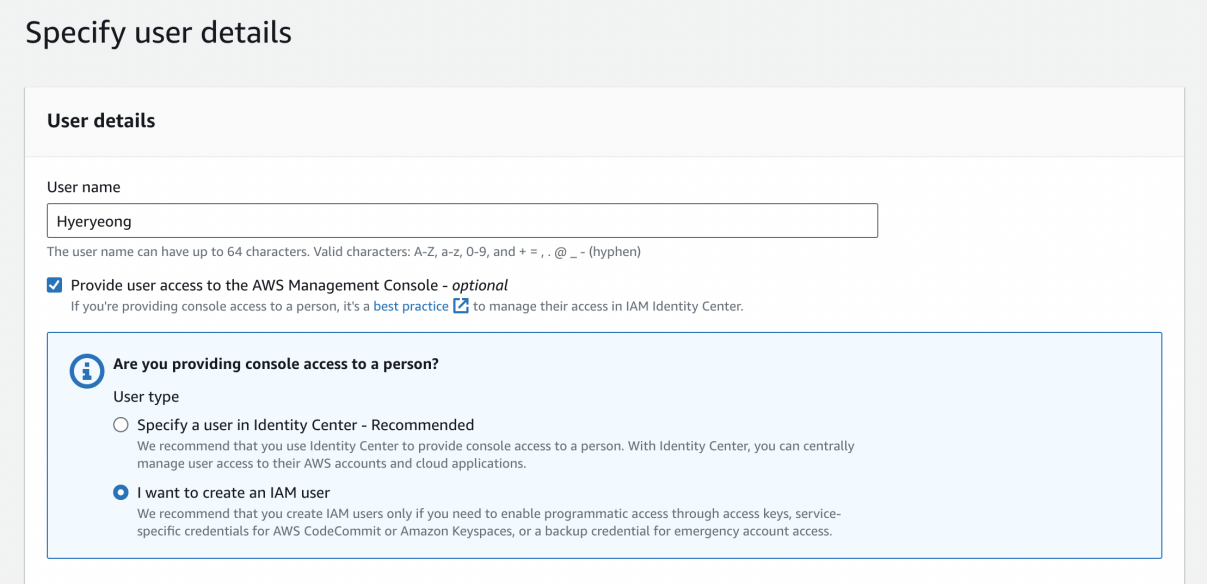
```
{
    "Version": "2012-10-17",
    "Id": "S3-Account-Permissions",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:root"]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": ["arn:aws:s3:::mybucket/*"]
        }
    ]
}
```

- Version: 필수
- Id: 옵셔널
- Statement
  - Sid: 옵셔널 (Optional)
  - Effect: 해당 액션을 허용할지, 거부할지 (Allow/Deny)
  - Principal: 해당 정책을 적용할 대상 (account/user/role)
  - Action: 허용 또는 거부할 액션
    - * : 모든 것을 의미 (ex. s3:*, s3:Get*)
  - Resource: 특정 버킷 등 정책이 적용될 리소스
  - Condition: 해당 Statement가 언제 적용될 지(Optional)

👩🏻‍💻 실습

- 원하는 권한만 부여한 정책을 생성하는 방법
- 유저에게 권한을 부여하는 방법
  - 유저에게 그룹 추가하기
  - 인라인 정책 추가하기
  - AWS에서 제공하는 기본 정책 그룹 부여하기

🧐 궁금한 점



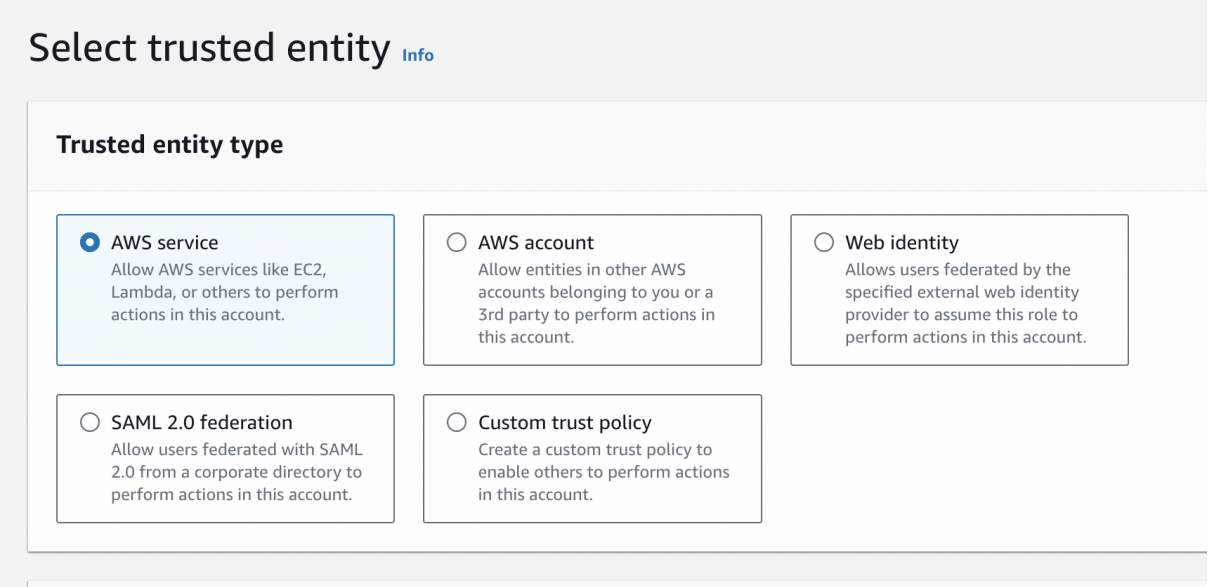
- 루트 계정으로 접속해서 어드민 유저 만들기
  - User type 에 대해서 두 가지 차이 알아보기

Roles (역할)

- AWS 엔티티들에게 AWS에서 작업을 수행할 수 있는 권한을 부여하는 것
- 사용자가 아니라 AWS 서비스가 사용하도록 하기 위해 만들어진 것

🧐 궁금한 점

- 정책은 사용자꺼, 역할은 서비스꺼?



MFA (Multi Factor Authentication)

- 계정을 보호하기 위해 2단계 인증을 추가하는 방법
- MFA = password + security device(물리적 장치)
- AWS의 MFA 디바이스
  - Virtual MFA device - Google Authenticator, Authy

    - Universal 2nd Facor Security Key - YubiKey
    - Hardware Key Fob MFA Device
    - Hardware Key Fob MFA Device for AWS GovCloud

👩🏻‍💻 실습

- custom 비밀번호 정책 설정하기
- root 계정에 MFA 적용하기

🧐 궁금한 점

- MFA는 root 계정에만 적용할 수 있는 것인가?
    - 일반 유저들에게도 적용하려면 어디서 설정해주어야 하지?

AWS에 접근하는 방법

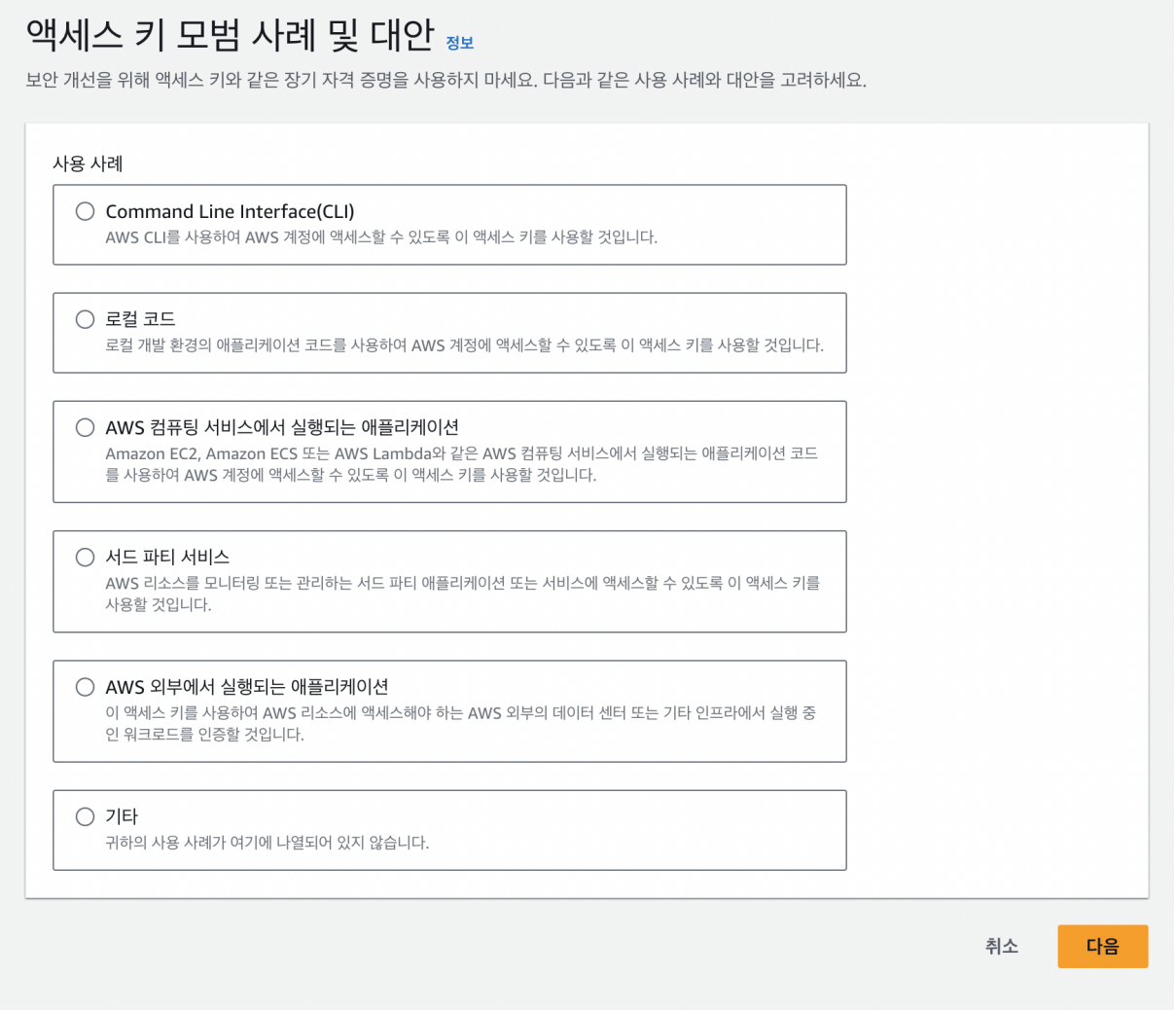
- AWS Management Console
- **AWS Command Line Interface (CLI)**
- AWS Software Developer Kit (SDK)

CLI

- 터미널에서 AWS 서비스에 접근하는 방법
- **Access key ID, Secret Access Key**가 필요하다.

👩🏻‍💻 실습

- 액세스 키 생성하기



- AWS 기능 사용하기
  - AWS console에 접근
  - 액세스 키 + 시크릿 키를 생성해서 CLI로 접근

- CLI의 대안 > CloudShell

보안 도구

- Credential report → account level
- Users > Access Advisor → user-level

IAM 가이드라인 & 모범 사례

- 최초 계정 세팅할 때 외에 root 계정을 사용하지 말 것
- 한 명의 물리적인 유저 = 하나의 AWS User
- 권한을 그룹 단위로 관리하기 위해 유저를 그룹에 조인시킬 것
- 강력한 비밀번호 정책을 생성할 것
- 강력한 계정 보안을 위해 MFA를 사용할 것
- AWS 서비스에 권한을 부여하기 위해서 Role을 사용할 것
- CLI/SDK에서 AWS를 사용하려면 Access Key가 필요하다.
- 보안 감사를 위해 Credential report, Access Advisor를 적극 활용할 것
- IAM user & Access Keys를 절대 공유하지 말 것

✅ 헷갈리는 문제

잘 하셨습니다!
IAM 정책의 문장은 시드, 효과, 원칙, 조치, 리소스, 그리고 조건으로 구성됩니다. 버전은 IAM 정책 자체의 일부이지, 문장의 일부가 아닙니다.

질문 9:

IAM 정책은 하나 이상의 문장으로 구성됩니다. 다음 중 IAM 정책 내 문장의 구성 요소가 **아닌** 것을 고르세요.

- ○ 효과
- ○ 원칙
- ◉ **버전**
- ○ 조치
- ○ 리소스

- 정책(Policy) vs 역할(Role)
- IAM Credentials Report (account-level) vs IAM Access Advisor (user-level)