

# 대학생을 위한 AWS 강의(5)

AWS Identity and Access Management

서진호

# 제 4 강 목표

- IAM 특징과 구성
- IAM 구분 - 자격 증명과 권한의 차이점
- IAM 유의사항
- 실습: 사용자 만들기

# 1. IAM 이란 무엇인가?

---

AWS 리소스에 대한 액세스를 안전하게 제어



IAM 사용자

AWS와 상호 작용하는 사람 또는 애플리케이션



동일한 권한을 가진 사용자 모음



엔터티가 맡을 수 있는 임시 권한

역할

- IAM (Identity and Access Management)

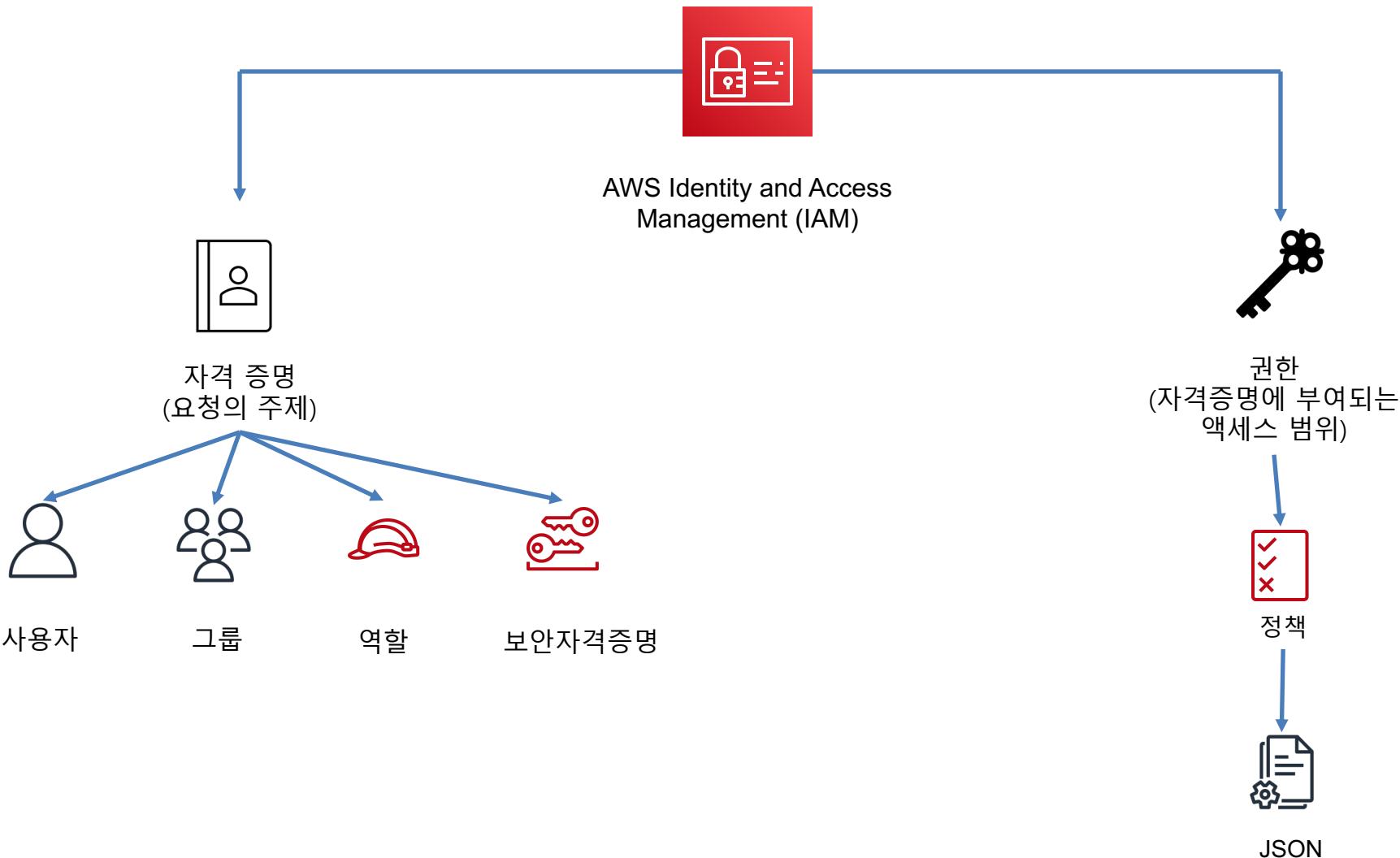
- 루트 계정을 사용하지 않고도 각각의 사용자들이 AWS 리소스 접근 가능.
- IAM을 통해 사용자, 사용자 그룹을 만들어 각각의 사용자 혹은 그룹별로 필요한 권한만을 제한적으로 부여함.

- 루트계정:

- 이메일 아이디로 만든 AWS 계정.
- 모든 AWS 리소스에 접근할 수 있는 권한을 가지고 있기 때문에 여러 명의 사용자가 루트 계정을 사용하는 것은 보안에 좋지 않음.

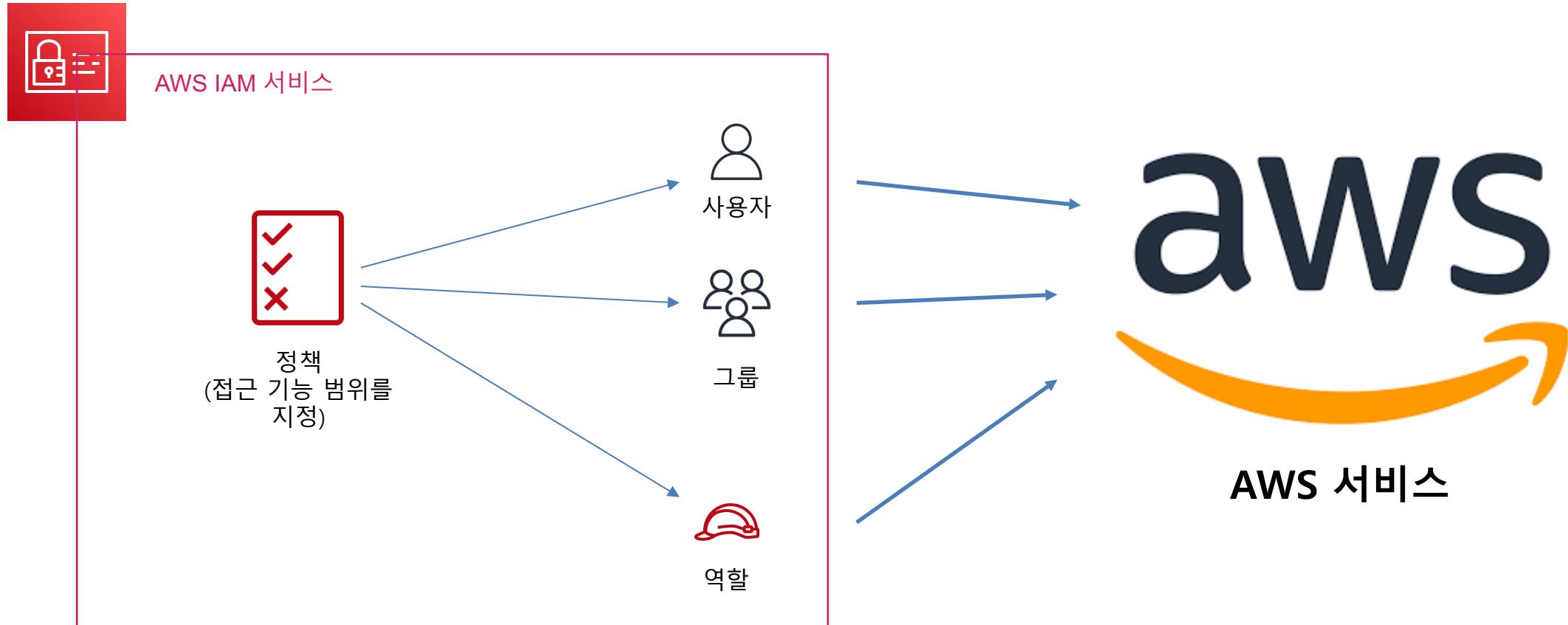
## 2. IAM 구분 – 자격증명과 권한

---



### 3. IAM 특징 및 서비스 정책

---

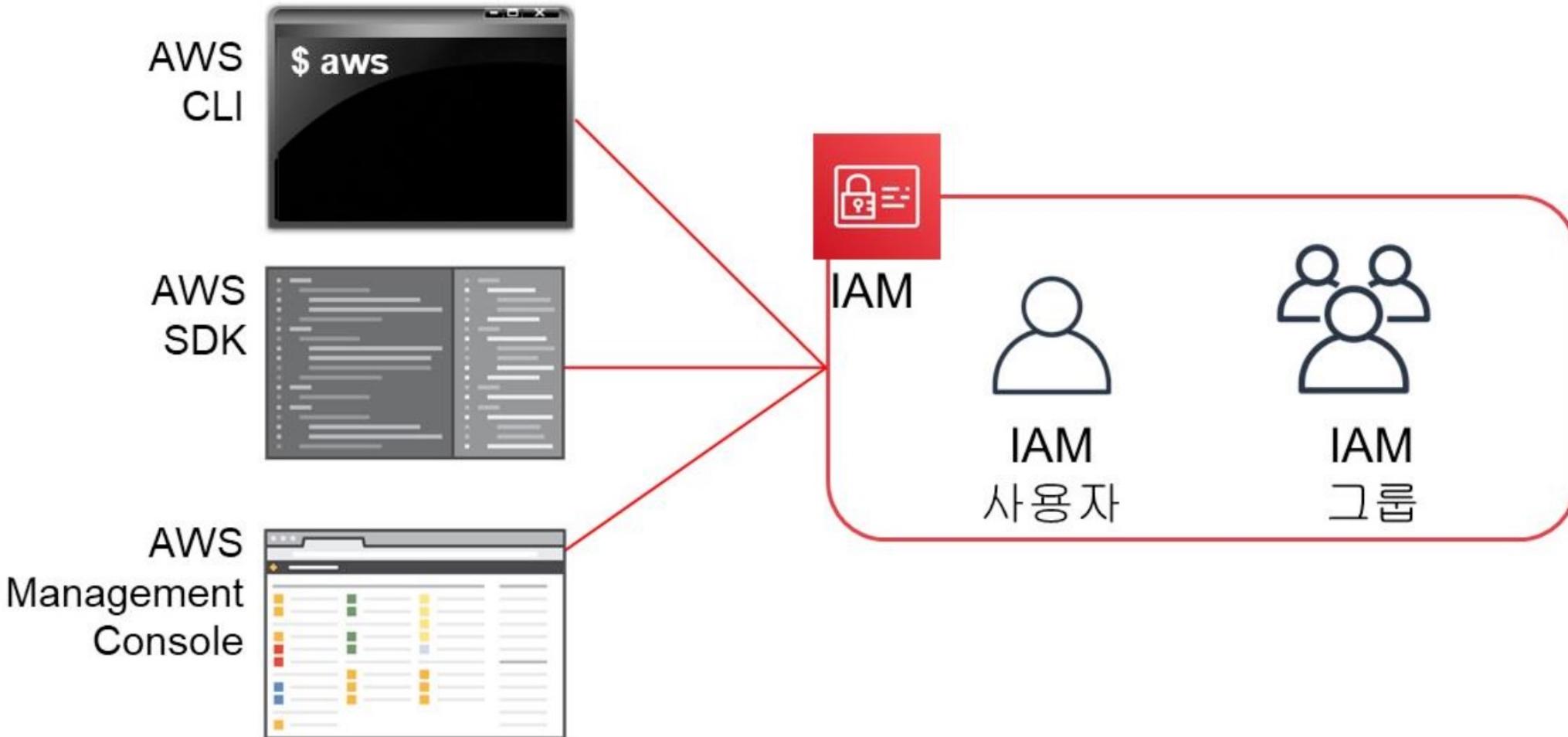


## 4. IAM 구성 – IAM 사용자

---

- IAM 구성:
  - 사용자 정의하는 IAM 사용자, 그룹, 역할
  - 각 사용자의 권한을 정의하는 IAM 정책
- IAM 사용자
  - 루트 사용자
    - 모든 접근을 가지는 가장 중요한 사용자
    - 특정 그룹에 속하지 않고 사용자를 만들 수 있는 권한을 가짐
    - AWS 콘솔에 아이디와 비밀번호로 접속함.
  - 사용자
    - 루트 사용자와 마찬가지로 AWS 콘솔에 아이디와 비밀번호로 접속 가능.
    - 그룹에도 속할 수 있지만 사용자는 부여된 정책에 한해서만 리소스에 접근.

## 5. IAM 접속 방법 – 사용자 인증



## 6. IAM 구성 – 그룹, 역할과 정책

---

- 그룹
  - 사용자 관리를 편리하게 하는 기능
  - 그룹에 정의된 특별한 정책은 그룹에 속한 모든 사용자가 영향을 줌.
  - 모든 사용자를 수정할 필요 없이 간단히 그룹으로 묶어 그룹 권한을 수정함.
- 역할
  - 사용자와 유사하지만 비밀번호를 통해 접속할 수 없고 그룹에 속할 수도 없다.
  - 사용자와 마찬가지로 정책에 한해서만 리소스에 접근할 수 있다. 그러나 정책이 부여되지 않았다면 아무것도 할 수 없다.
  - 또한 리소스가 다른 리소스를 사용할 때도 역할이 필요하다.
- 정책
  - AWS 리소스에 접근하기 위해 권한을 허용할지 거부할지를 결정
  - JSON 형태로 저장되며 각 그룹, 사용자, 역할에 부여할 수 있다.
  - 기존 AWS에서 제공하는 정책들을 이용하여 고객이 직접 관리하는 정책을 만들 수 있으며 더욱 정밀하게 설정할 수 있다.

# 7. 로그인 주소의 차이

---

## 루트 사용자 로그인

이메일

synabreu@outlook.com

비밀번호

로그인

로그인 화면

## IAM 사용자로 로그인

계정 ID(12자리) 또는 계정 별칭

534520364753

사용자 이름:

암호:

이 계정 기억하기

로그인

계정 하위 로그인

- 일반 접속 주소(루트 계정): <https://console.aws.amazon.com/console/home>
- 계정 하위 로그인: [https://\[사용자ID\].signin.aws.amazon.com/console](https://[사용자ID].signin.aws.amazon.com/console)

## 8. IAM 유의사항

- 계정 루트 사용자는 모든 AWS 서비스에 대한 완전한 액세스 권한을 가짐

Create an AWS account

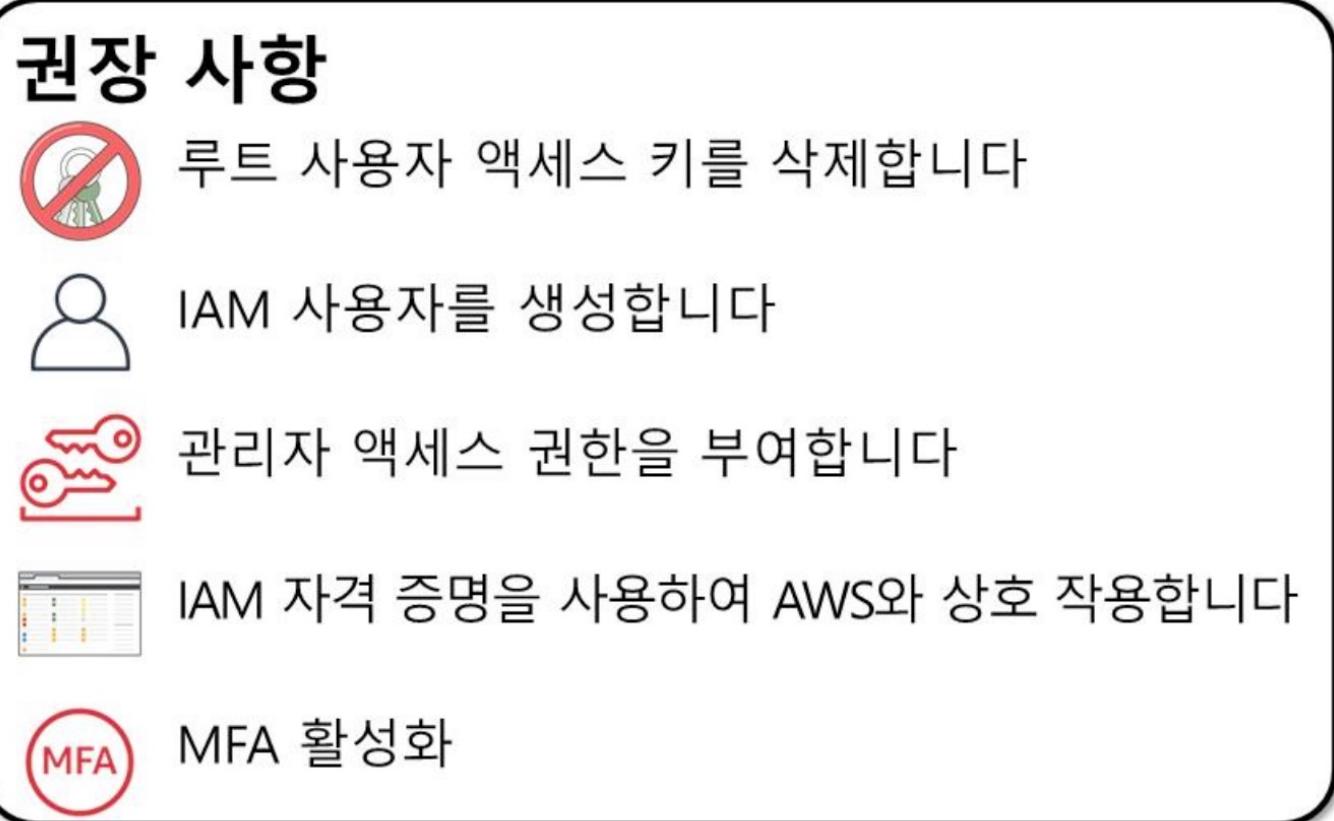
Email address  
newuser@example.com

Password  
\*\*\*\*\*

Confirm password  
\*\*\*\*\*

AWS account name ⓘ  
examplecorp

Continue



## 9. 사용자 추가 – 권한설정 및 태그

---

- 사용자 추가 - 권한 설정
  - 그룹에 권한을 부여한 후 사용자를 그룹에 포함시키는 방법
  - 기본 사용자의 권한을 복사하는 방법
  - 기존 정책을 연결하는 방법
- 태그
  - AWS 리소스를 식별(구분)하거나 확인하기 위한 용도로 사용.
  - 주요한 용도로 리소스들을 그룹화하여 관리하기 위한 용도로 사용.

# 실습 – IAM에서의 사용자 만들기

