AWS기반 리눅스 서버 구축

AWS 기초 강의

- **박 예 원**

Digital learning Team

Cloud Developer

목차

IAM (Identity and Access Management)

- **AWS 서비스 및 리소스에 대한 액세스 관리**
- **AWS 사용자 및 그룹 단위로 액세스 권한 관리**

IAM (Identity and Access Management)

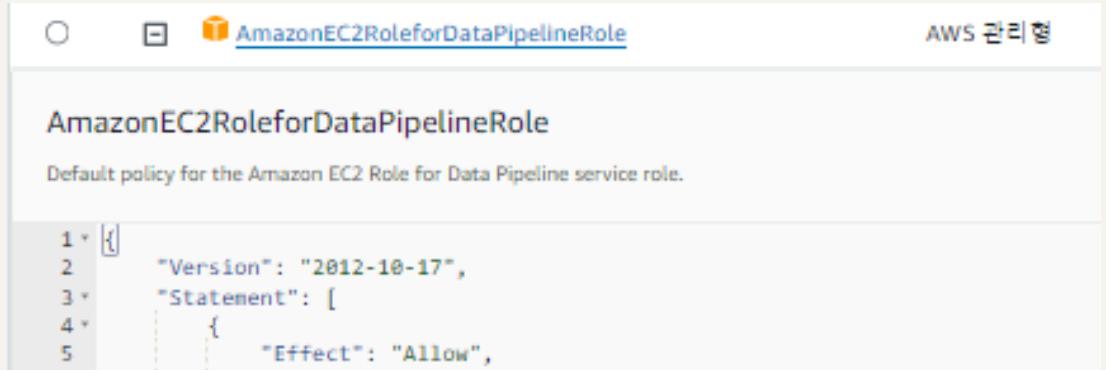
- **AWS Account / Resource / User / Service 권한 제어**
  - 서비스 사용을 위한 인증 정보 부여

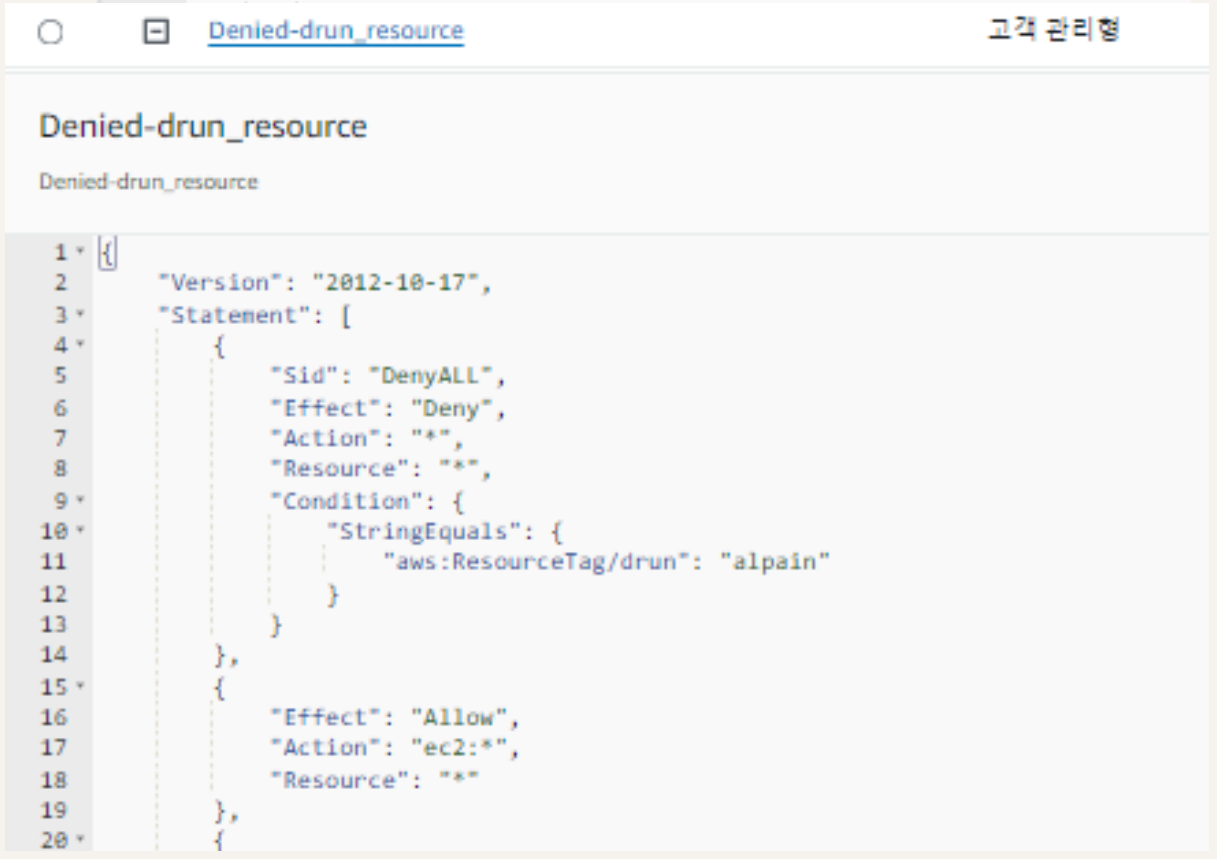
- **사용자 생성 및 계정 보안 관리**
  - 서비스 사용을 위한 인증 정보 부여

글로벌 서비스

IAM 구성

- **Policy / 정책**
  - **권한을 정의하는 AWS 객체**
  - **Json 형식으로 정의**
  - **AWS 제공 정책 (AWS 관리형)**
  - **Custom 정책 (고객 관리형)**





IAM 구성

- **Policy / 정책**

  Version : IAM 정책 언어 버전

  Id : 정책 식별 ID (opt)

  Statement : 권한 정의 영역

  Sid : Statement id로써 문장 식별 id (opt)

  Effect : 허용/거부 여부

  Principal : 정책이 적용될 주체

  - User, account, role 등

  Action : 허용하거나 거부할 AWS 작업

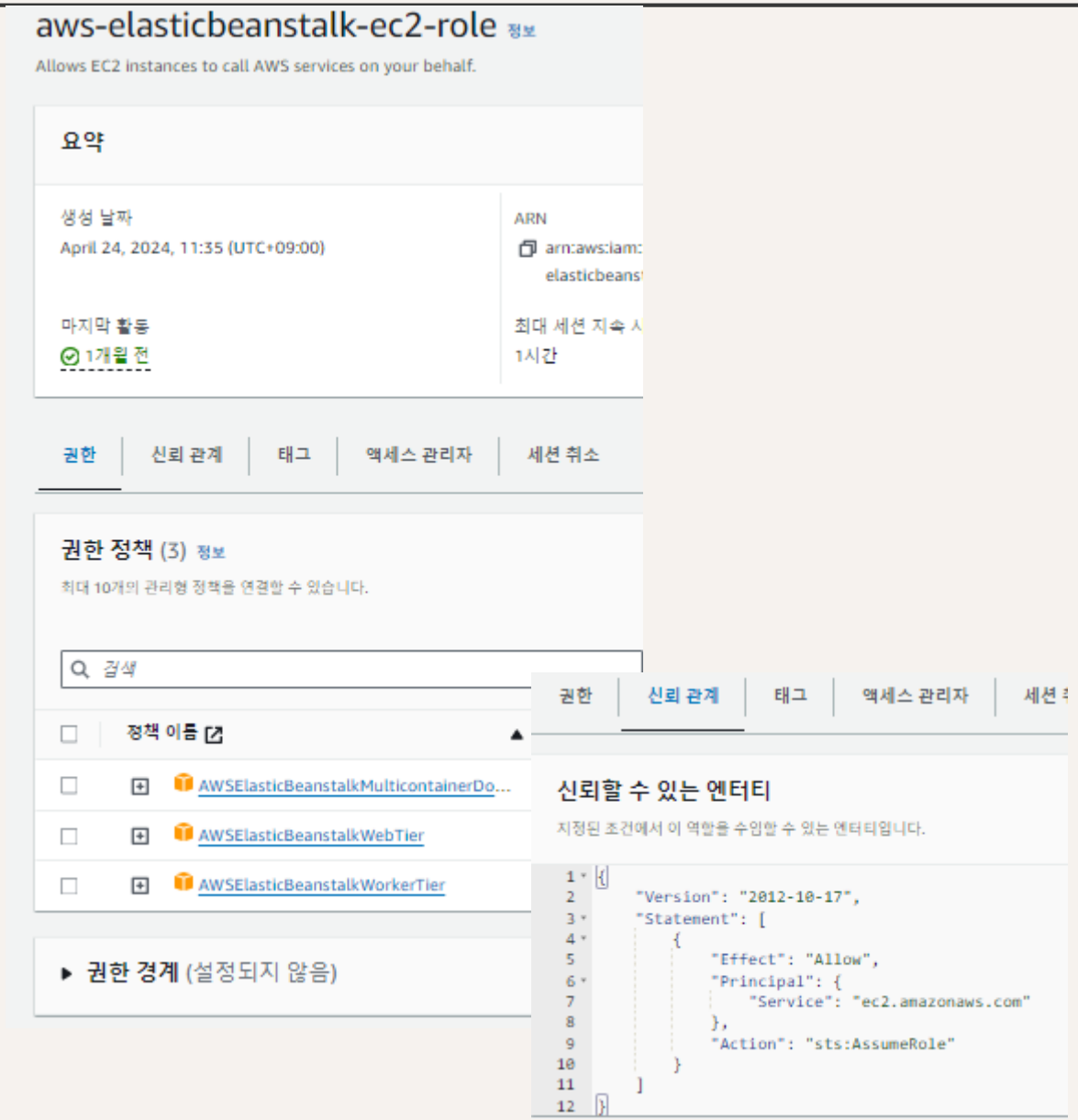
  Resource : 작업이 적용되는 대상의 정보

  - ARN으로 표현

```
{
  "Version": "2012-10-12",
  "Id": "...",
  "Statement": [
  {
    "Sid": "1",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["arn:aws:iam:12345:root"]
    },
    "Action": ["s3:GetObject", "s3:PutObject"],
    "Resource": ["arn:aws:s3::mybucket/"]
  }
  ]
}
```

IAM 구성

- **Roles / 역할**
  - 사용자나 리소스에 할당
  - 최소 권한 원칙
  - 권한(Policy) 부여
  - 신뢰 관계 부여



IAM 구성

- **Root 계정과 최소 권한의 원칙**
  - **최초 생성된 계정은 Root 계정**
  - **Root 계정은 사용자를 생성하는 용도 (공유 금지)**
  - **많은 권한은 비용이나 보안 문제를 야기함**
  - **필요 이상의 권한은 제공하지 않기**

Summary

IAM	AWS 액세스 관리
정책(Policy)	권한을 정의하는 AWS 객체
역할(Role)	권한을 임시로 부여 받는 AWS 객체
IAM 관리 원칙	Root 계정 보호 / 최소 권한의 원칙

감사합니다.

Thank You