AWS IAM 설정

AWS 에서는 서비스를 안전하게 이용하기 위해 권한을 설정할 수 있습니다.이러한 권한은 AWS Identity and Access Management(IAM) 이라는 서비스를 이용하여 설정하게 됩니다.이 글에서는 AWS IAM 이란 무엇인지 알아봅니다.기초적인 내용을 살펴보기 때문에 올바른 모범 사례나 리소스의 상세 설정에 대한 설명 등은 기술하지 않습니다.

AWS IAM

> AWS Identity and Access Management(IAM)은 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스입니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다. - AWS IAM

서두에서 설명한 것과 같이 AWS 리소스에 대한 액세스를 제어하는 서비스입니다.

IAM 기능

공식 문서를 보면 IAM의 기능으로서 여러 기능들이 기술되어 있지만 정리하자면

누가, 무엇을, 어떻게 할 것인지에 대해 인증과 인가를 제어

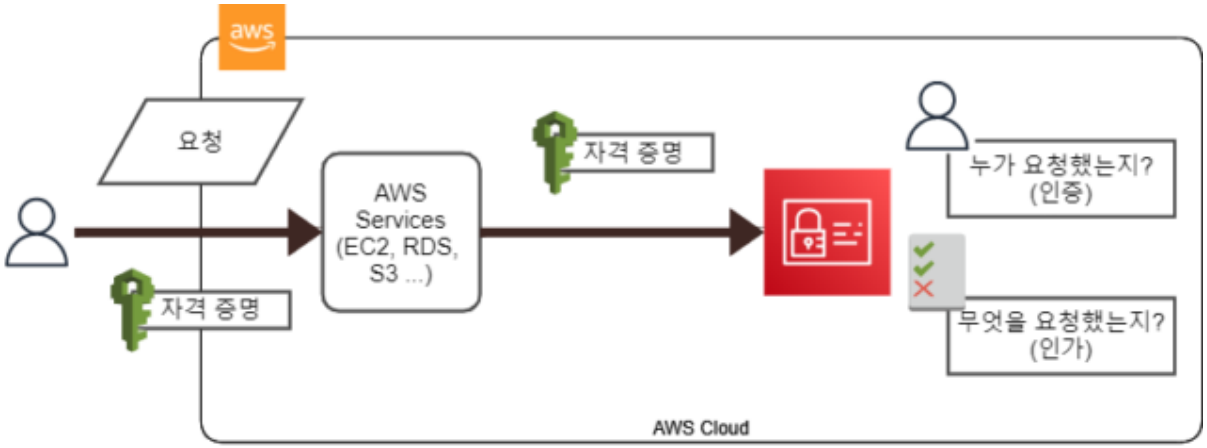
하는 서비스입니다.

(출처 - **공식 페이지**)

자세히 보자면 어떤 유저가 어느 AWS 서비스에 어떠한 요청을 보내면서 인증을 위한 유저의 자격 증명도 함께 보냅니다.

AWS 서비스에서는 해당 요청을 처리하기 전에 우선 자격 증명을 IAM에 보냅니다.

그리고 IAM에서는 해당 자격 증명을 보고 해당 유저가 올바른 유저인지(인증), 유저가 올바르다면 해당 서비스와 서비스의 기능을 이용해도 되는지(인가) 등을 판별한 뒤 문제가 없다면 서비스 이용을 허용합니다.



또한 AWS 계정을 생성하면 모든 권한을 가진 루트 유저가 기본적으로 생성되어 있습니다. 하지만 루트 유저를 그대로 이용하면 보안 측면이나 운영 측면으로 좋지 않기 때문에 IAM의 유저나 역할을 이용하여 AWS를 이용하는 것이 일반적입니다.

이 외에도 다른 AWS 계정 간에 리소스를 이용하기 위한 교차 계정 액세스 등을 위해서 IAM을 이용합니다.

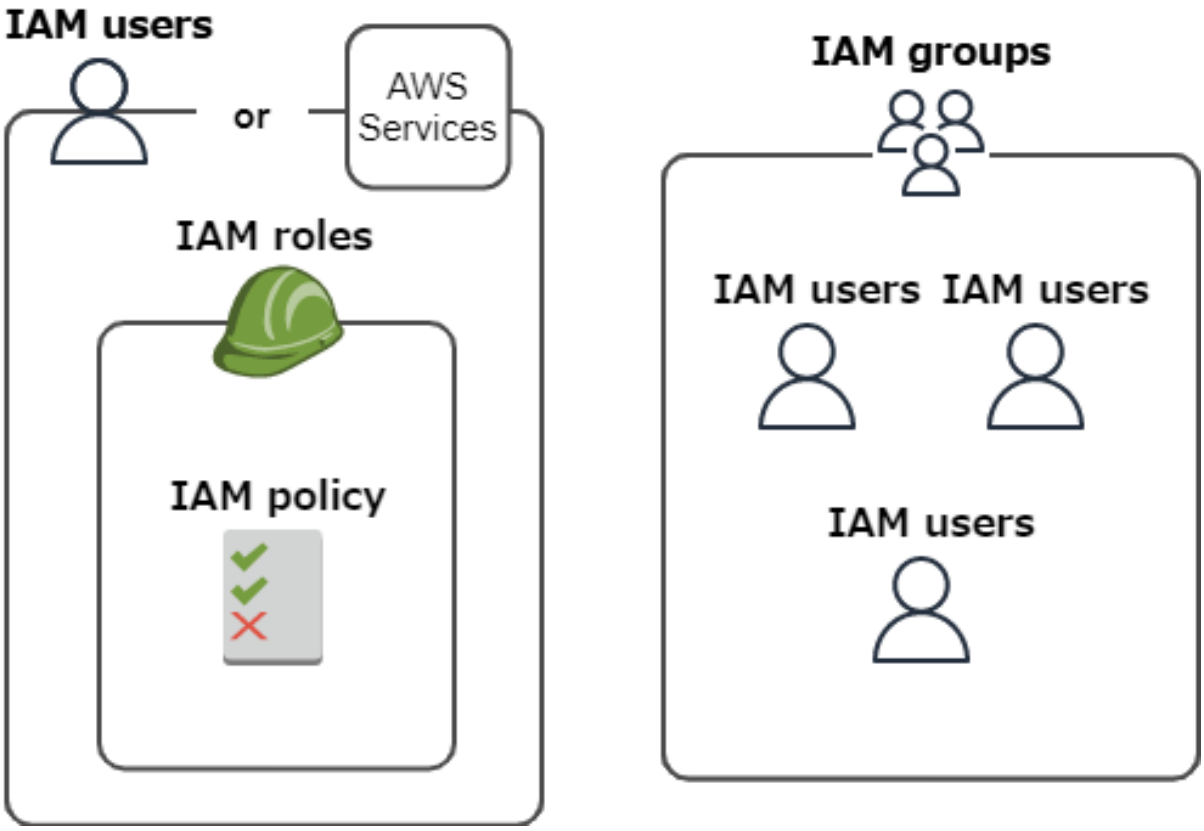
IAM의 리소스

IAM 에서 관리하는 리소스를 크게 보면 다음과 같습니다.

- IAM 사용자(users)
- IAM 그룹(groups)
- IAM 역할(roles)

- IAM 정책(policy)

정책에는 어떠한 권한에 대한 상세한 설정을 합니다. 그리고 이 정책을 역할을 연결하고, 역할은 사용자나 AWS 리소스에 연결되어 해당 리소스나 유저의 권한을 설정합니다.



IAM의 리소스에 대해 더 상세히 알고 싶다면 **공식 문서**를 참고해주세요.

IAM 사용자

IAM 사용자는 **인증** 을 위한 리소스입니다. IAM 사용자를 만든 후에는 다음 자격 증명을 생성할 수 있습니다.

- 관리 콘솔에 로그인하기 위한 비밀번호
- 자격 증명(액세스 키 ID, 비밀 액세스 키)

사용자는 반드시 사람일 필요가 없으며 어플리케이션 등에서 액세스 키 ID나 비밀 액세스 키를 활용하여 인증을 하는 데에도 많이 사용됩니다.

IAM 역할

IAM 유저나 특정 AWS 서비스들은 IAM 역할을 이용하여 권한을 설정할 수 있습니다.

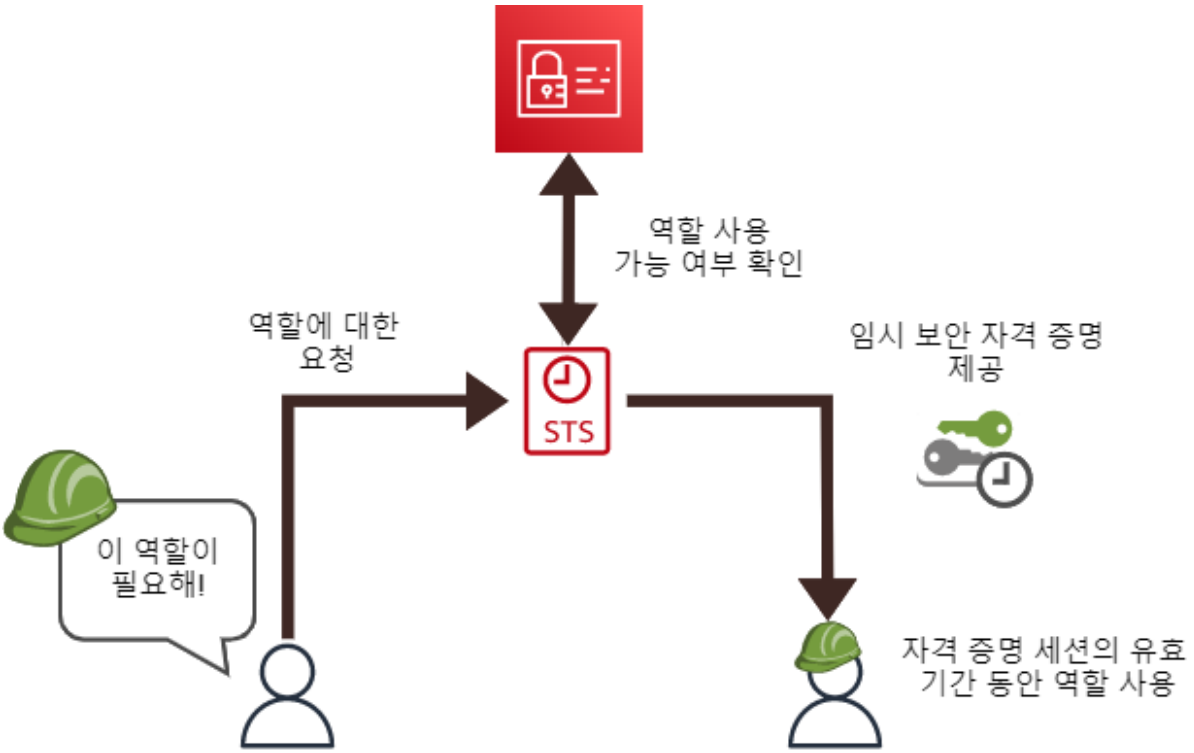
IAM 역할도 **인증** 을 위해 사용되지만 유저와 다른 점은 역할 자체가 요청을 보내는 주체가 되지는 않습니다.즉 역할을 맡은 유저나 서비스가 요청의 주체가 됩니다.

또한 역할은 하나의 유저에 귀속되지 않고 해당 역할이 필요한 모든 유저나 서비스에 연결될 수 있습니다.

귀속되지 않기 때문에 유저가 해당 역할을 이용하기 위해 AWS Security Token Service(STS) 라는 서비스에 임시 보안 자격 증명을 요청합니다.

그럼 STS에서 IAM에 해당 유저가 역할을 맡을 수 있는지 확인한 후 역할을 이용할 수 있는 임시 보안 자격 증명을 제공합니다.

그리고 해당 증명 세션이 유효한 시간 동안 유저는 해당 역할의 권한이 이용 가능합니다.



IAM 역할은 IAM 사용자 뿐만 아니라 AWS 서비스나 자격 증명 공급자(IdP)로 인증된 외부 사용자 그리고 다른 AWS 계정의 사용자에게도 연결할 수 있습니다.다른 AWS 계정과 연결하는 경우에는 본인의 계정 내의 서비스를 다른 계정과 공유해야하는 경우에 많이 사용됩니다. 설정 방법은 **공식 문서**를 참고해주세요.

AWS 외부에서 자격 증명을 관리하고 있는 경우 IAM 사용자를 생성하는 대신 IAM 자격 증명 공급자를 사용할 수 있습니다.IAM은 OpenID Connect(OIDC) 또는 SAML 2.0(Security Assertion Markup Language 2.0)과 호환되는 IdP를 지원합니다.자세한 내용은 **공식 문서**를 참고해주세요.

IAM 역할에 누가 연결할 수 있는지는 다음과 같이 신뢰 관계로 정의합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

IAM 정책

IAM 정책은 권한을 부여하는 리소스입니다.

IAM에는 다음과 같은 6가지 정책 유형이 있습니다. 가장 자주 사용하는 정책 유형에서 빈도가 낮은 정책 유형 순으로 나열하면 다음과 같습니다.

- 자격 증명 기반 정책
- 리소스 기반 정책
- 사용 권한 경계(Permissions boundary)
- Organizations SCP
- 액세스 제어 목록(ACL)
- 세션 정책

이 중 많이 쓰이는 자격 증명 기반 정책과 리소스 기반 정책에 대해 간략히 설명하자면 다음과 같습니다.

자격 증명 기반 정책IAM 자격 증명(사용자, 역할, 그룹)에 연결할 수 있는 소위 IAM 정책입니다. 무슨 작업을 어느 리소스에서 어떤 조건에서 수행할 수 있는지를 제어하는 JSON 권한 정책 문서(Permission Policy)라고 합니다.

자격 증명 기반 정책은 다음과 같은 종류로 나누어져 있습니다.

- 관리형 정책
    - AWS 관리형 정책(AWS에서 생성 및 관리하는 관리형 정책입니다.)
    - 고객 관리형 정책
- 인라인 정책

관리형 정책은 독립적인 자원입니다. 어떤 자격 증명에도 연결되지 않은 상태에서도 존재할 수 있으며, 여러 자격 증명에서 공유할 수도 있습니다.인라인 정책은 자격 증명에 내장된 형태로 존재하는 것으로, 자격 증명의 파라미터 중 하나로서 생각하는 것이 이해하기 편합니다.

리소스 기반 정책요청이 적용되는 AWS 리소스 측에 연결하는 정책입니다.모든 리소스가 리소스 기반 정책을 지원하는 것은 아닙니다. 지원되는 리소스는 **공식 문서**에서 확인할 수 있습니다.

각 정책 유형을 하나하나 알아보기에는 너무 길어지므로 상세한 내용은 **공식 문서**를 참고해주세요.

액세스 제어 목록 이외의 유형의 IAM 정책은 모두 JSON 형식으로 정의됩니다. 필요한 요소를 적용하여 어떤 리소스를 사용할지, 해당 정책은 어떤 요청에 대해서 적용되는지, 어떤 조건에서만 허용 및 거부를 할지 등을 조절할 수 있습니다.정책 요소의 상세한 내용은 **공식 문서**를 참고해주세요.

IAM 그룹

IAM 그룹에는 IAM 사용자 또는 IAM 역할과 달리 자격 증명이 없습니다. 인가를 담당하는 IAM 정책을 여러 IAM 사용자에게 효율적으로 배포하기 위한 틀이라고 생각하면 됩니다.

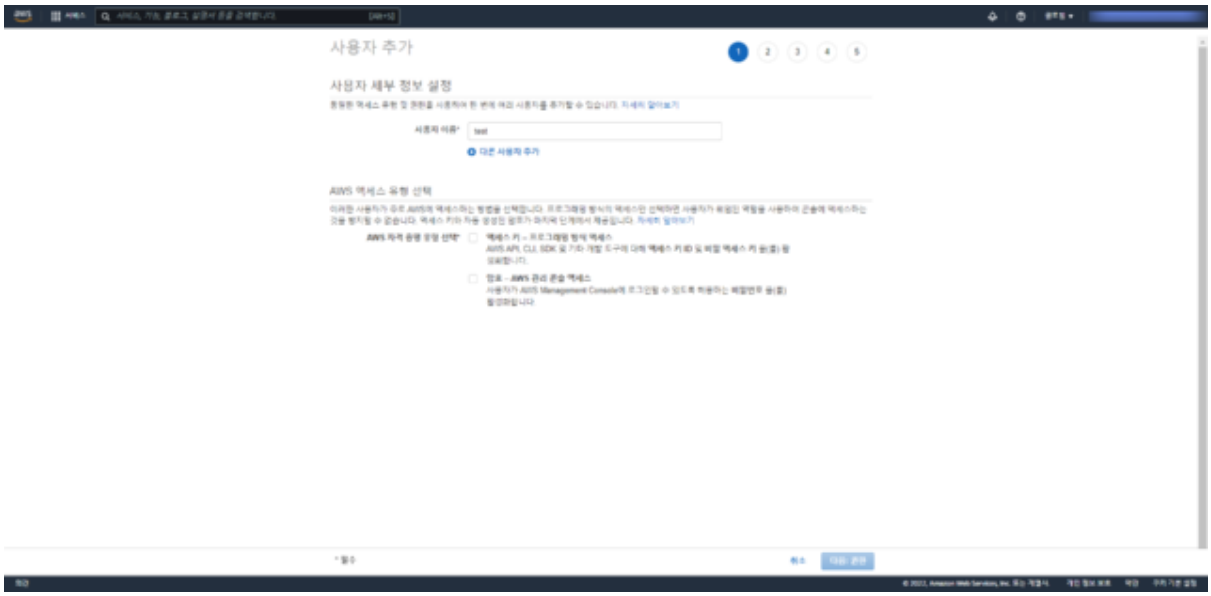
IAM 리소스 만들어보기

콘솔에서 IAM 사용자와 IAM 역할, IAM 정책을 생성해보겠습니다.무엇을 먼저 만들어야 한다는 순서는 따로 없으며 작성하더라도 나중에 자유롭게 수정 할 수 있습니다.이어서 실제로 작성하는 방법을 간단하게 설명합니다.

IAM 사용자 만들기

우선 IAM 사용자부터 작성해보겠습니다.

IAM 사용자의 작성은 IAM 서비스 콘솔의 [사용자] 에서 만들 수 있습니다. [사용자 추가]를 클릭하면 다음과 같은 화면이 표시됩니다.



이 중 해당 사용자가 어떤 방식으로 로그인하는지 선택한 후 권한이나 그룹 등의 설정 없이 사용자를 만듭니다.

마지막 화면에 나오는 액세스 키는 해당 화면에서 받지 않으면

똑같은 액세스 키를 다시 발급 받을 수 없으니 꼭 다운로드

합니다.

IAM 역할 만들기

IAM 서비스 콘솔의 [역할]에서 만들 수 있습니다.

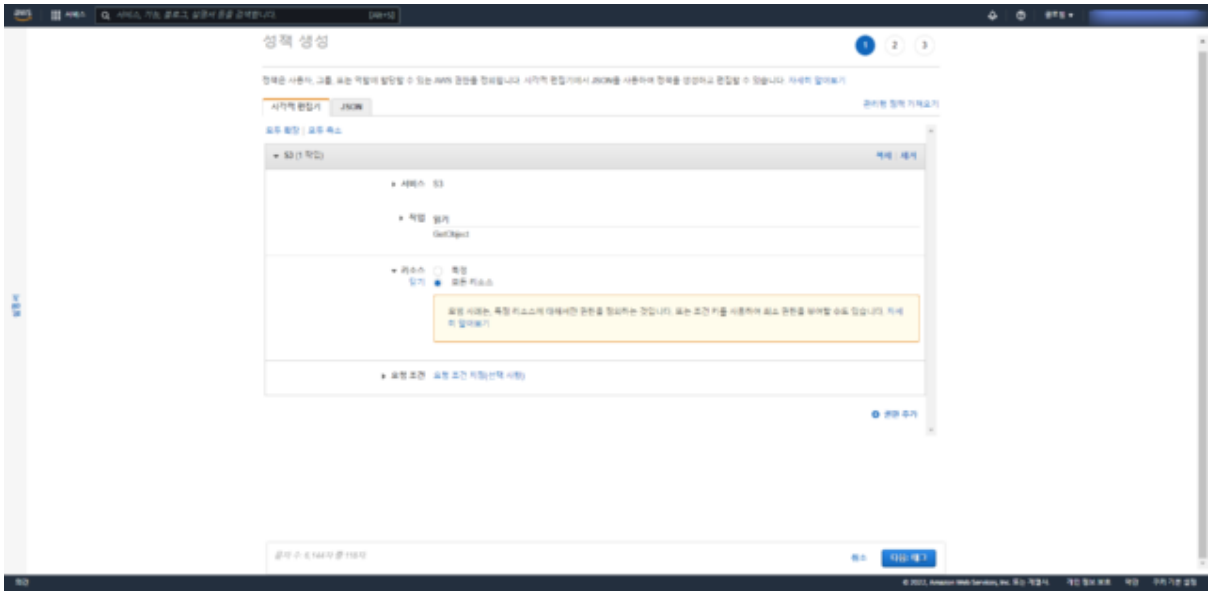
위에서 설명한대로 해당 역할을 연결할 자격 증명(엔터티)를 선택하여 생성합니다.

마찬가지로 권한은 설정하지 않고 역할 이름 등을 설정한 후 그대로 만듭니다.

IAM 정책 만들기

IAM 서비스 콘솔의 [정책]에서 만들 수 있습니다.

화면과 같이 에디터나 json 으로 값을 설정할 수 있습니다.



정책은 필요한 권한만을 부여하는 최소 권한 원칙을 지키는 것이 모범 사례입니다.

이후 작성한 사용자나 역할의 [권한 추가] 를 통해 작성한 IAM 정책을 연결하는 것이 가능합니다.