[IAM - Identity And Access Management]

-계정 권한 관리

-**AWS 의 계정 및 권한 관리 서비스**이다

-AWS 서비스 + 리소스에 대한 접근 관리

-리전 단위 X

-계정 보안 강화 목적 - **" 루트 계정은 최초 계정생성 이후는 사용하지 않는것 권장 "**

- 루트계정말고, **IAM 계정으로 서비스를 사용하고 최소한의 권한만 부여**한다(최소권한 원칙)

-**루트계정 - 개별사용자** 사이 : **강력한 암호 + 멀티팩터인증(MFA)- 다중 인증이라고 생각하면된다 -- 적용**이 된다.

-사용자의 암호 복잡성 요구 + 의무 교체 주기 적용

-엑세스 키를 공유지 않도록

-**루트 계정없이도 연락처 정보 / 결제 통화기본설정 / 리전 등의 설정 가능**하다

" 만약 AWS IAM 사용자 권한을 실수로 부여하거나 삭제한 경우 ? "

루트 사용자 로그인 후 -> 정책 수정을 통해서 복원이 가능하다.

[루트 계정이 필요한 경우 ?]

1. **루트계정 관련된** 엑세스 키나 암호, 이메일 주소 , 계정 이름 등의 계정 설정을 변경할 때 사용한다
2. **AWS 계정을 닫**을때
3. **AWS 지원플랜을 변경 , 취소**할때
4. **인스턴스를 팔려고**할때 (인스턴스 매매가능하다- 마켓플레이스 판매자로 등록가능)
5. MFA - **멀티팩터인증(다중인증) 삭제 Delete를 활성화하도록 Amazon S3 버킷(오브젝트 데이터 저장서비스) 을 구성**할때
6. 잘못된 **VPC(AWS 네트워크임) ID 또는 VPC 엔드포인트 ID가 들어있는 Amazon S3 버킷 정책을 편집하거나 삭제**할때

[IAM 의 엑세스 관리]

밑의 이미지로 한번에 설명이 가능하다.

User 개념은 개인ID, 계정이라고 할 수 있다.

Group 은 User가 모인 집단 즉, 개발팀 혹은 인프라팀 등이라고 할 수 있고

Role 이란 AWS 리소스에서 사용하는 자격증명이다.

ex) AWS EC2에서 실행중인 애플리케이션이 S3스토리지, RDS 데이터베이스 와 같은 AWS 리소스에 엑세스 하는 권한

나아가 **IAM 정책**이라는 용어가 있는데

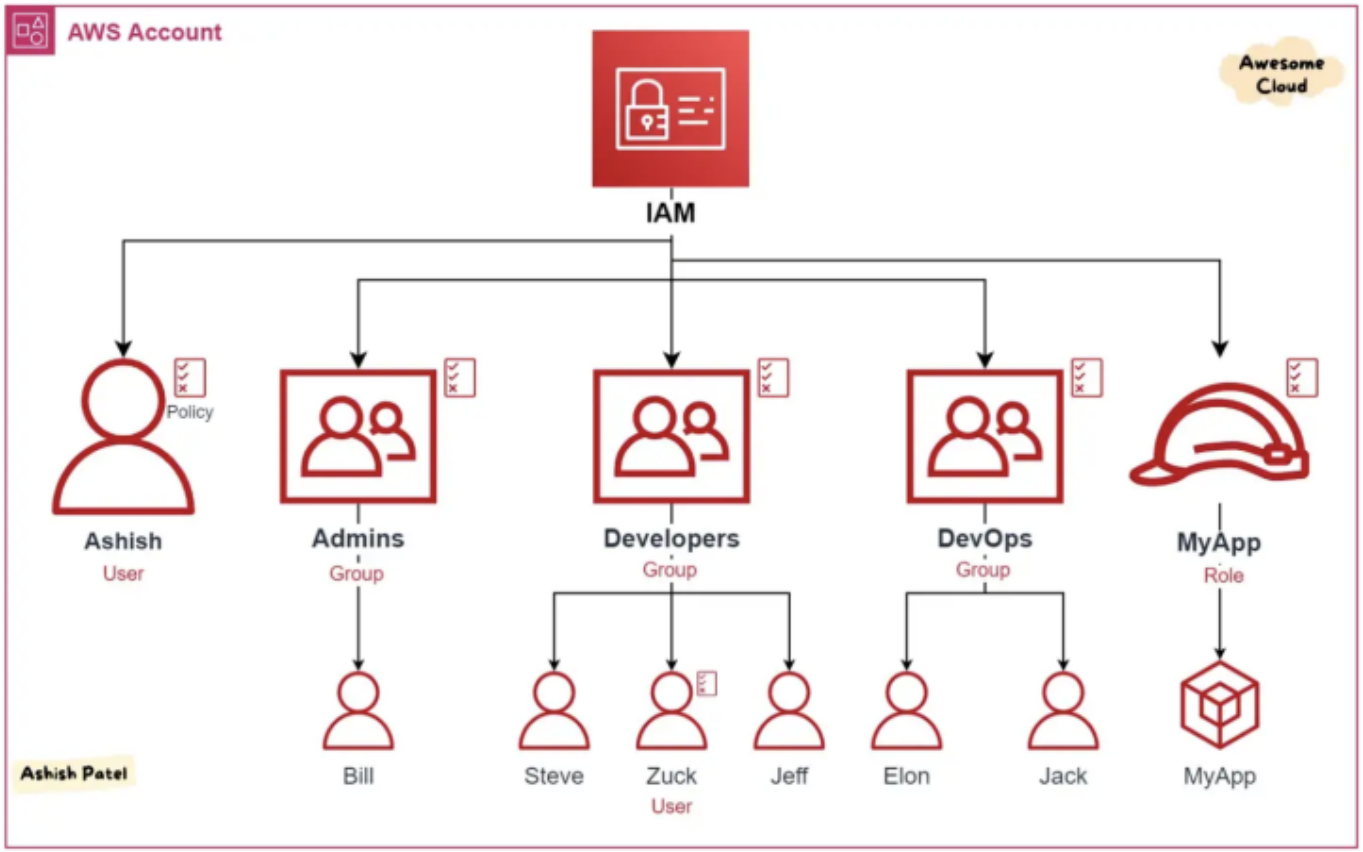
이는 AWS 리소스에 대한 엑세스 권한을 정의 한 것이라고 보면된다.

쉽게 말해 권한을 통해 인증되고, 이후 부여된 리소스 라고 생각하면된다.

AWS 에서 IAM 권장 정책사항은 **그룹으로 관리 , 관리형 정책 사용권장** 이다

그룹으로관리 : **" 개별사용자 User 에게 권한을 직접부여하지말고 속한 Group에 권한을 부여하라 "** 이다.

AWS 관리형 정책은 Json 문서 형식으로 이루어져있다. **정책이 명시가 되지 않는 경우 요청 거부**가 된다.

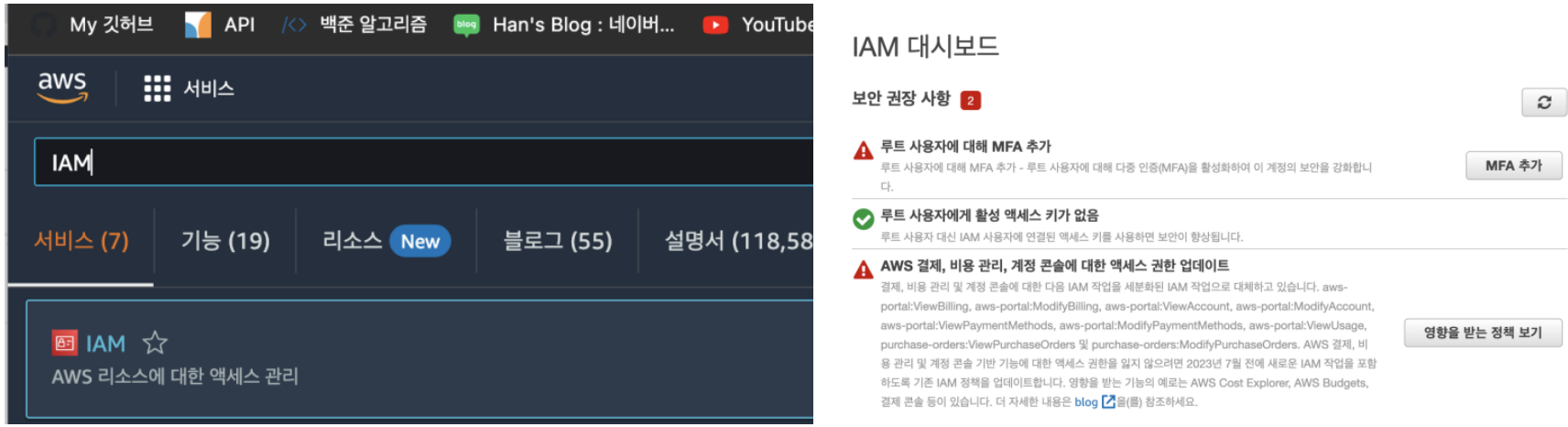


Awesome Cloud — AWS — IAM

IAM 구조 [출처: Awesome Cloud]

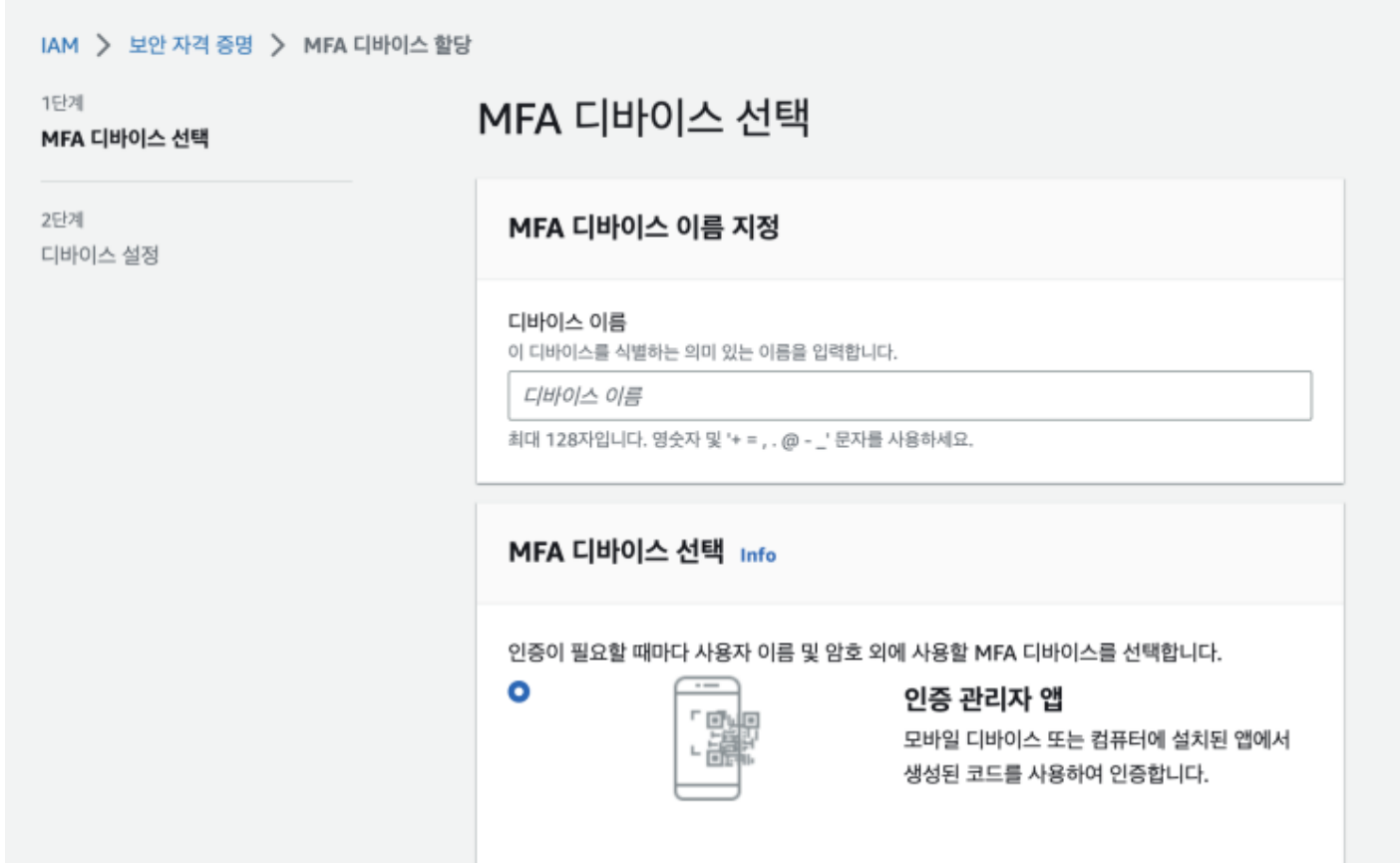
또한 마지막으로 **IAM 자격증명 보고서**를 제공하고 이를 다운받을 수 있다.
보고서에 기재된 정보들을 참고하여 운영할 수 있다.

[IAM 계정 생성 / 권한 부여]



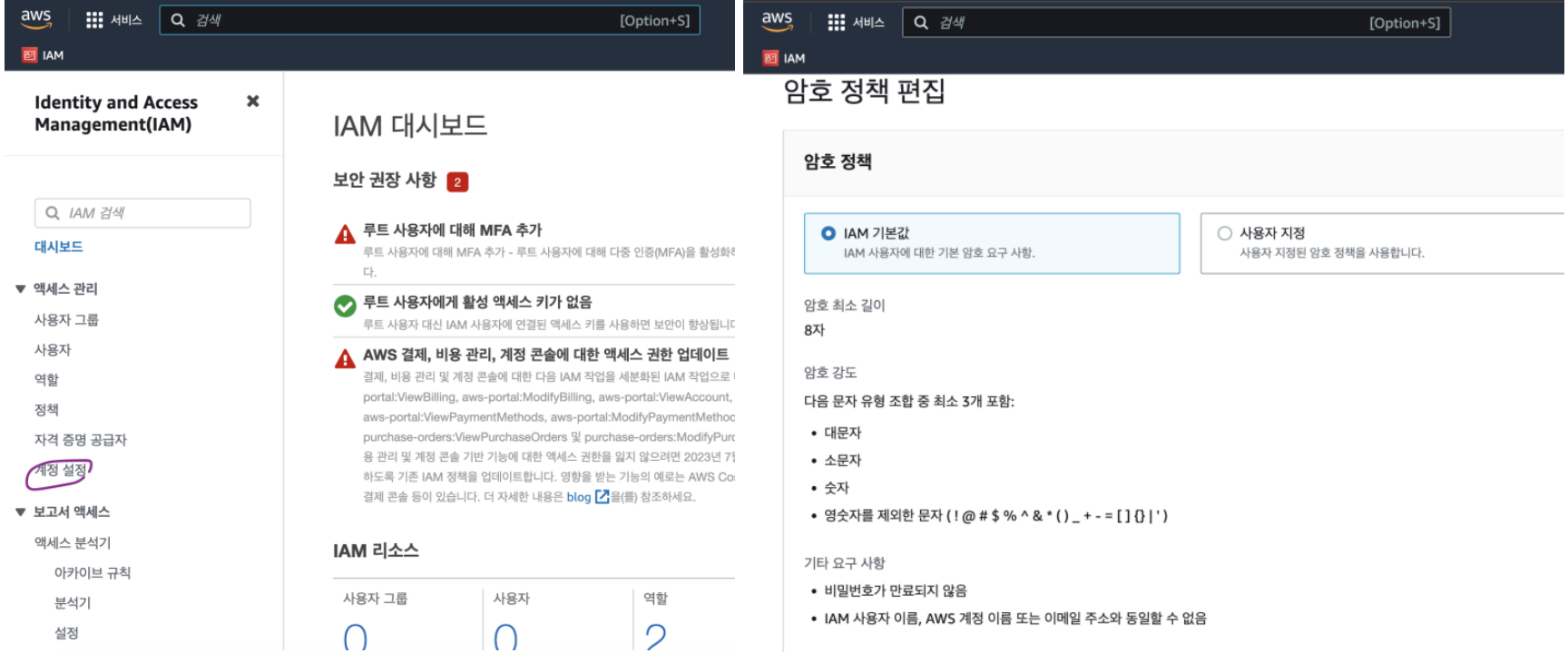
IAM 검색해서 IAM 에 대한 AWS 리소스에 대한 엑세스 관리로 들어간다.- 대시보드에 보면 MFA 도 추가가능

보안 자격증명-MFA (다중 보안이라고 생각) 디바이스 할당하여 아래와 같이 보안을 강화할 수 있다



MFA 활성화 방법

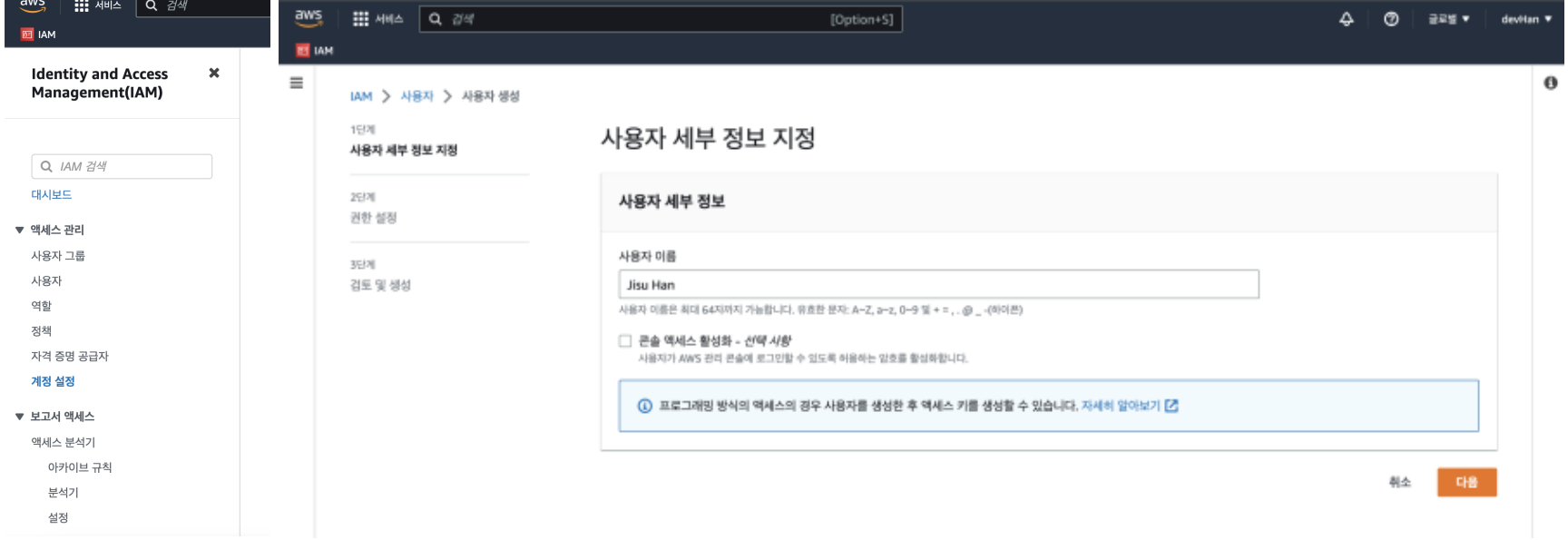
IAM 계정 설정 방법



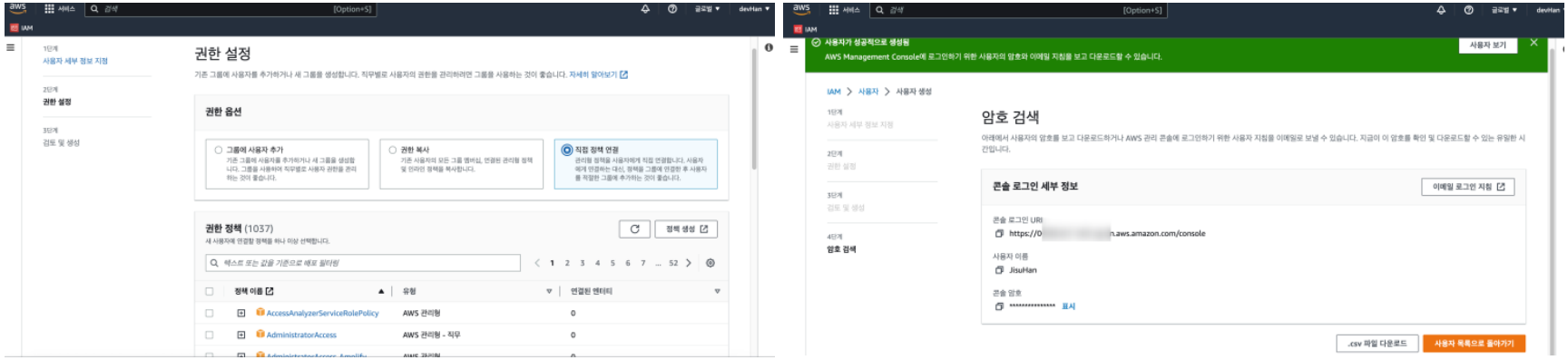
IAM-계정설정 - 암호정책 편집가능

아래 이미지와 같이 IAM 에 실제로 위의 이론에서의 User , Role , Policy 등이 존재한다.

[User IAM 설정]

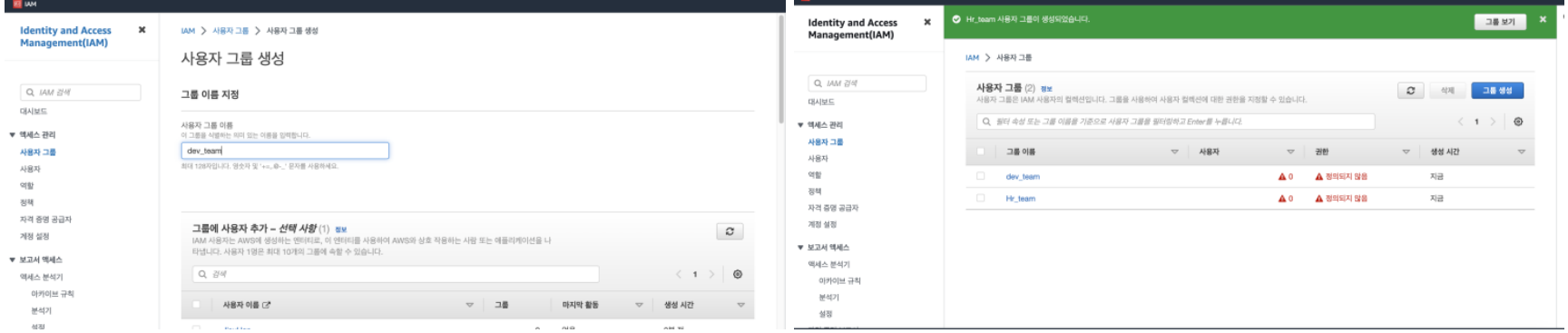


IAM 사용자(User) IAM 설정



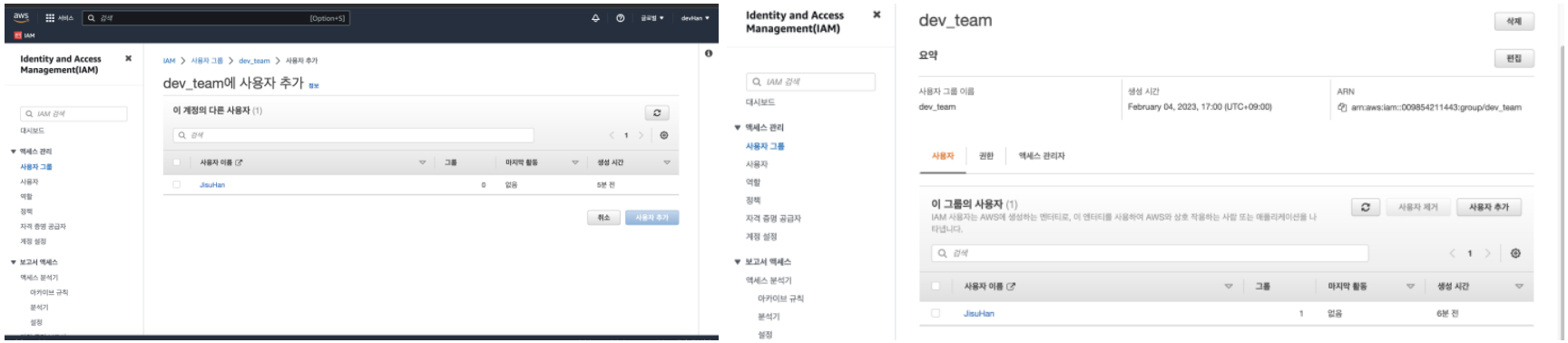
IAM 직접 권한 설정이 가능

[GROUP IAM 설정]



Group 설정을 한다. - 권한은 부여안하고 실습

Group 에는 User를 할당가능하다

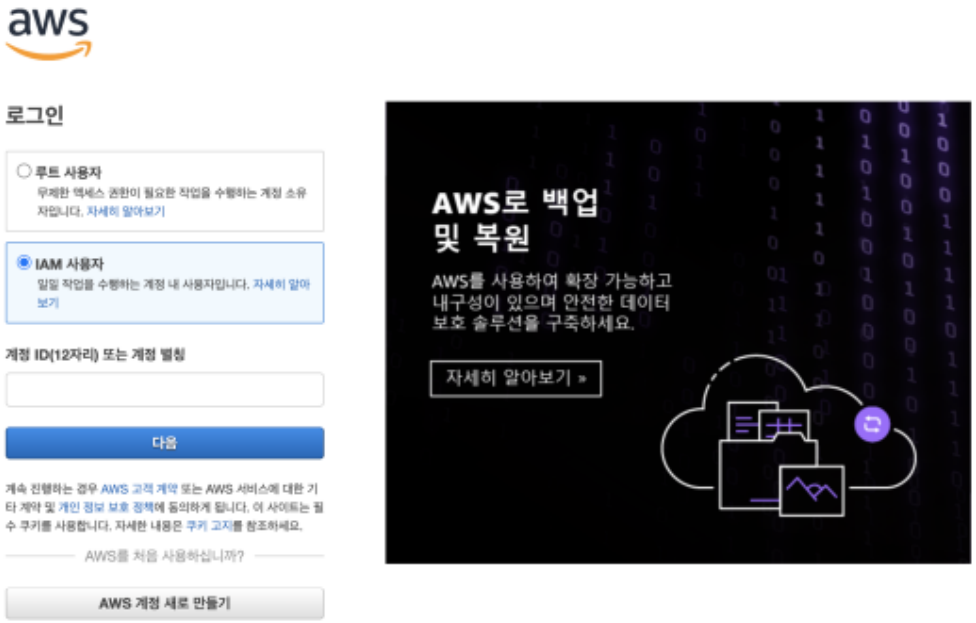


Group 에 User 추가

Group에 Group은 추가가 불가능하다.

이제 IAM 사용자로 콘솔에서 로그인을 해본다.

IAM 에서 로그인아이디는 아래와 같이 IAM 대시보드의 계정ID 12자리를 복사해서 붙여넣으면 된다.



두트가 아닌 IAM 사용자로 로그인

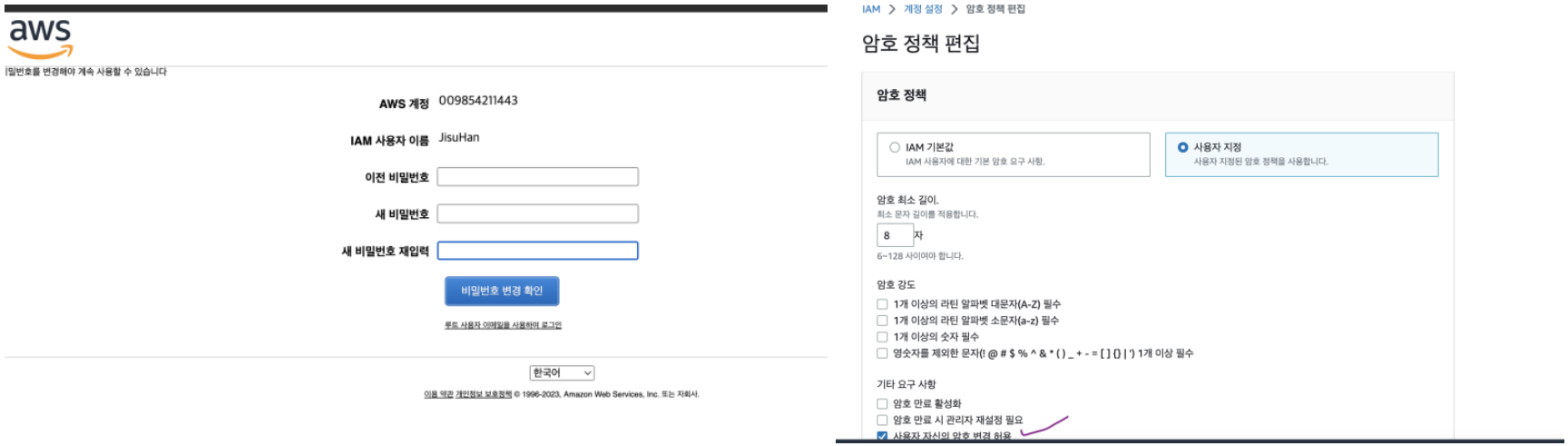
** IAM 최초로그인시 비밀번호 변경 페이지 오류

IAM 최초 로그인 시 본인은 IAM 비밀번호를 변경하고 시작하라고 떴다.

IAM 유저 비밀번호를 정책에 맞게 변경해도 변경이 안되었는데,

이는 IAM으로 들어가서 계정관리 - 사용자 자신의 암호변경 허용 체크를 하고 비밀번호를 변경하면

정상적으로 비밀번호가 변경되고 로그인이 된다.

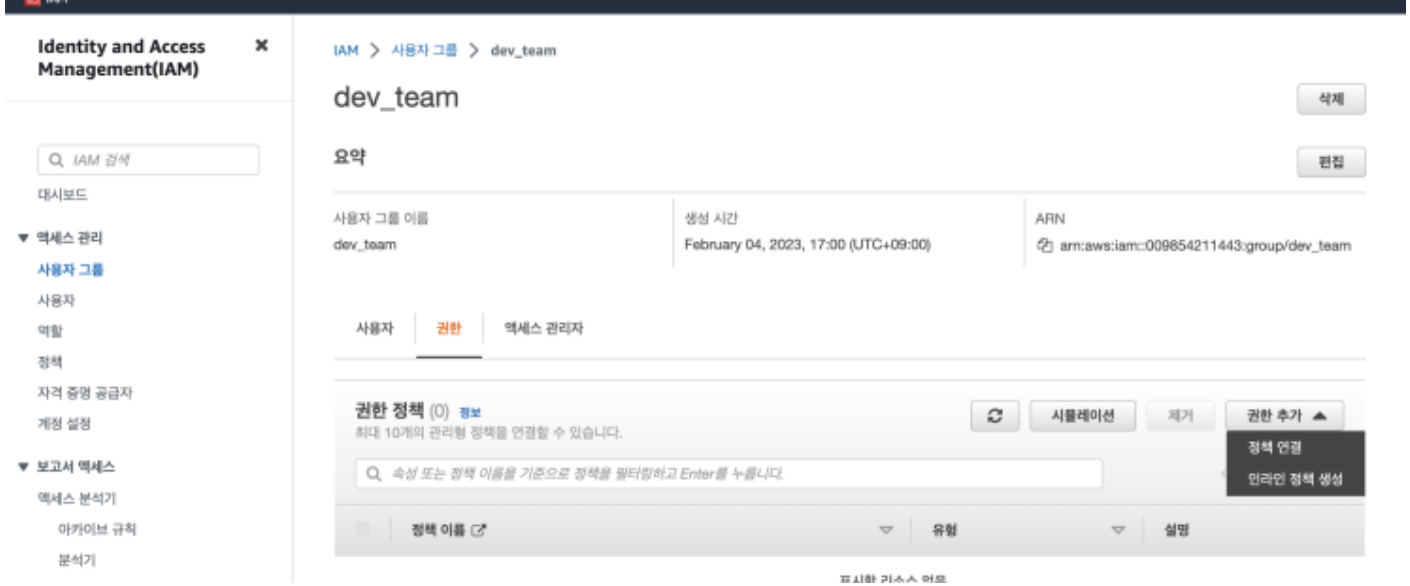


IAM 비밀번호 변경

IAM 로그인 이후 권한을 설정해주지 않으면 ,

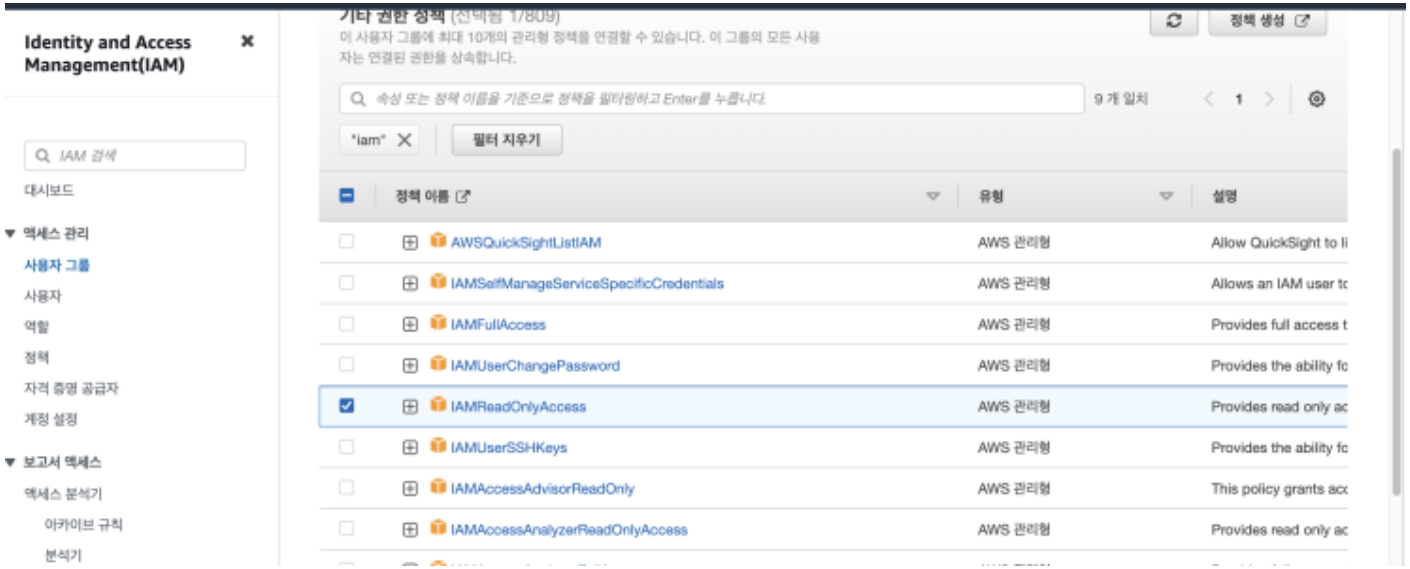
아무 권한이 없다.

따라서 IAM 권한을 설정해준다 - 그룹 사용자인 dev_team 에 권한을 설정해 주도록 하겠다.



IAM - 사용자 그둡 - dev_team 사용자 그둡에 권한을 추가할 것이다.

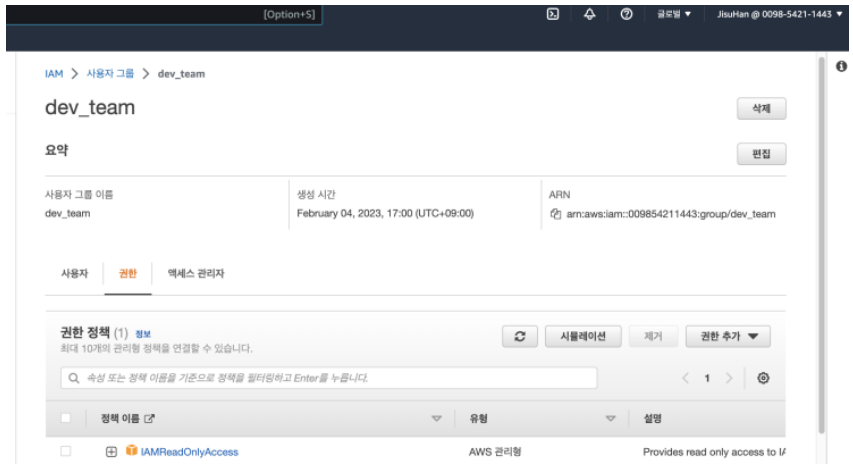
IAM에 read-only 로 IAM 에 대하여 읽기 권한만 있는 권한을 추가하도록한다



IAMReadOnlyAccess 권한 부여

권한 추가 이후 , 사용자 그룹(dev_team) 에 속한 사용자(JisuHan) 도 IAMReadOnlyAccess 를 갖게 된다.

확인해보면 아래와 같다



JisuHan 개인 User IAM 으로 접속해보면 dev_team 사용자 그룹 소속이기 때문에 IAMReadOnlyAccess 권한이 같이 부여되었다.