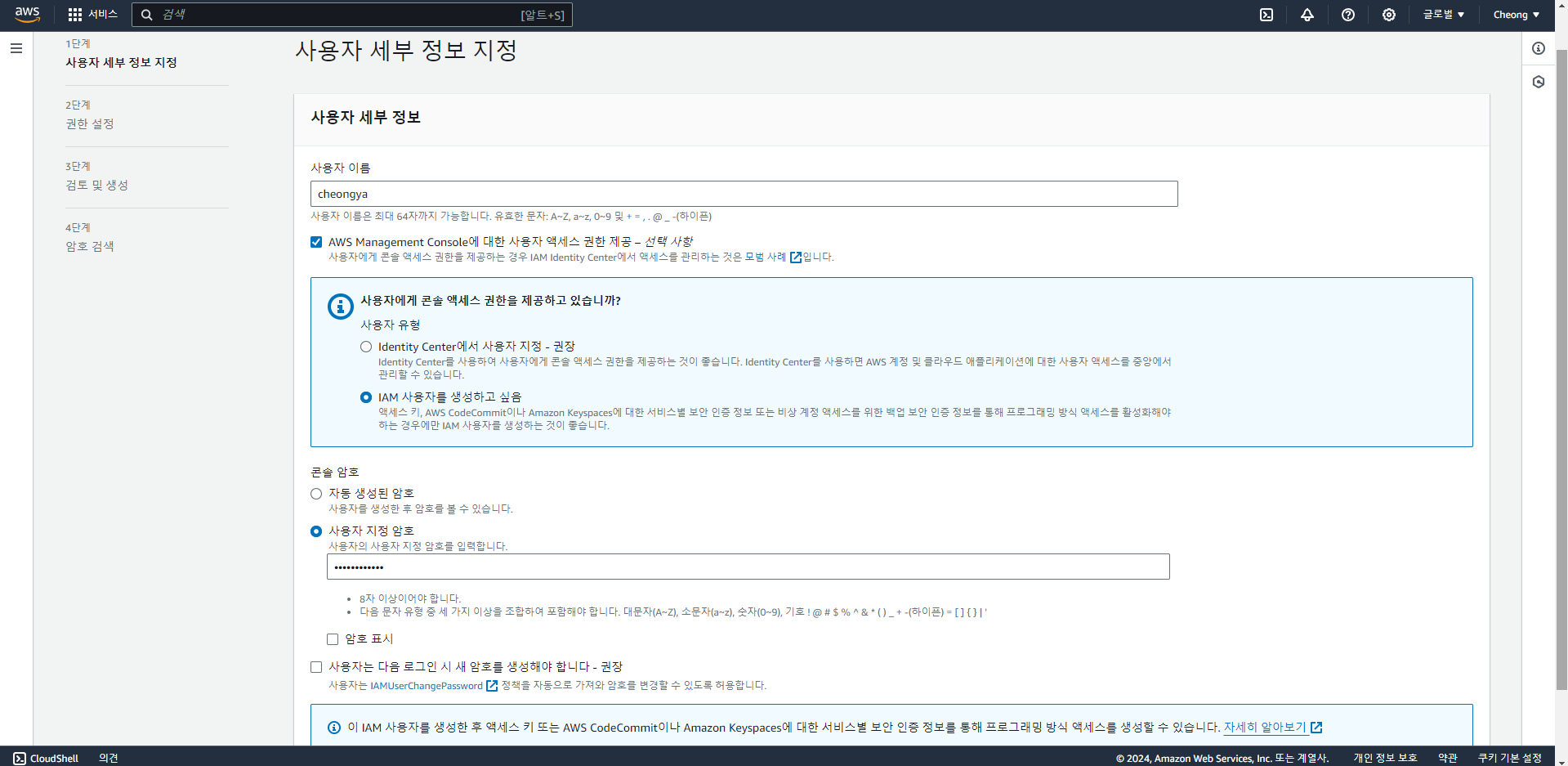
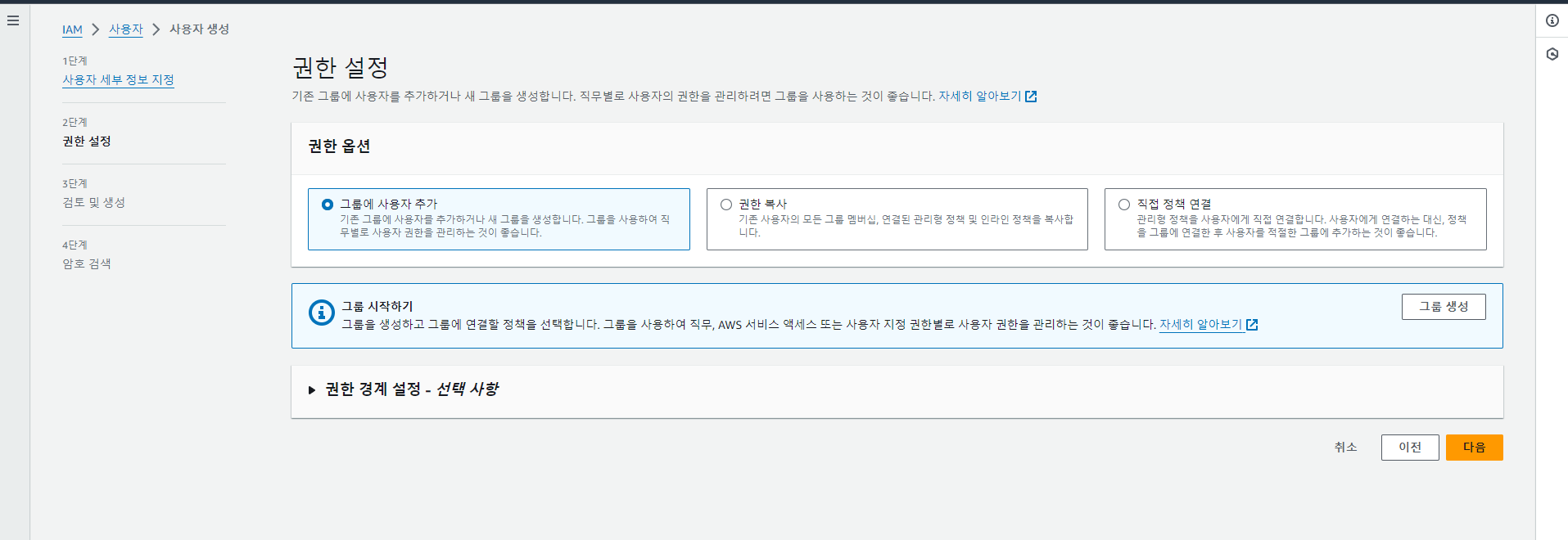
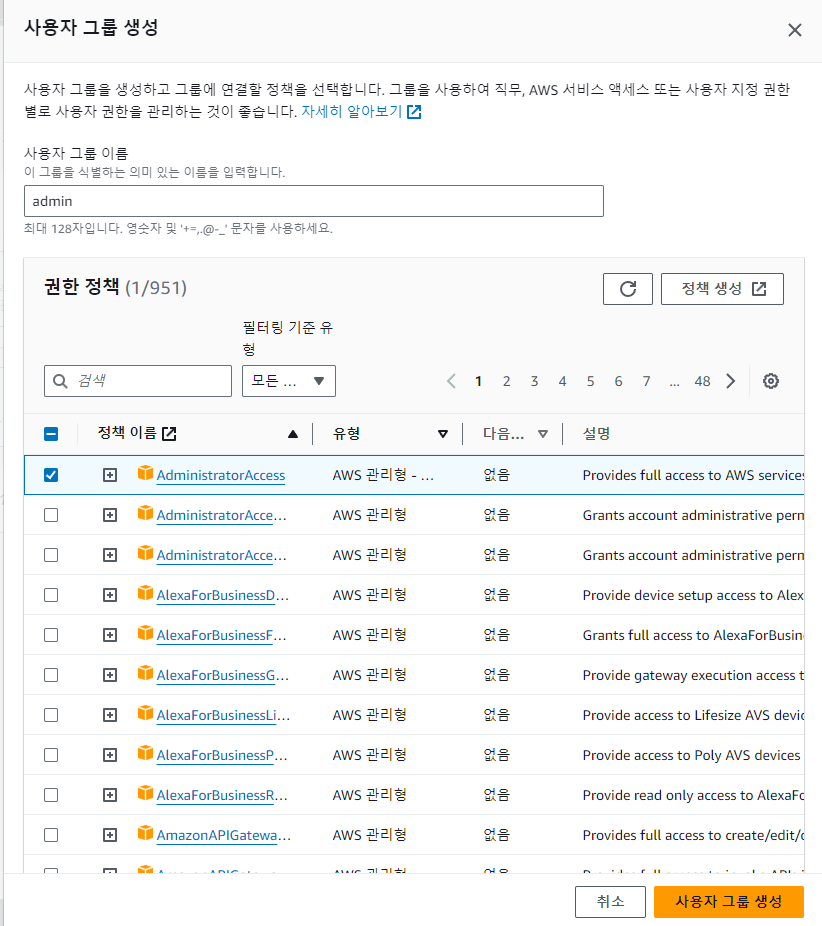
# IAM

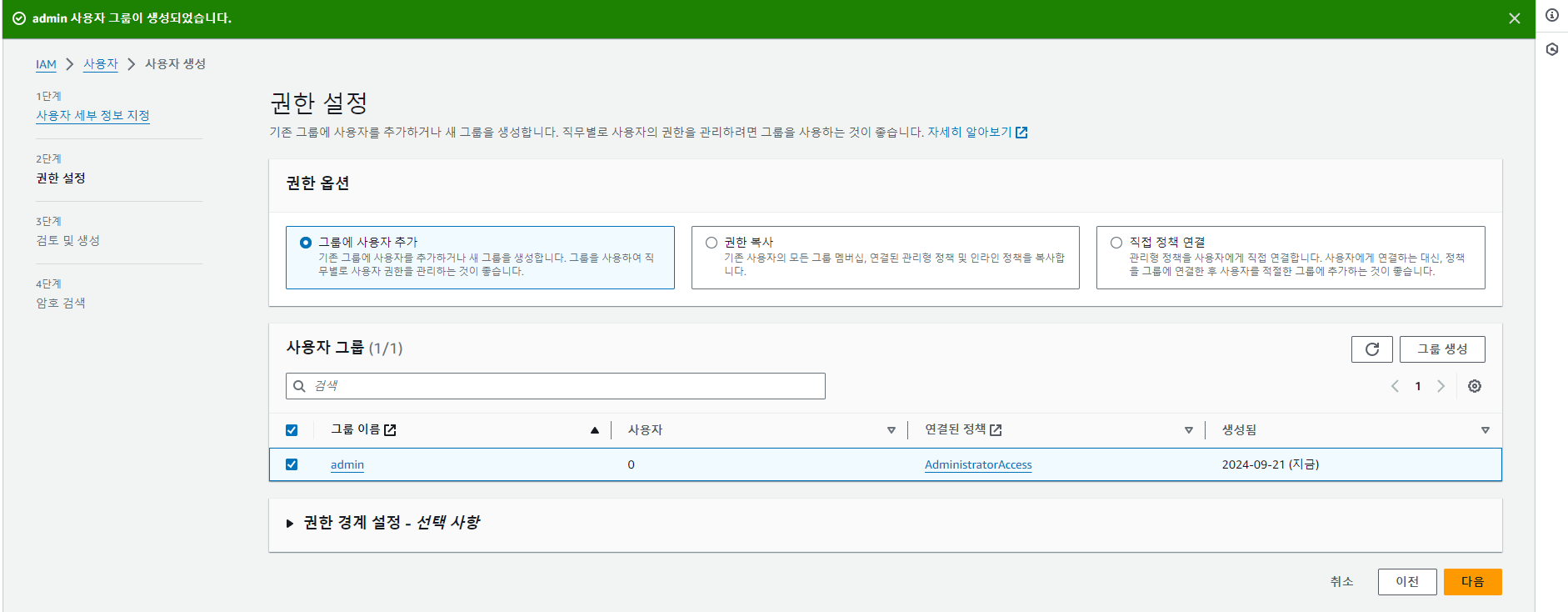
## IAM 사용자 계정과 그룹 생성 및 로그인

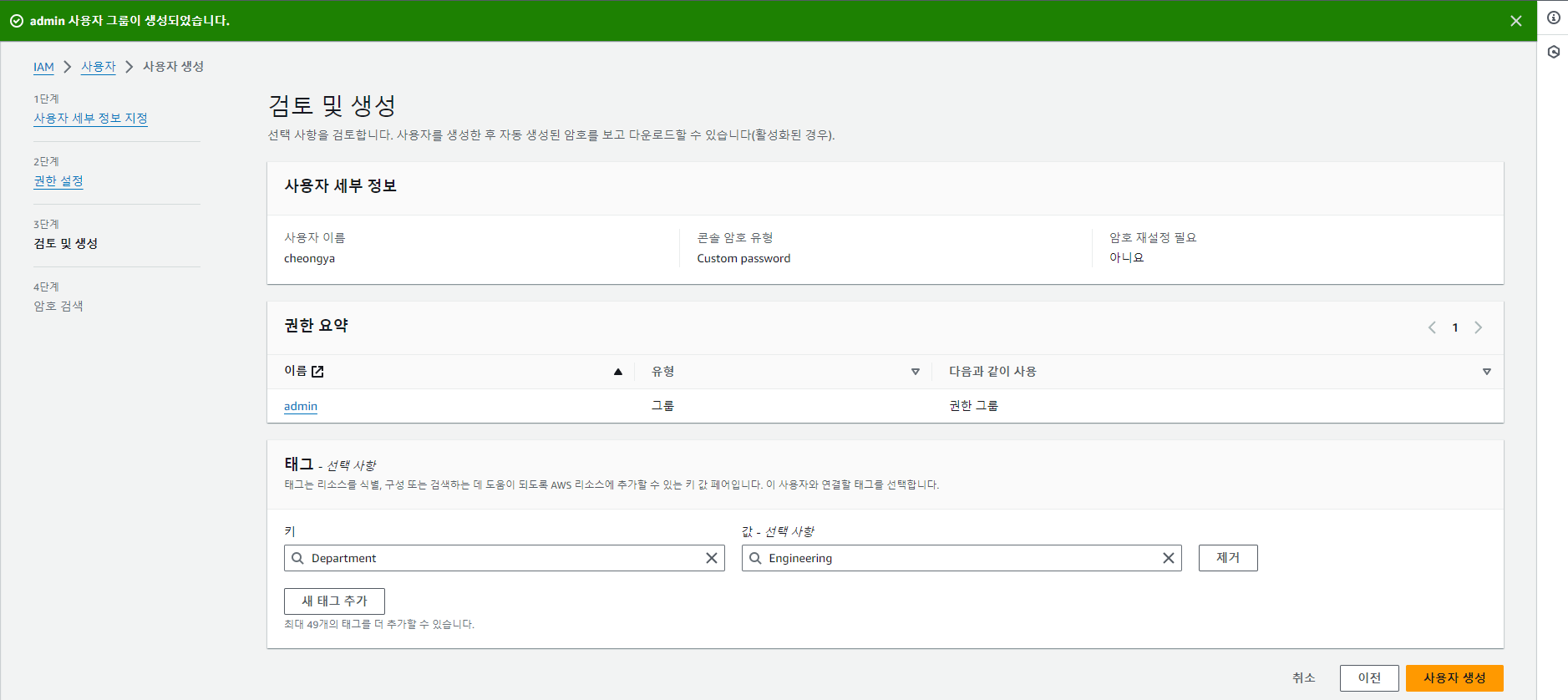
계정을 더 안전하게 사용하기 위하여 관리자 사용자가 아닌 일반 사용자를 생성하여 사용하기 위해 사용한다.



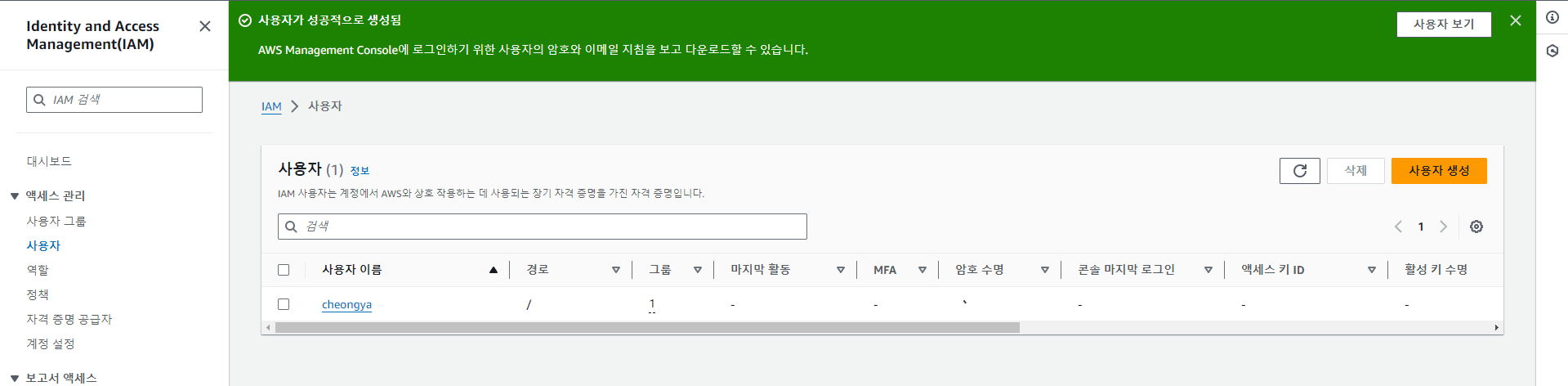


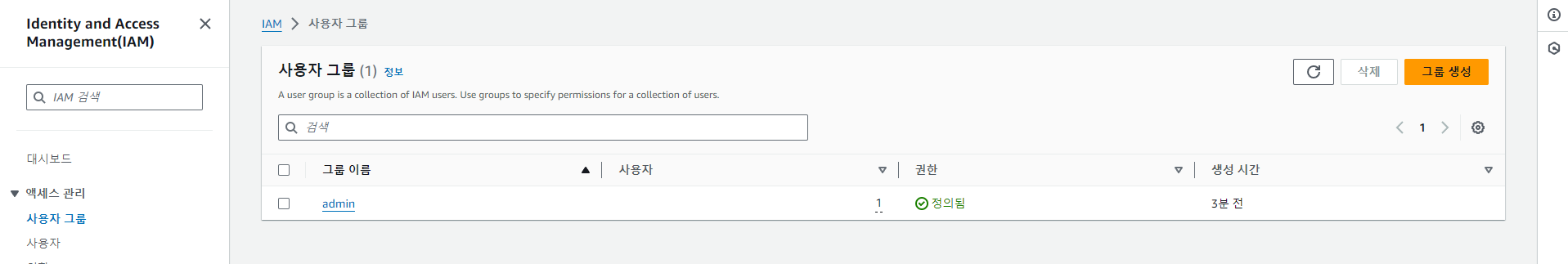


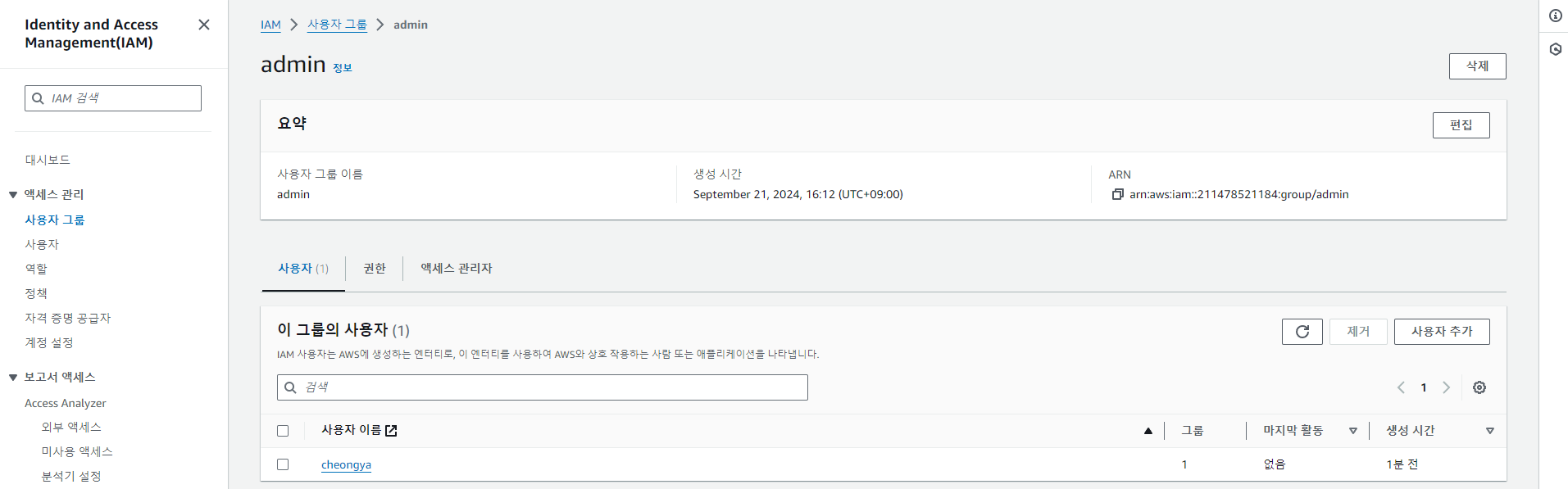


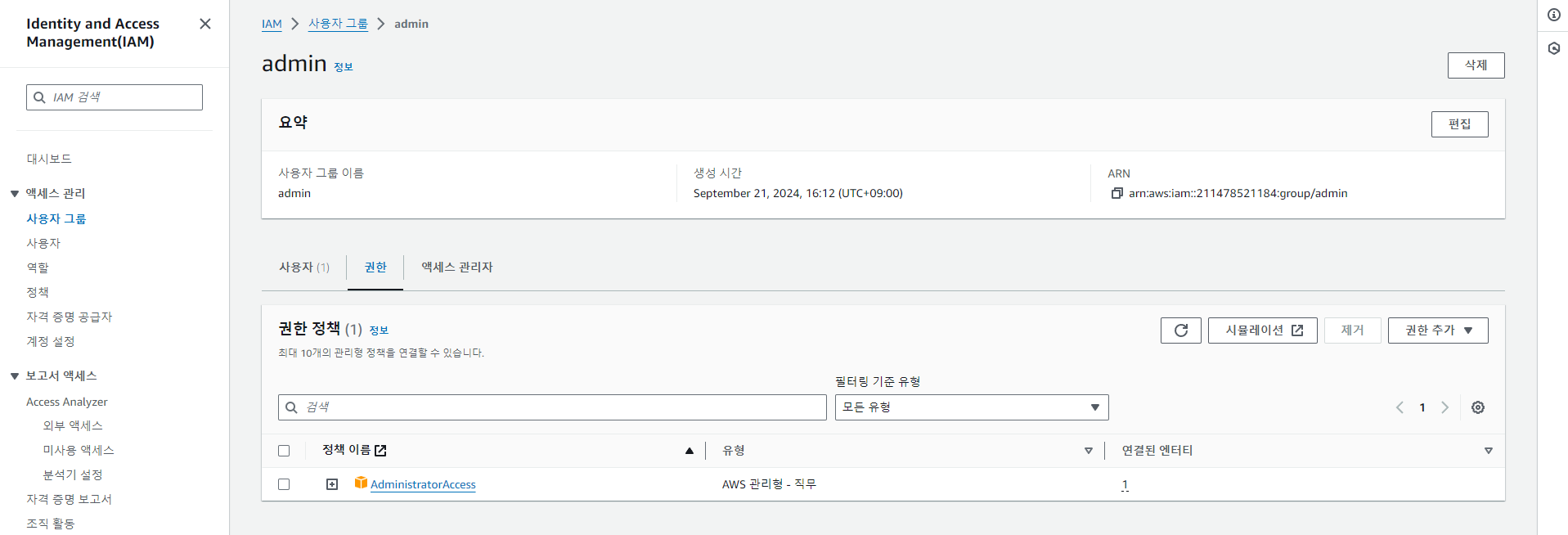


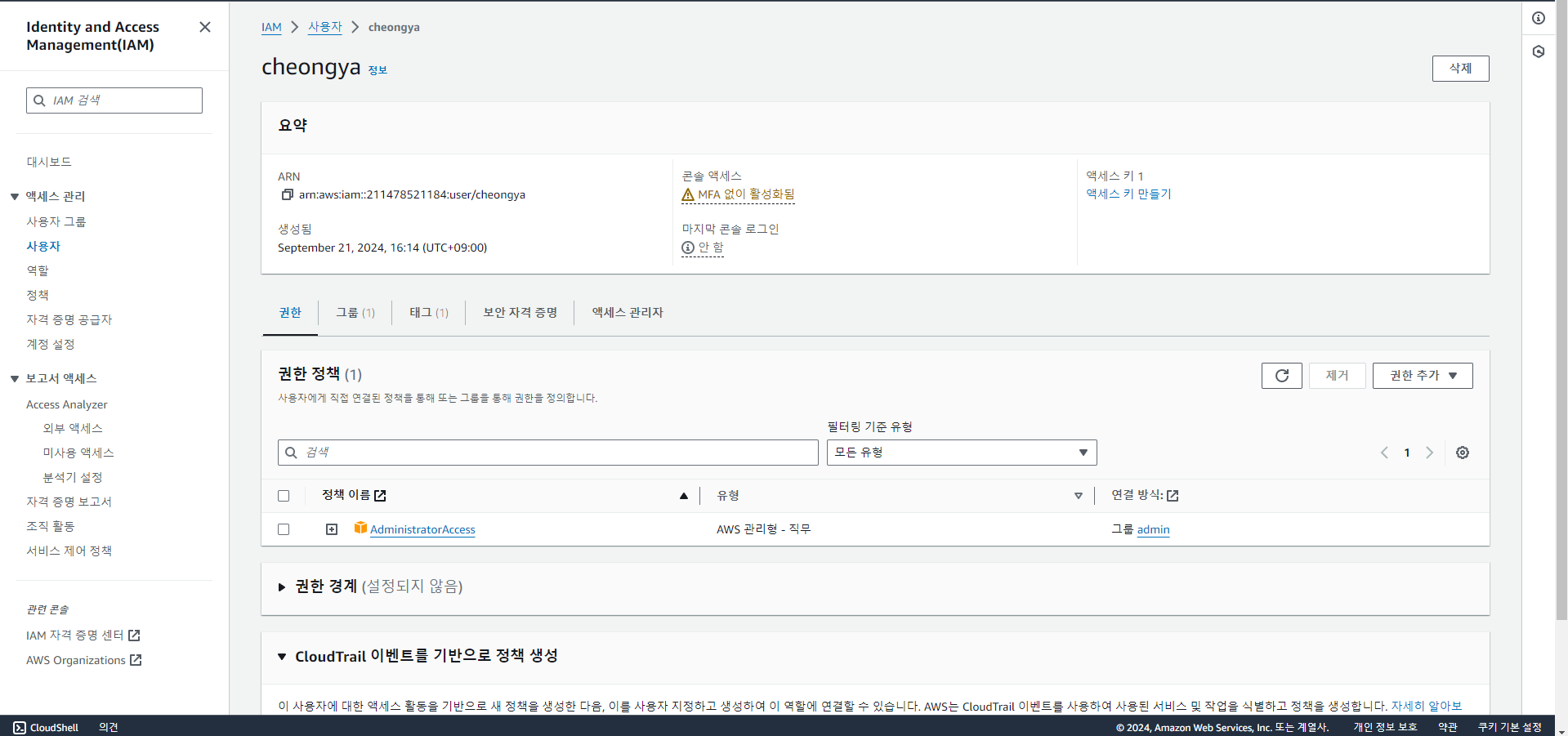




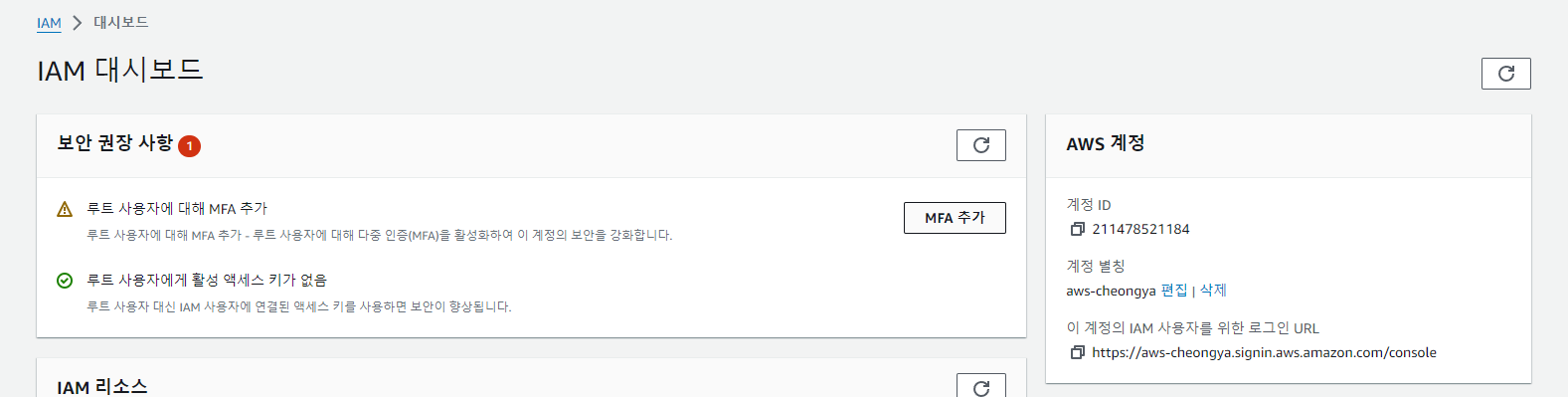


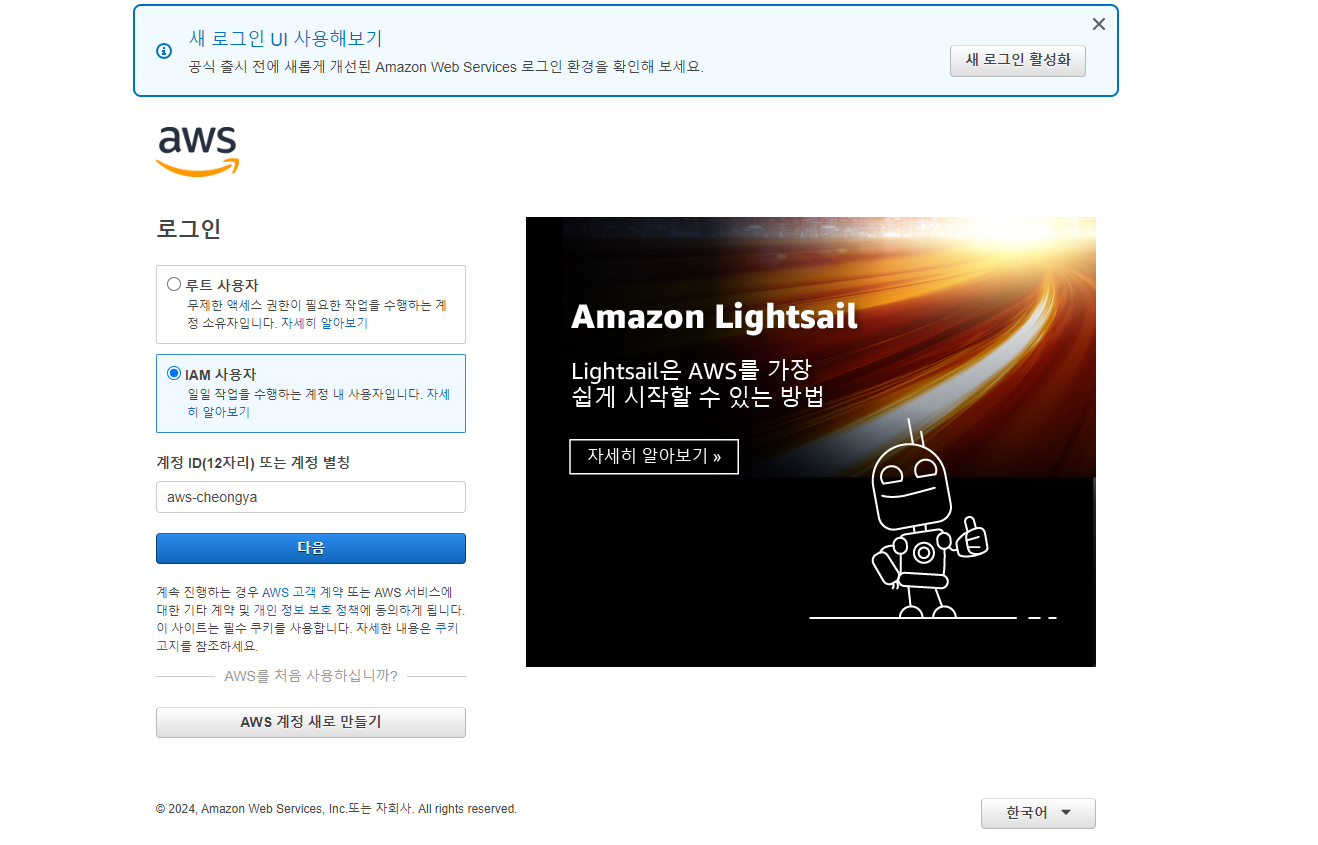


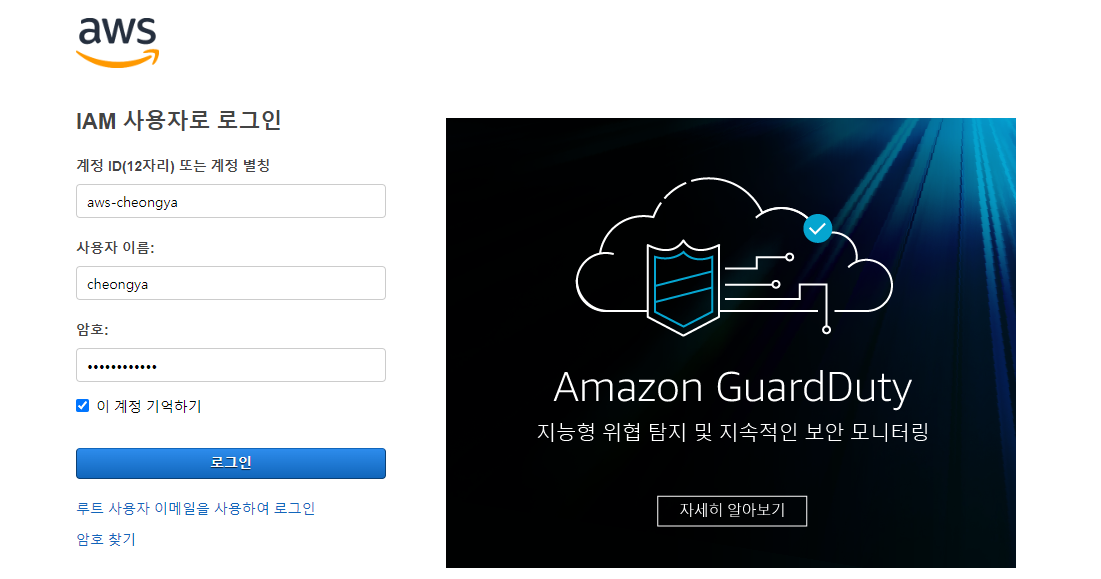


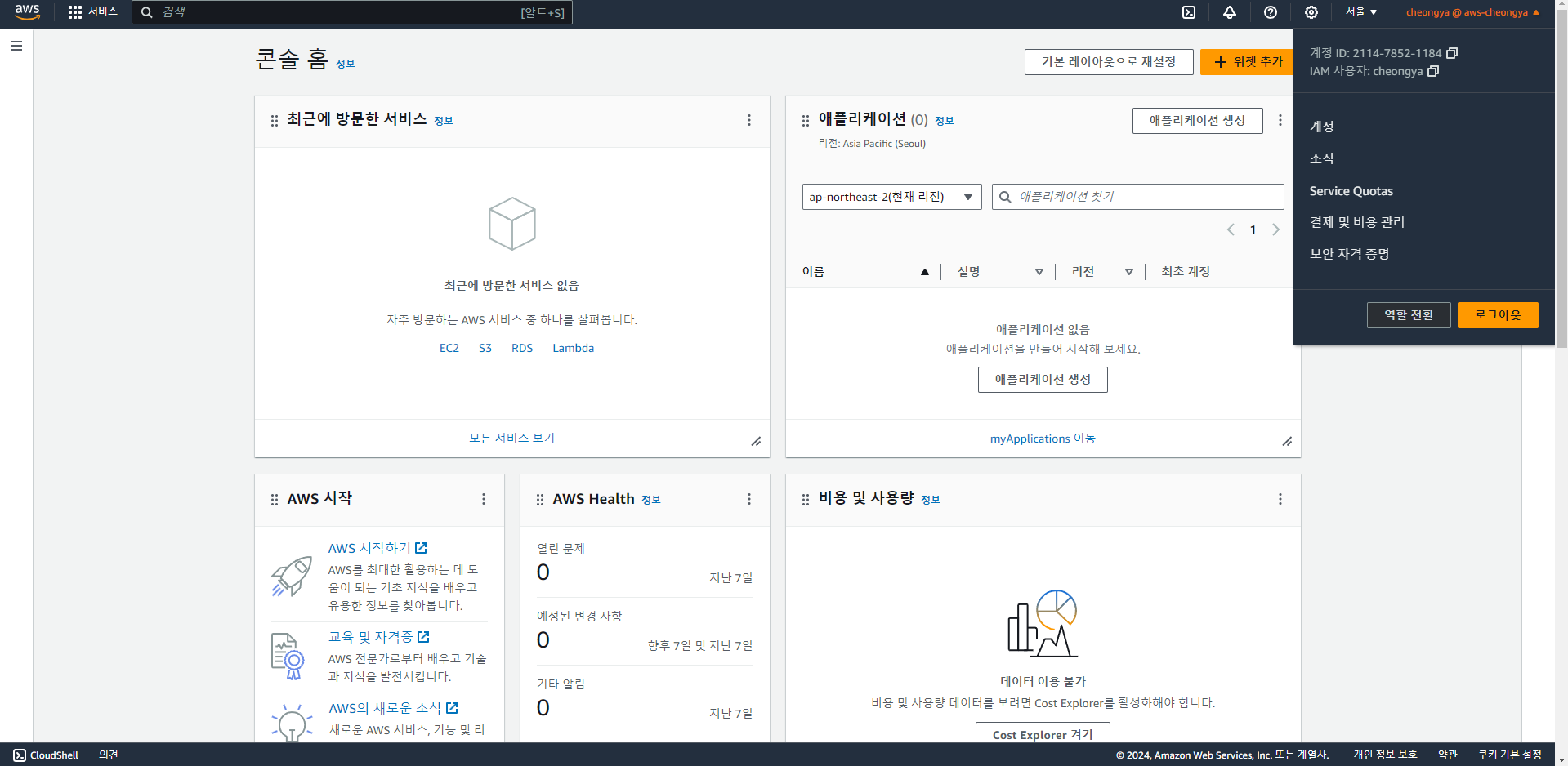


aws의 IAM 대시보드 – aws 계정의 계정 별칭을 사용하여 로그인 URL 변경 가능





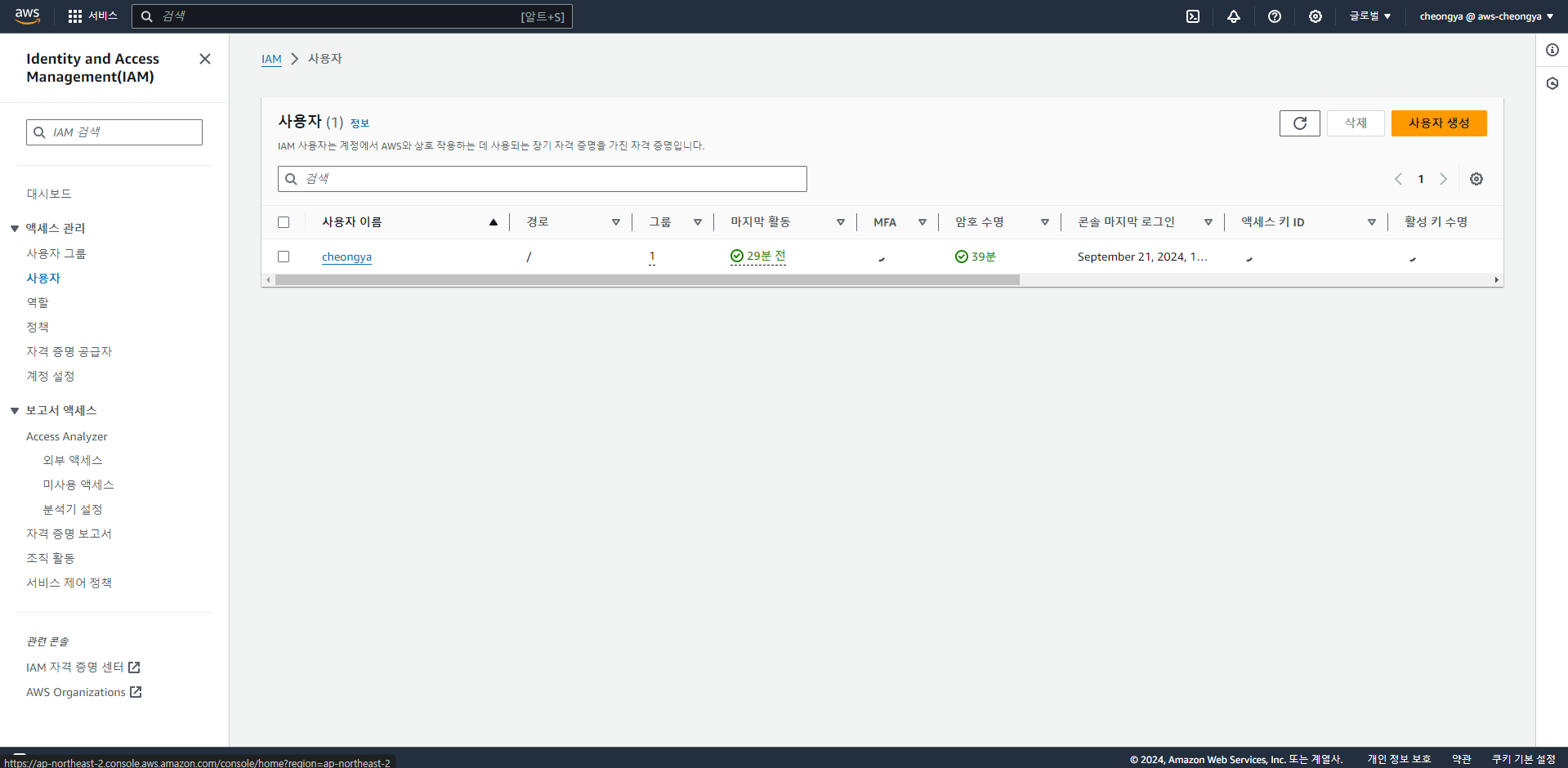




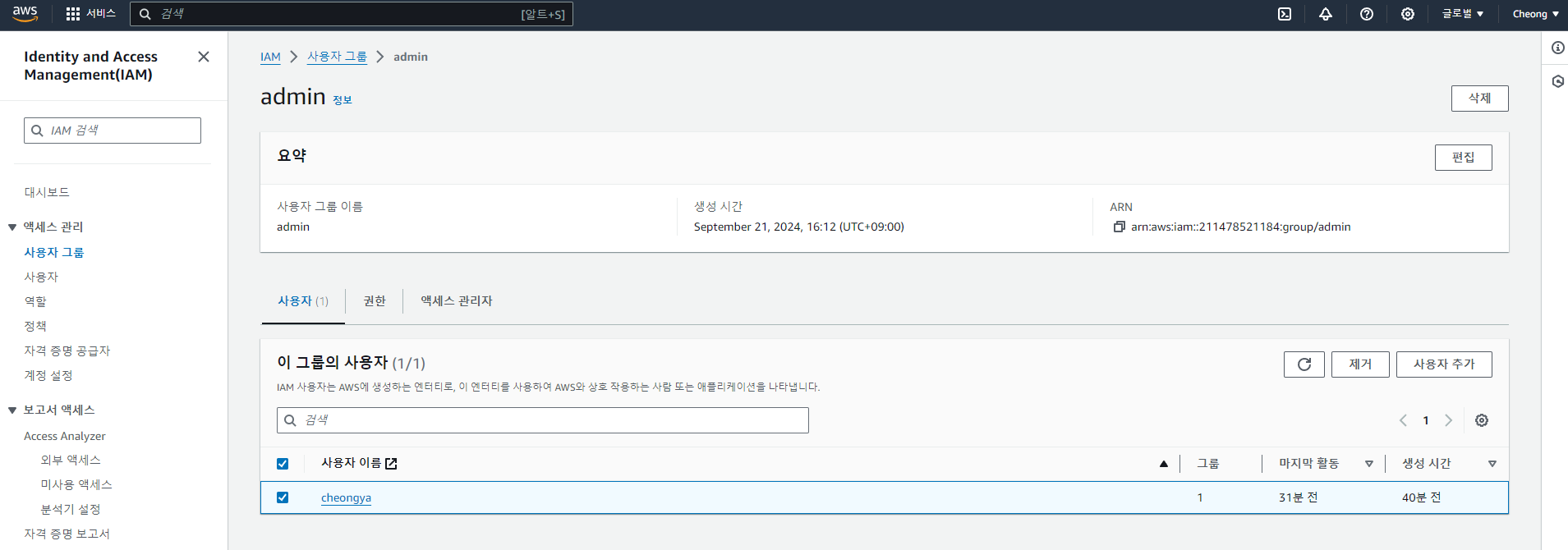
## 사용자 삭제 및 생성 / IAM 정책 실습

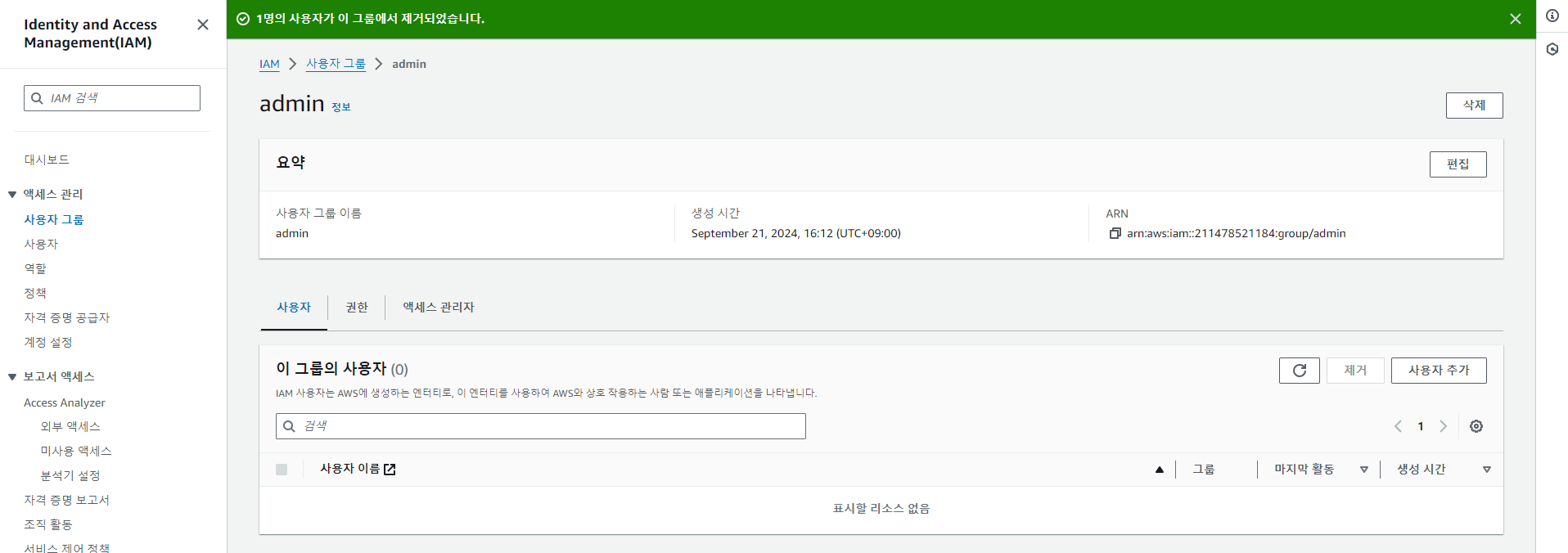
### 삭제

권한을 삭제하기 전에는 접속이 원활하게 되는 모습을 확인할 수 있다.

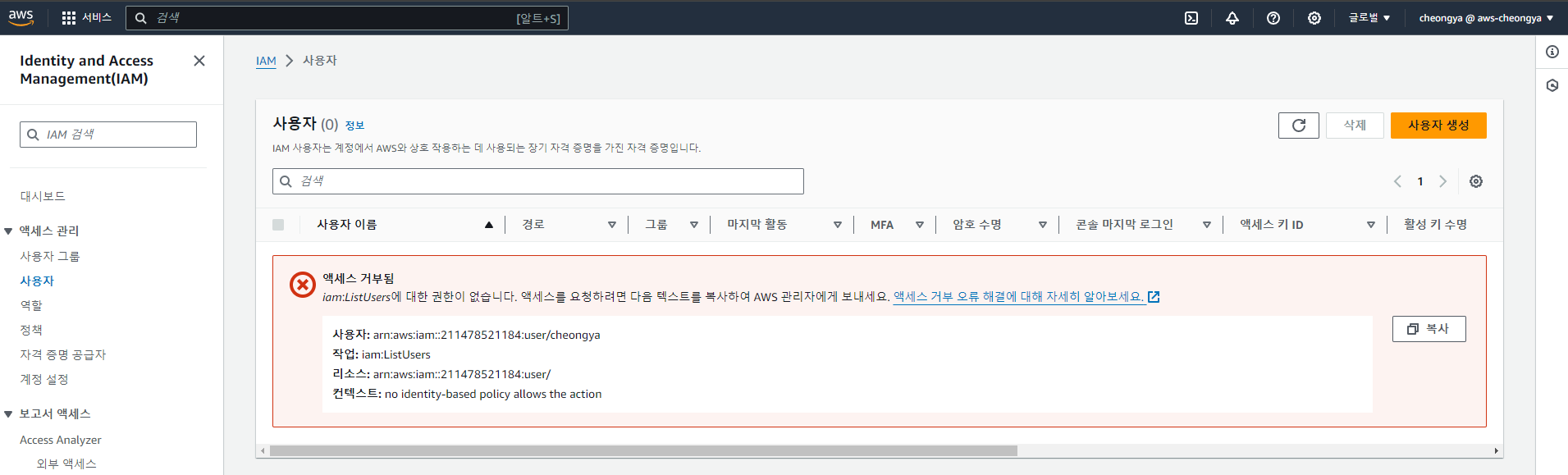


사용자 그룹 -> admin에서 사용자 삭제



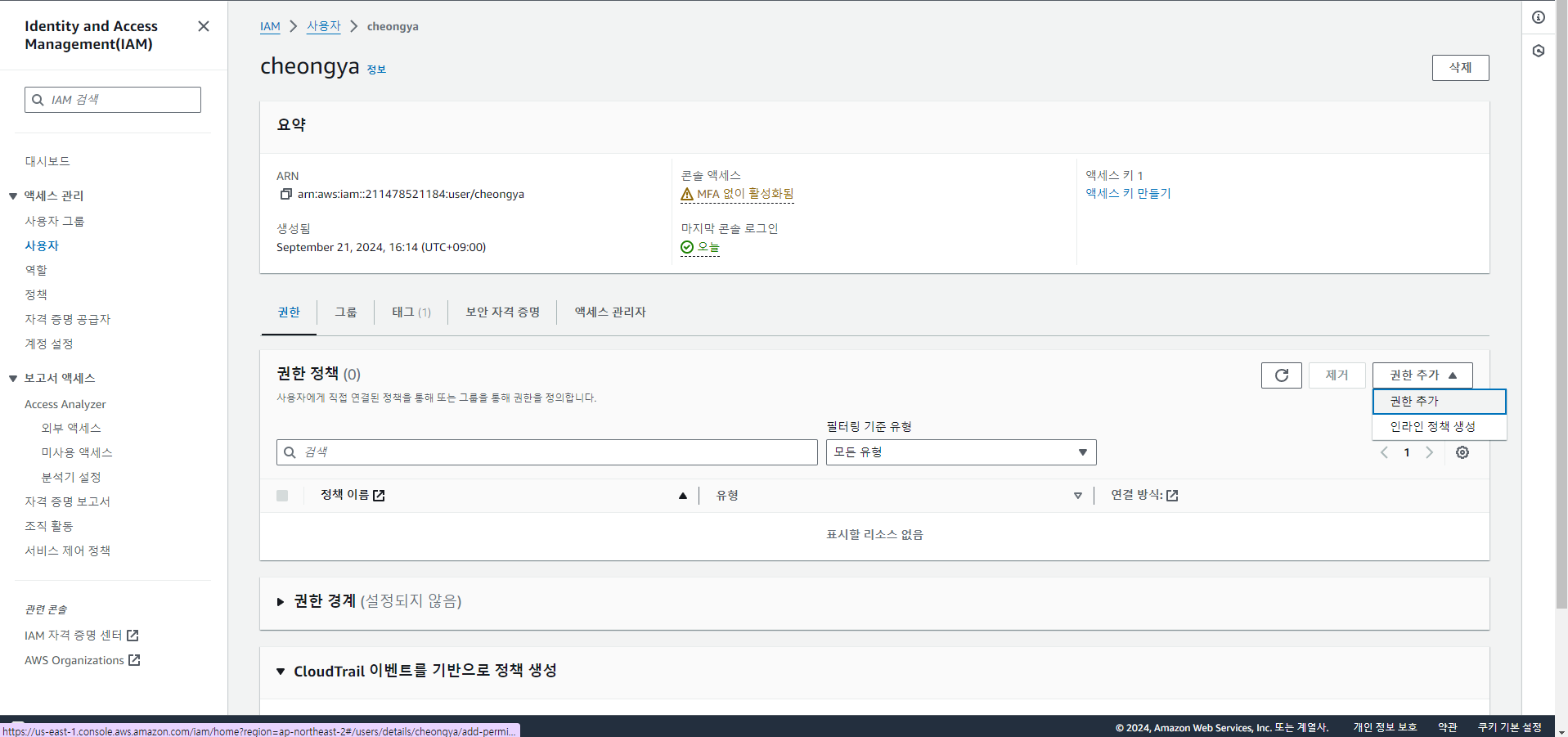


액세스가 거부되는 것을 확인할 수 있다.

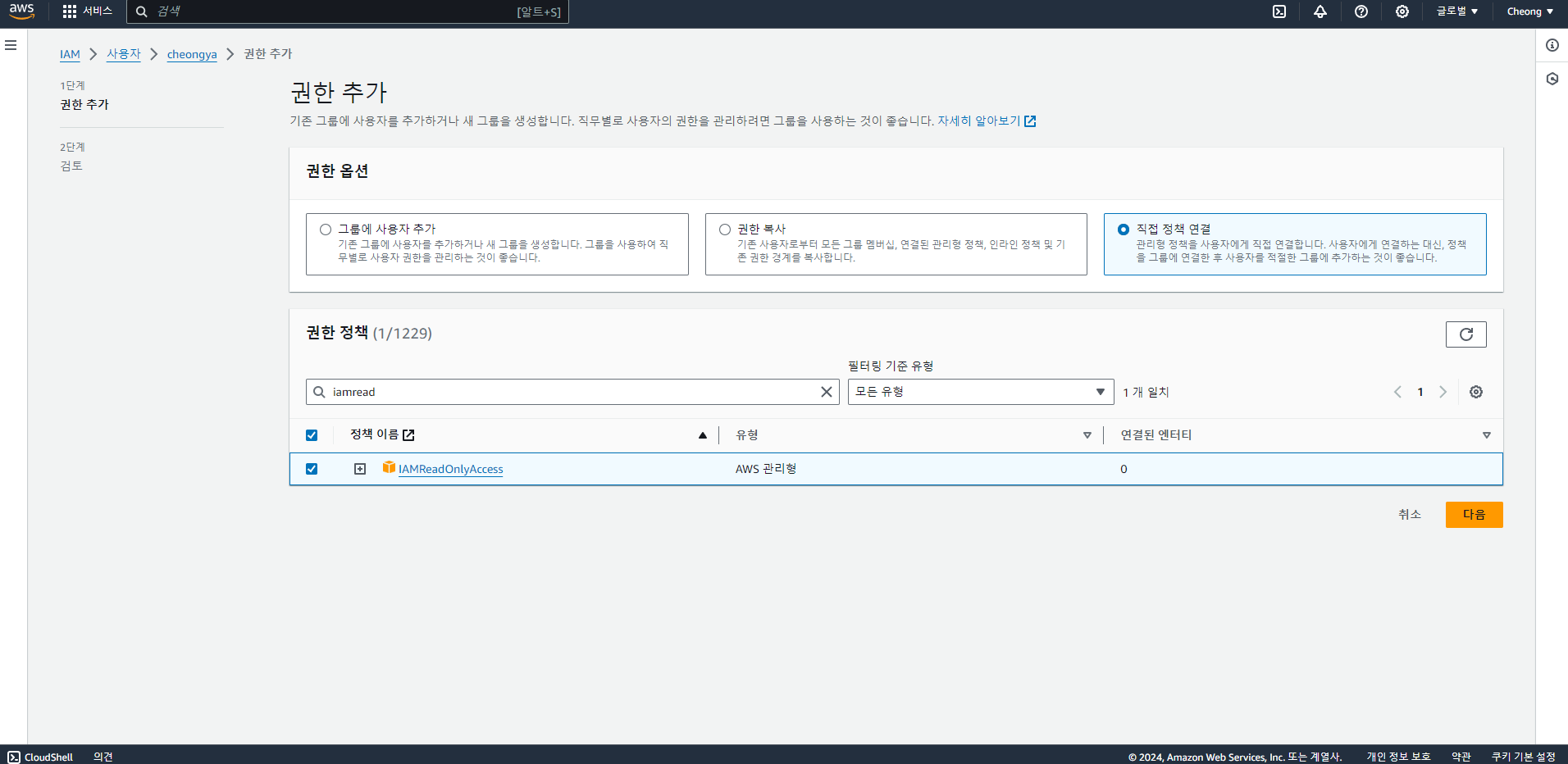


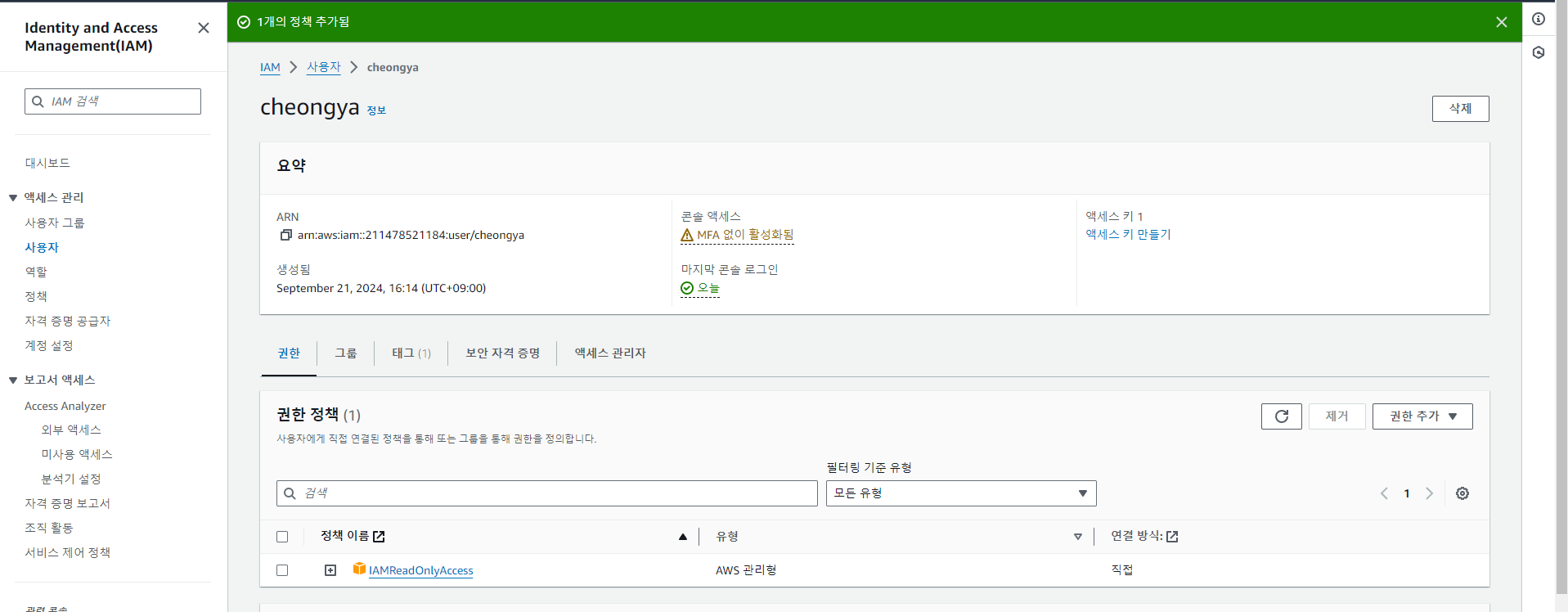
### 생성

사용자 -> 그룹에 포함 시킬 유저 명 -> 권한 추가

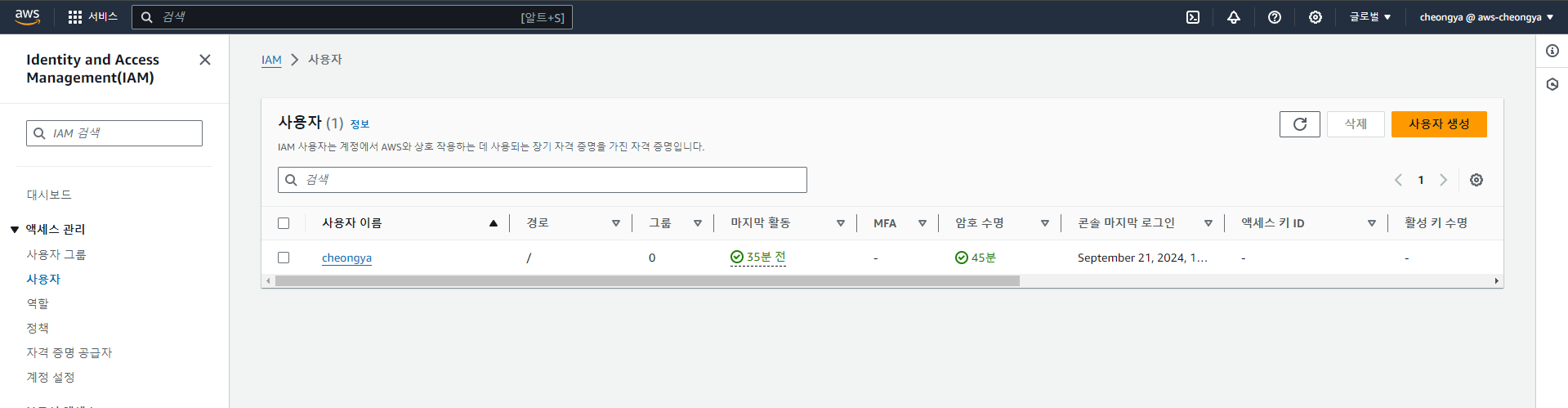


IAMReadOnlyAccess 권한만 직접 선택하여 부여

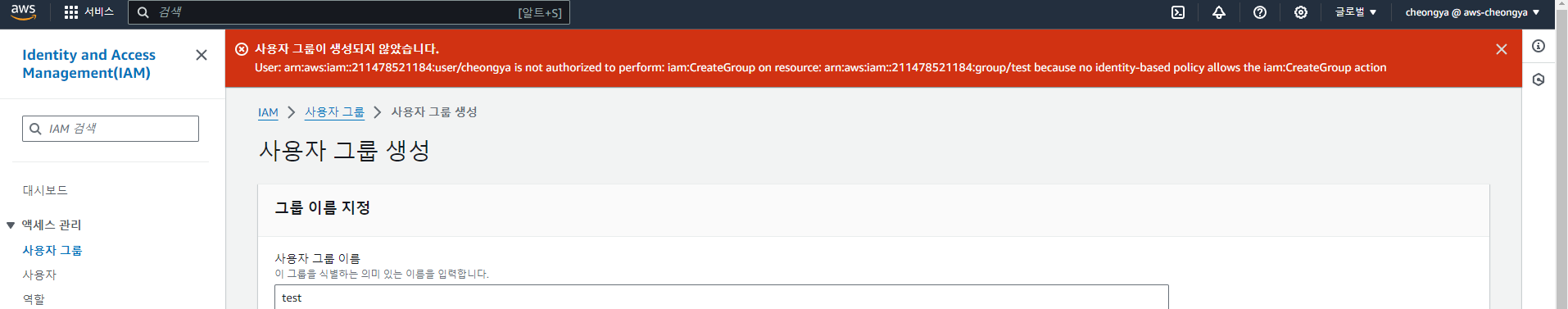




액세스가 허용된 것을 확인할 수 있다.



하지만 ReadOnly 권한만 부여했기 때문에 생성할 수 없다.

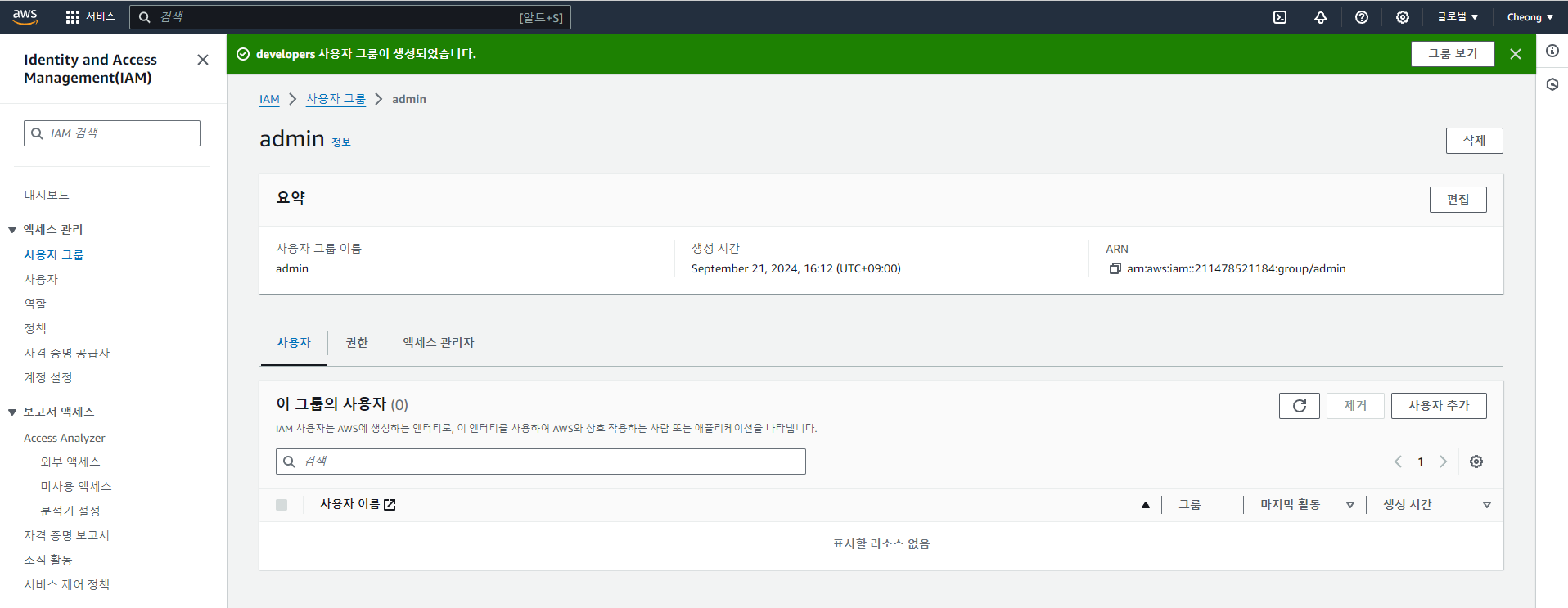


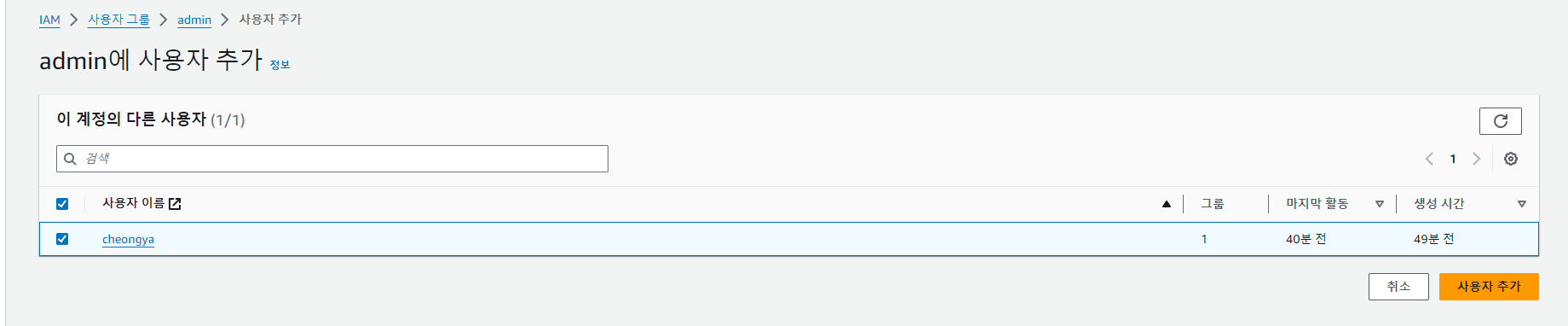
### IAM 정책

사용자 그룹 -> 그룹 생성 -> 권한 정책은 아무거나 고른 후 생성



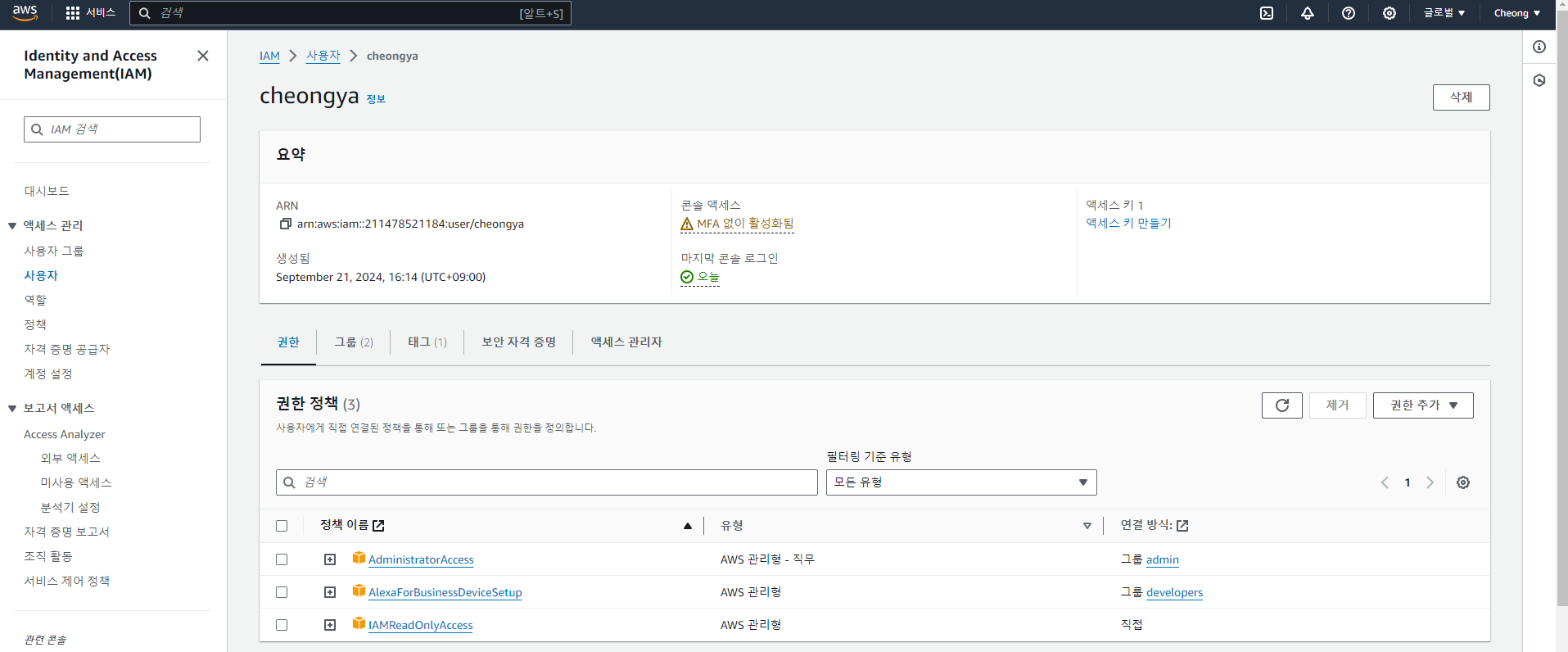
사용자 그룹 -> 기존 생성해둔 admin에서 사용자 다시 추가



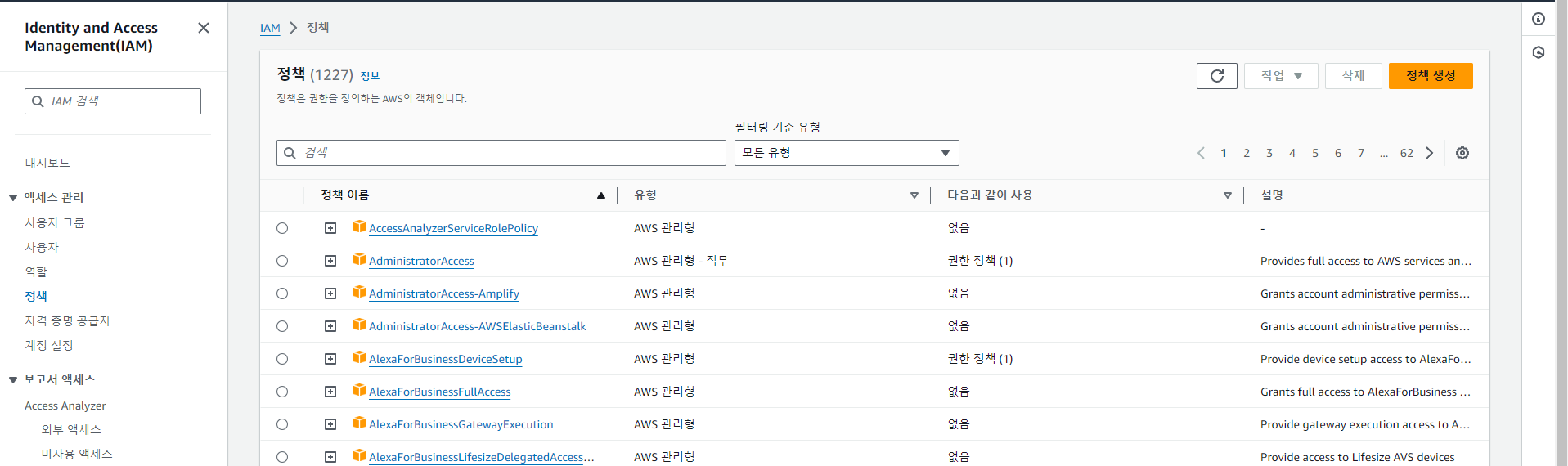


이후 사용자 -> 사용자 명을 클릭하여 정보를 보면 권한이 추가되어 있는 것을 확인할 수 있다.

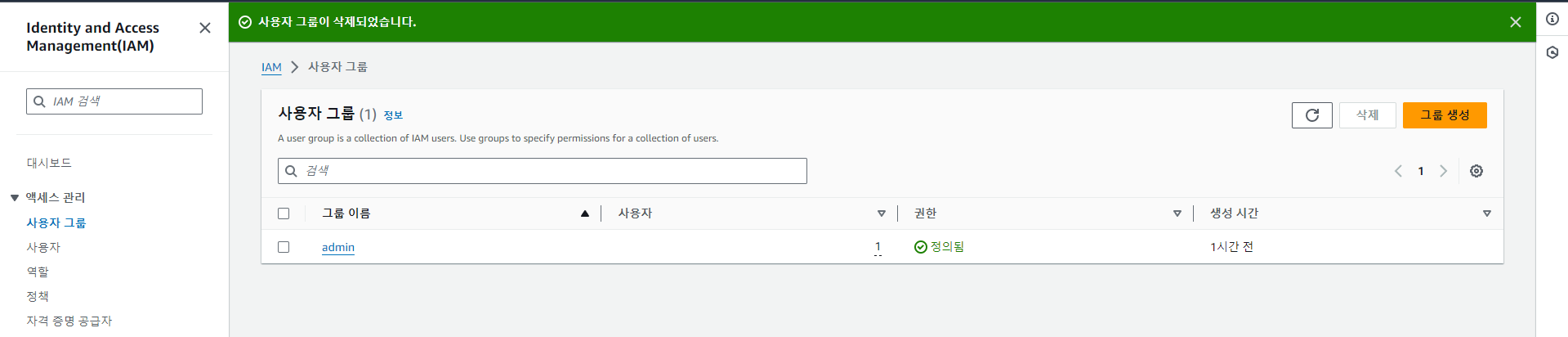
각각 admin, developers, 그리고 직접 권한을 받게 된 것을 확인할 수 있다.

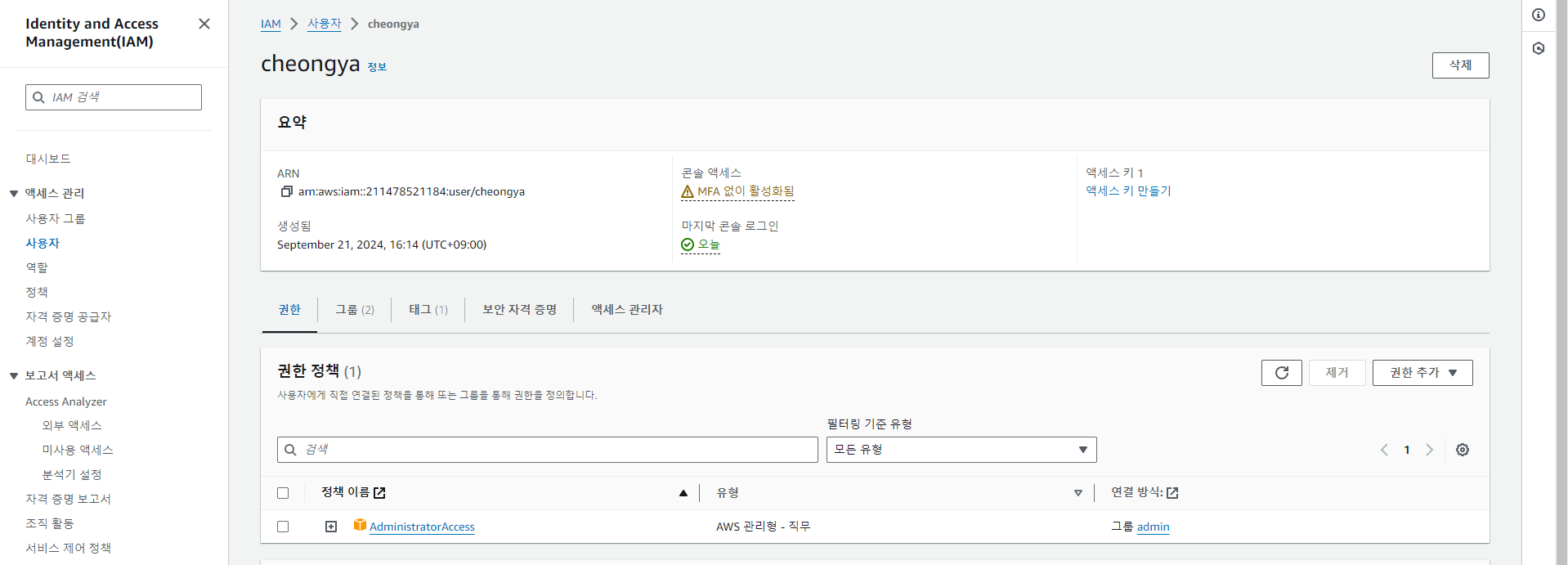


또한 정책을 스스로 생성할 수도 있다.



필요 없어진 developers와 직접 넣어줬던 ReadOnly 정책을 삭제한다.

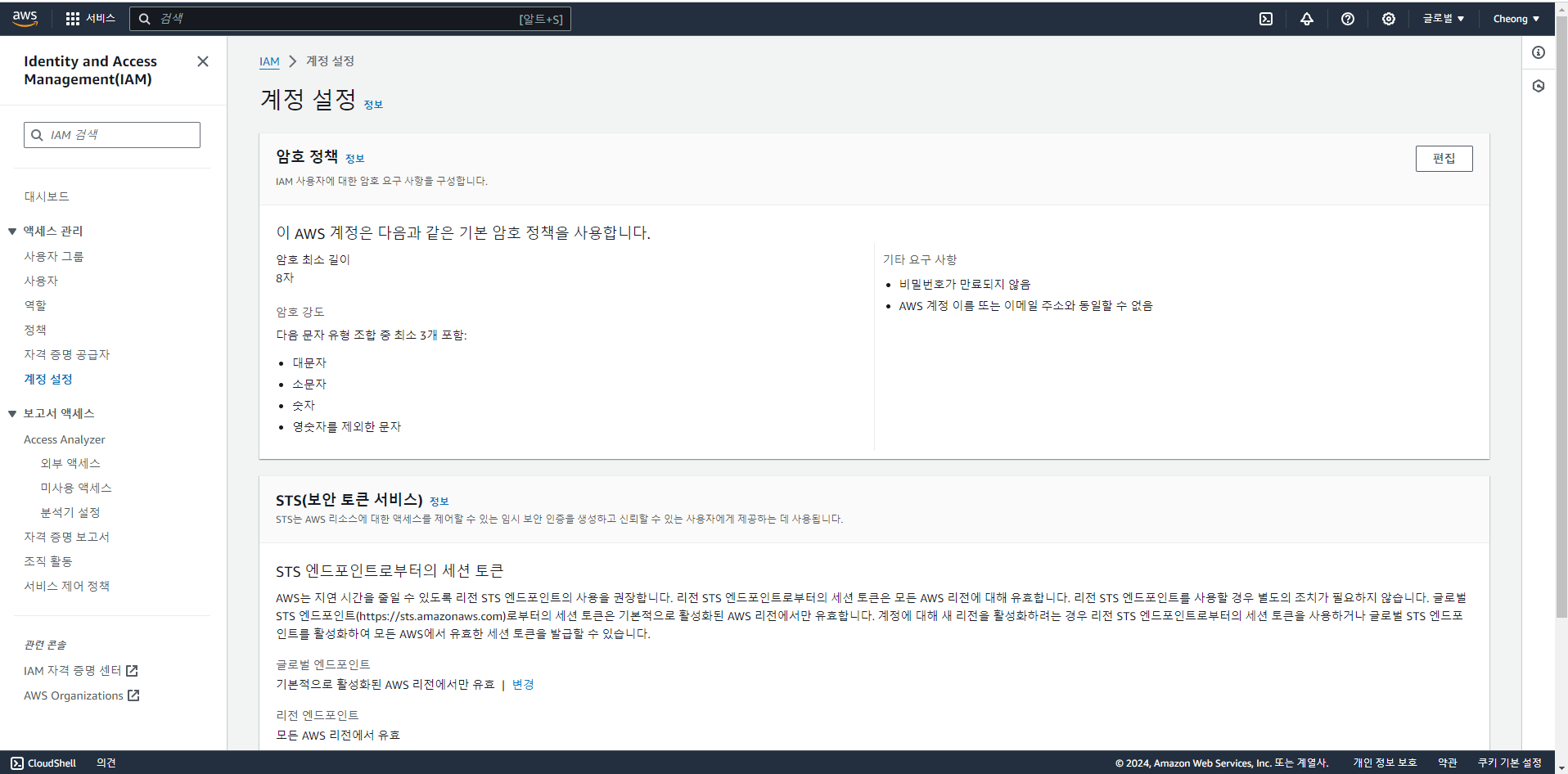


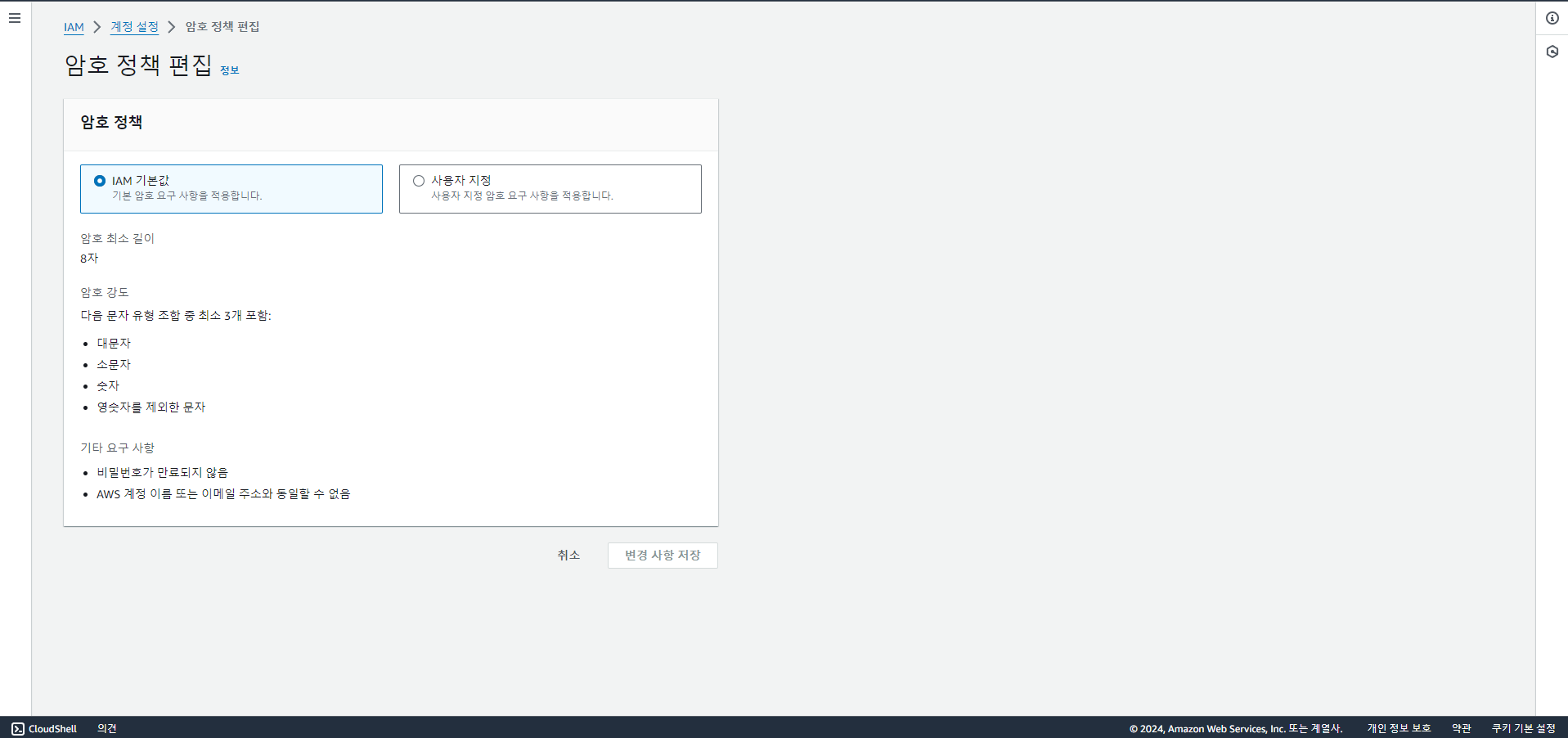


## IAM MFA 실습

### 기본 암호 정책 설정

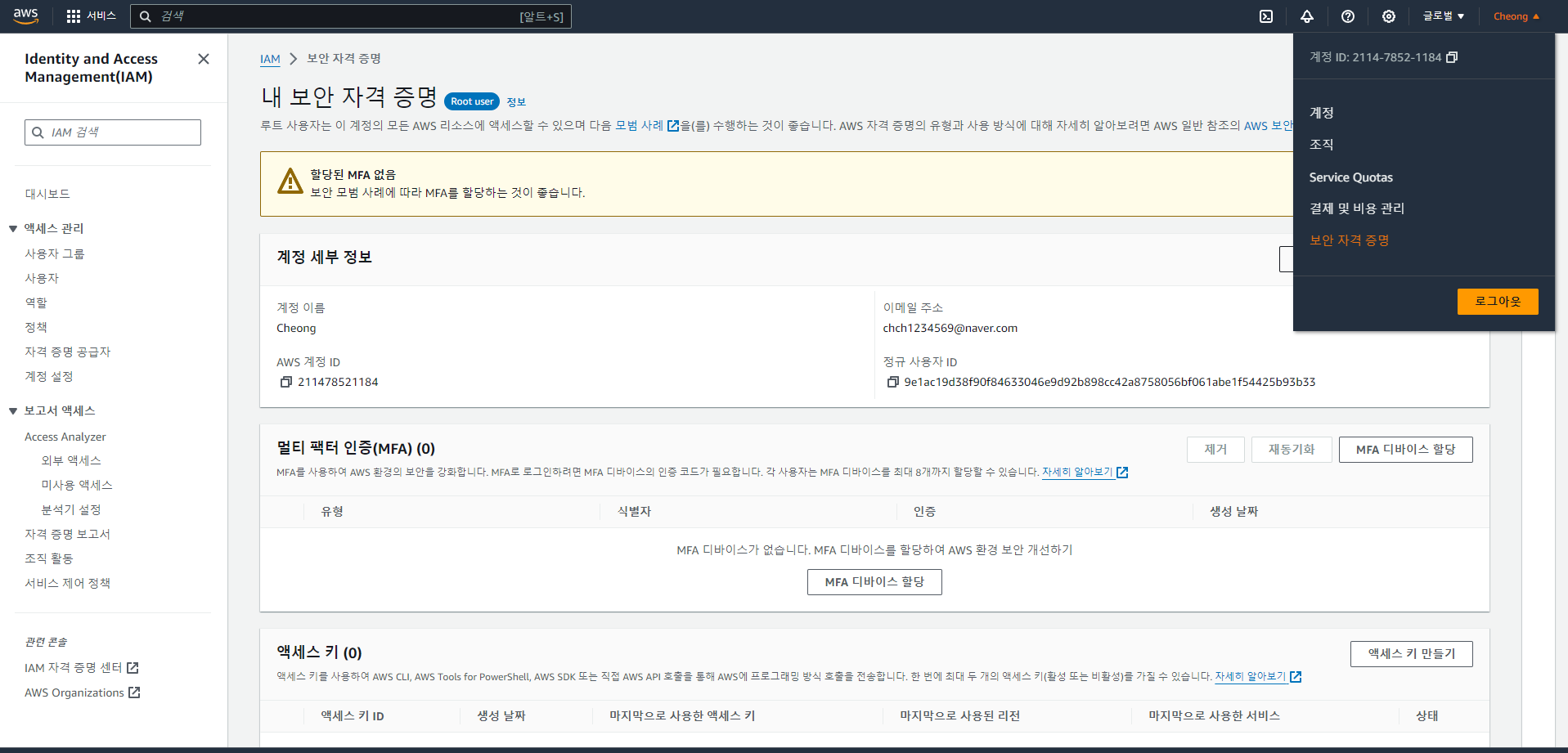
계정 설정 -> 암호 정책 -> 편집 클릭



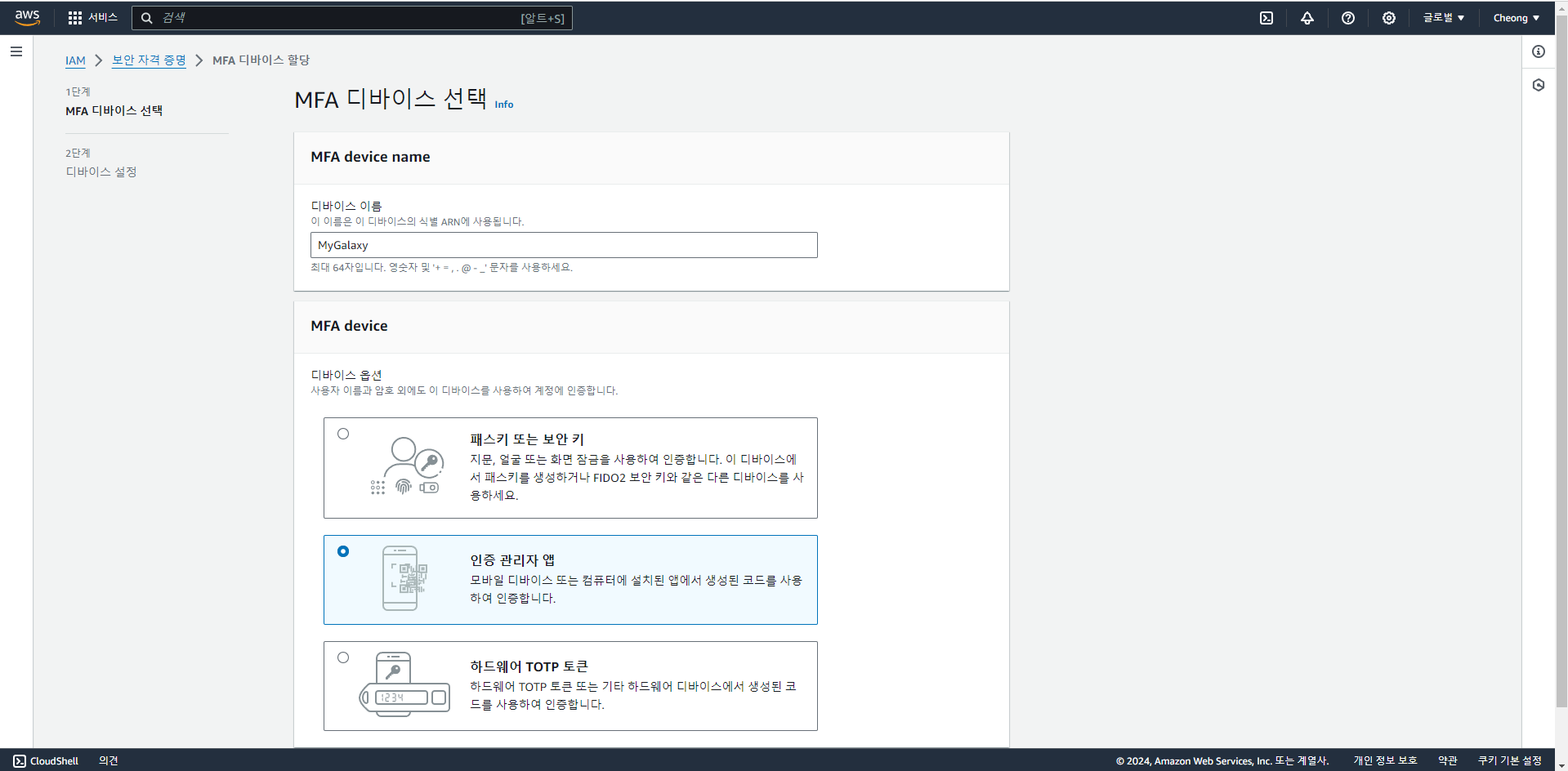


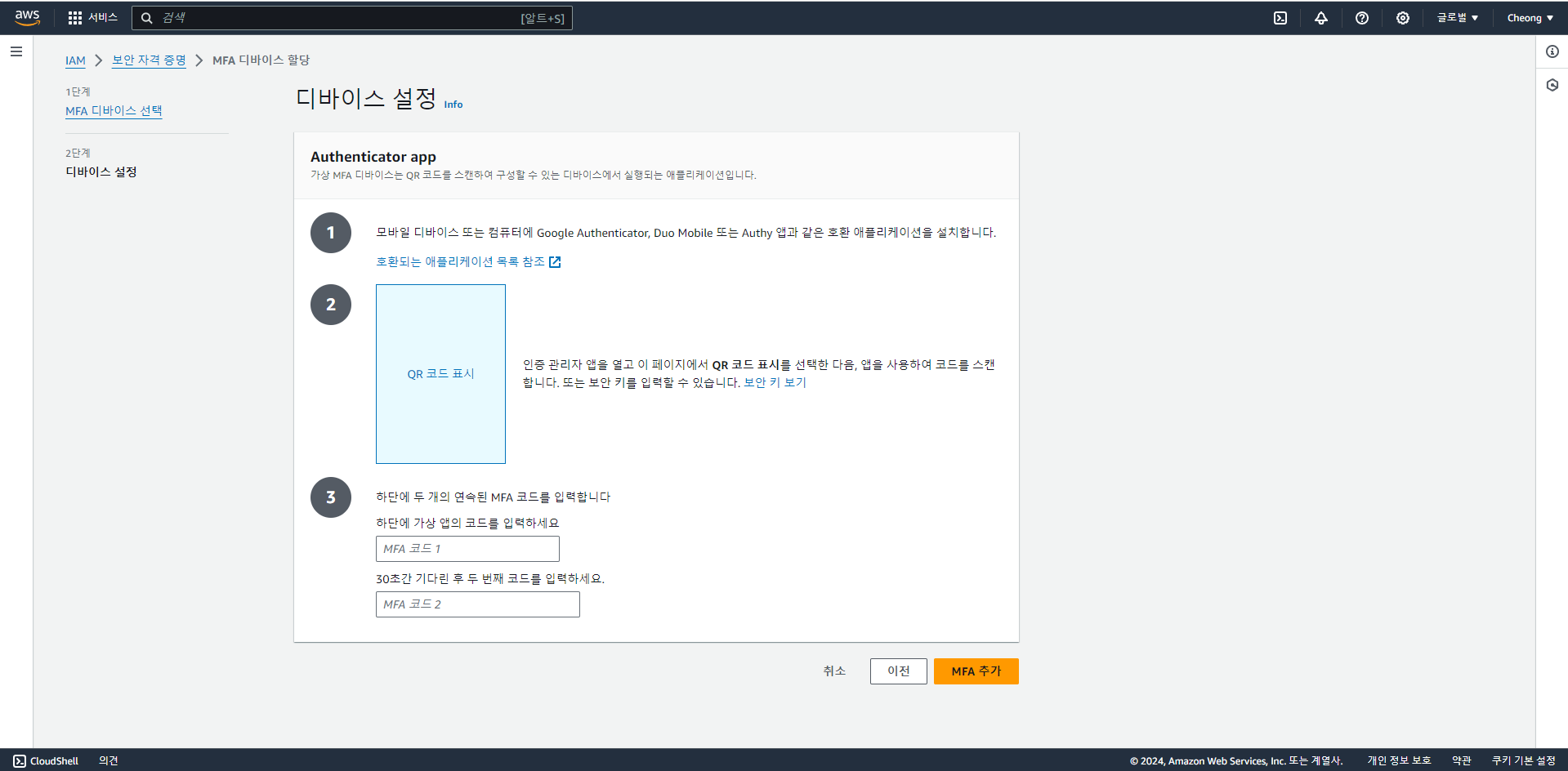
### 루트 계정에 대한 다단계 인증 설정

보안 자격 증명을 눌러 접속 후 MFA 할당 시작

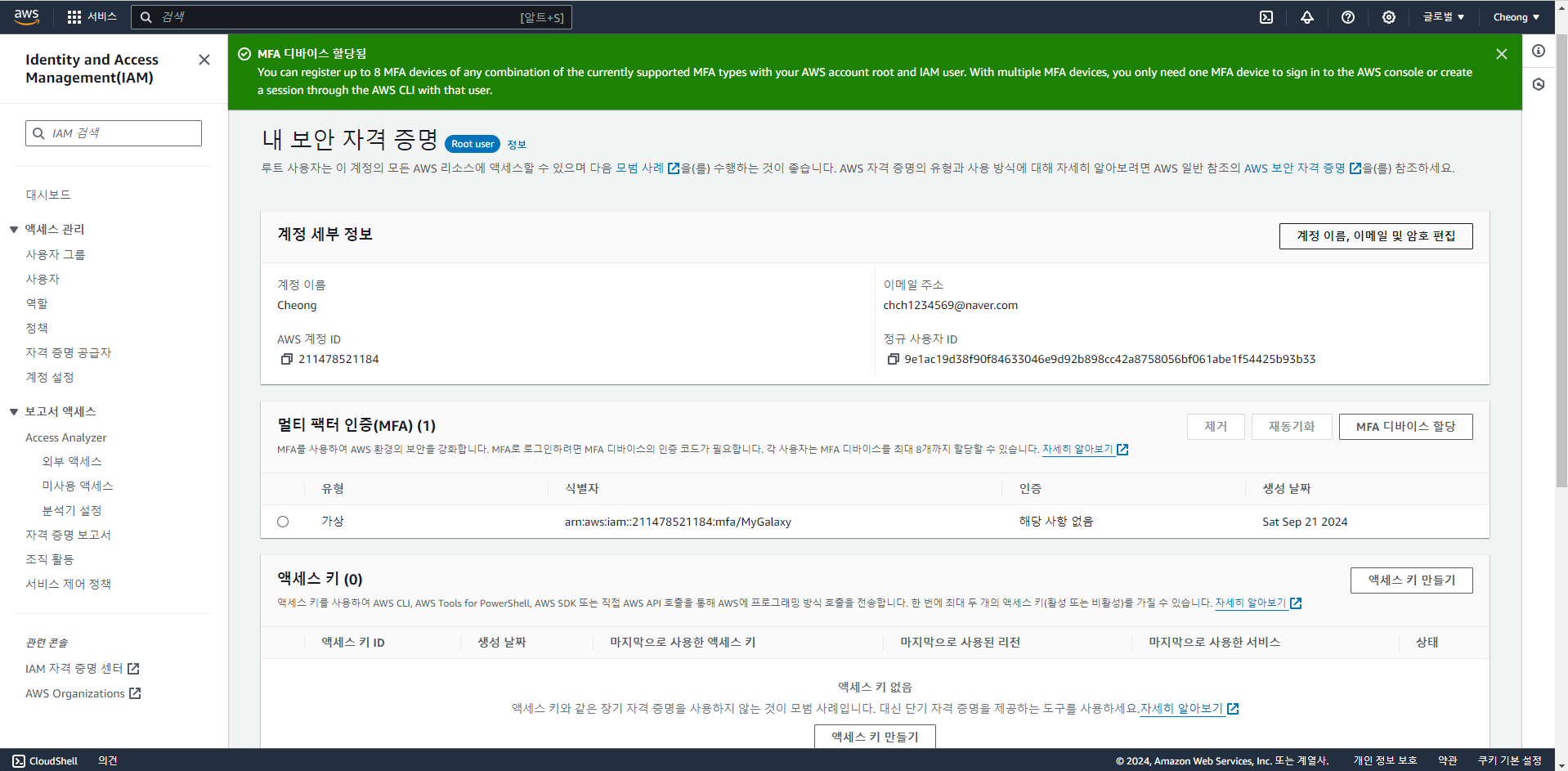


디바이스 이름을 간단하게 설정 후 사용자가 원하는 디바이스 옵션 선택



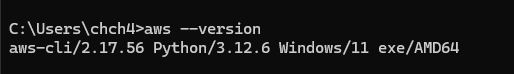


인증을 완료한 후 멀티 팩터 인증(MFA)에 생성이 된 것을 확인할 수 있다.



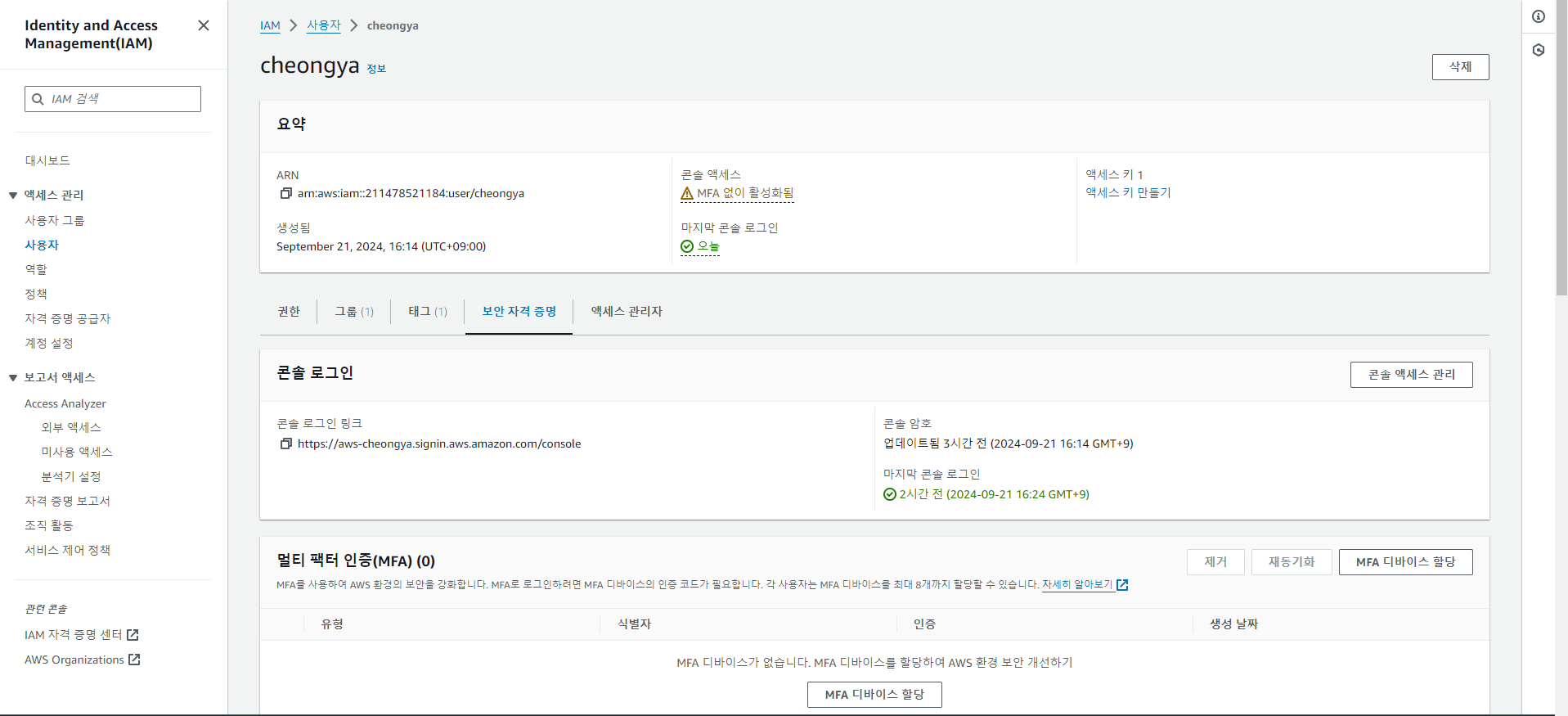
## AWS CLI

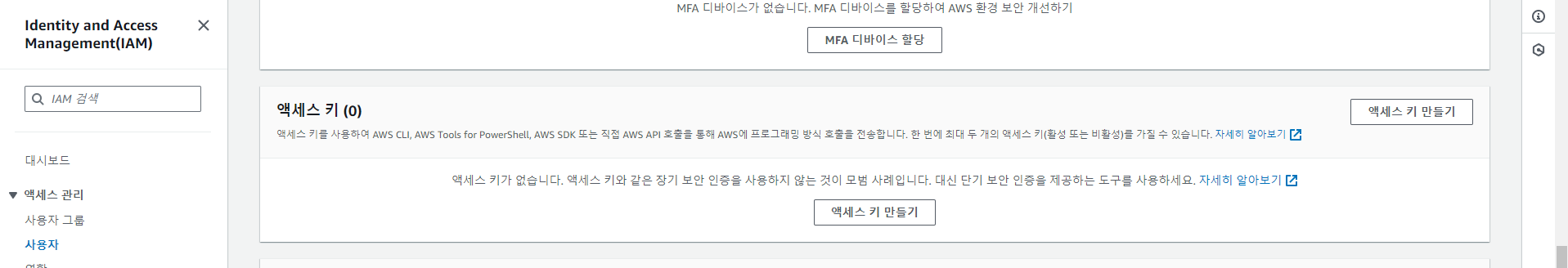
<https://docs.aws.amazon.com/ko_kr/cli/latest/userguide/getting-started-install.html> 에서 설치



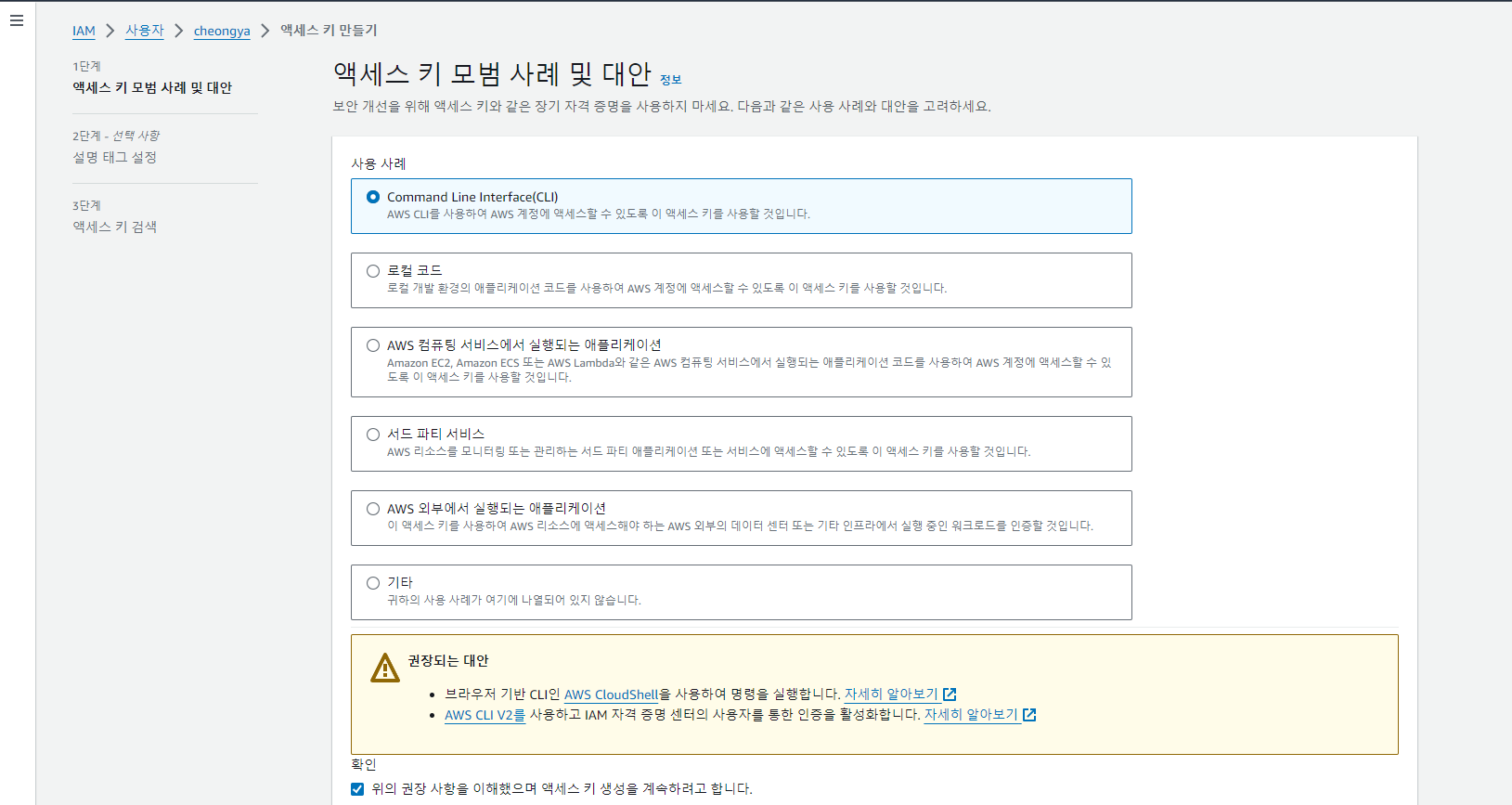
### 액세스 키 생성

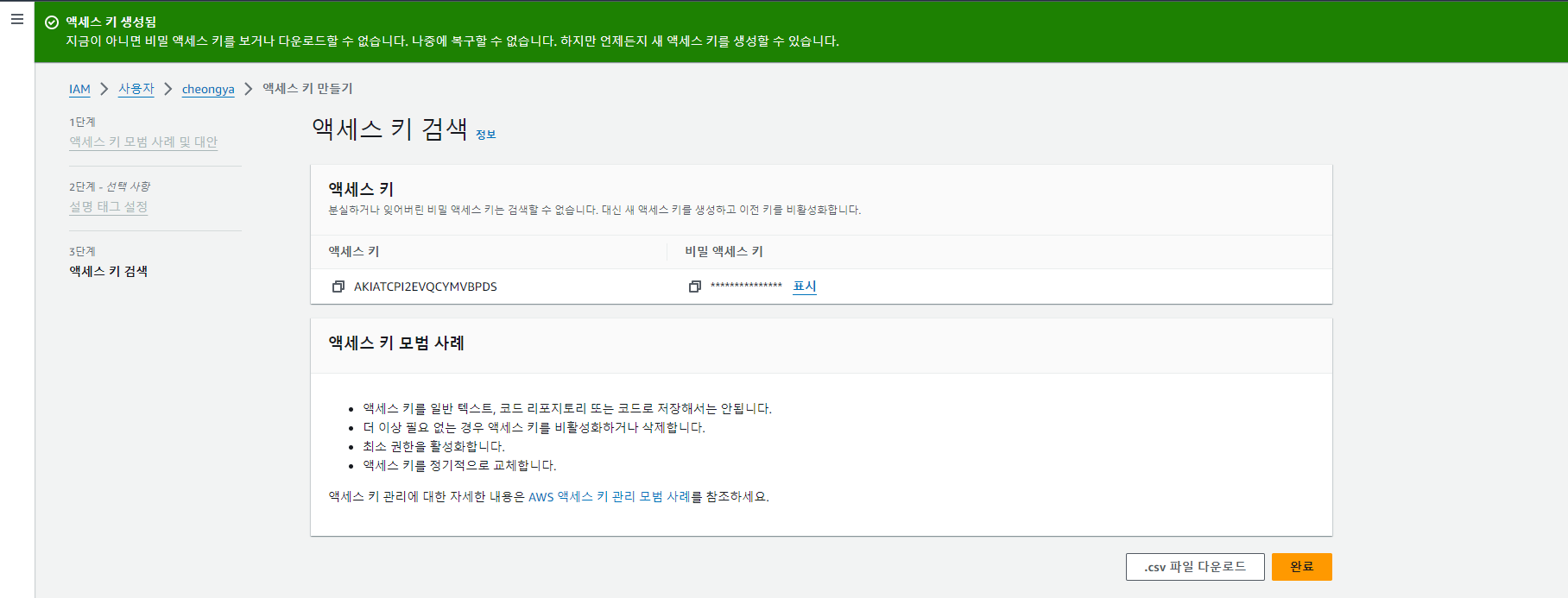
사용자 -> 사용자 명 클릭 -> 보안 자격 증명 -> 액세스 키



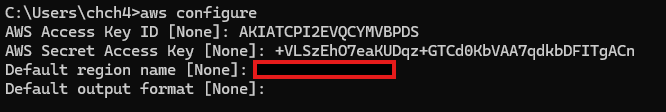


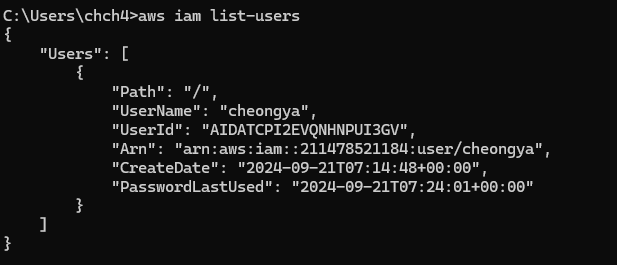
액세스 키 만들기 클릭





### CLI + 액세스 키





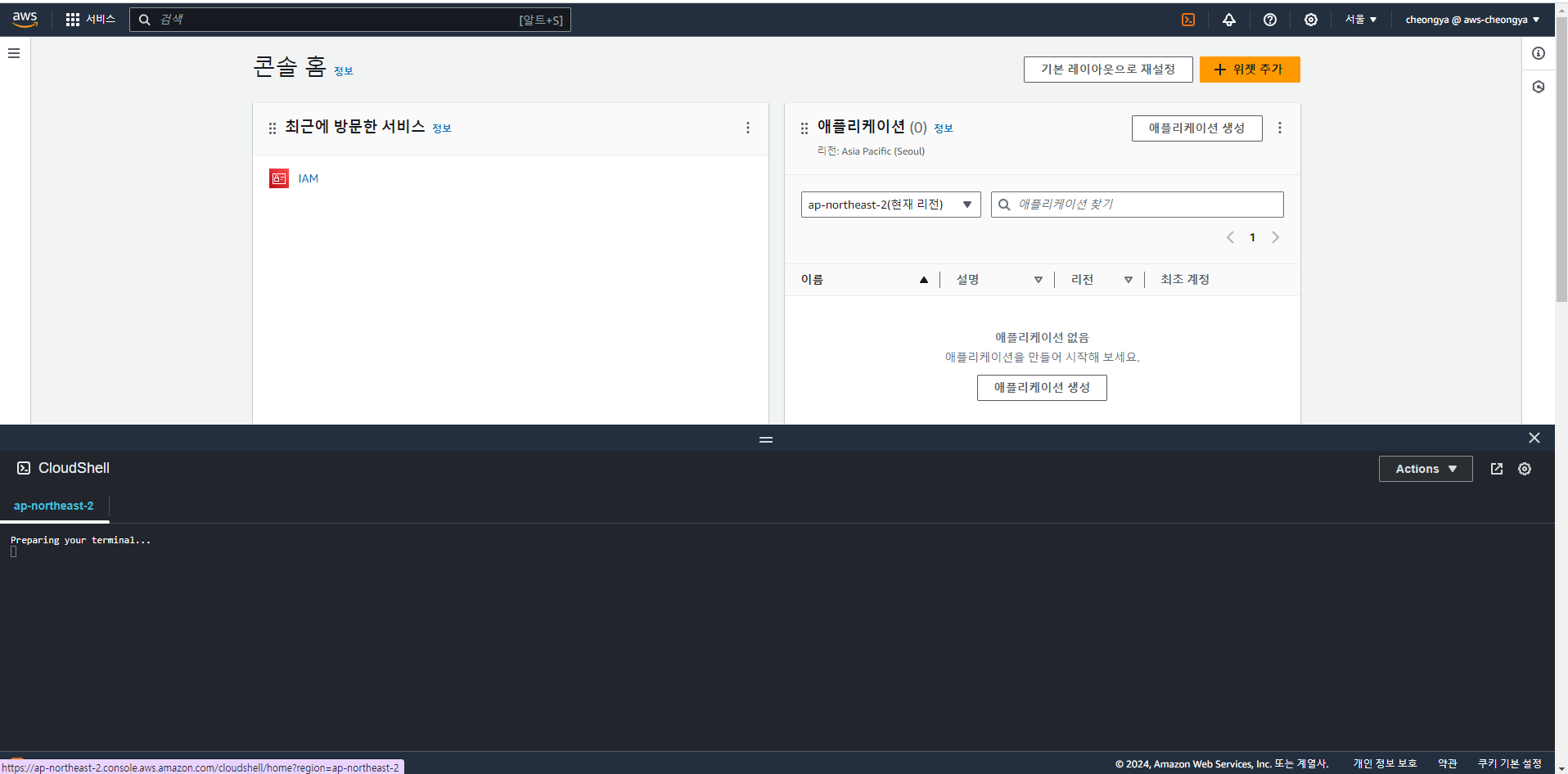
## AWS CloudShell

미국 동부(오하이오), 미국 동부(버지니아 북부), 미국 서부(오리곤), 아시아 태평양(뭄바이), 아시아 태평양(시드니), 아시아 태평양(도쿄), 유럽(프랑크푸르트), 유럽(아일랜드) AWS 리전에서 사용할 수 있다.

가장 왼쪽에 있는 터미널 아이콘을 클릭한다.

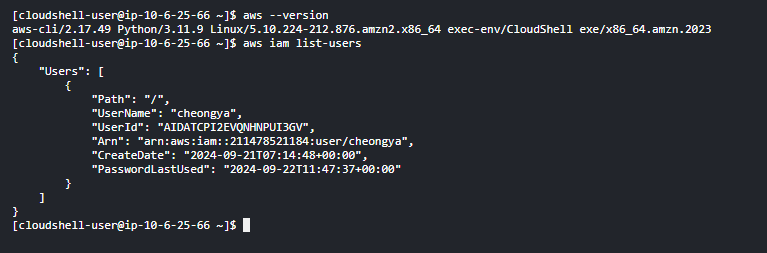


그러면 화면의 하단에 CloudShell이 생성되는 것을 확인할 수 있다.

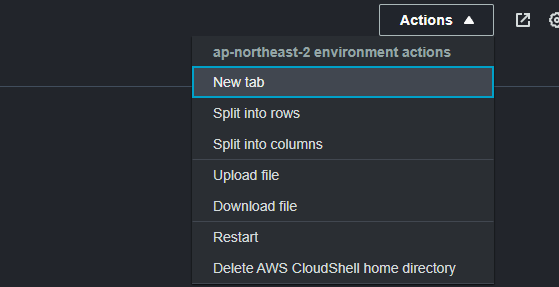


### 특징

aws의 명령어 기능을 수행할 수 있다.



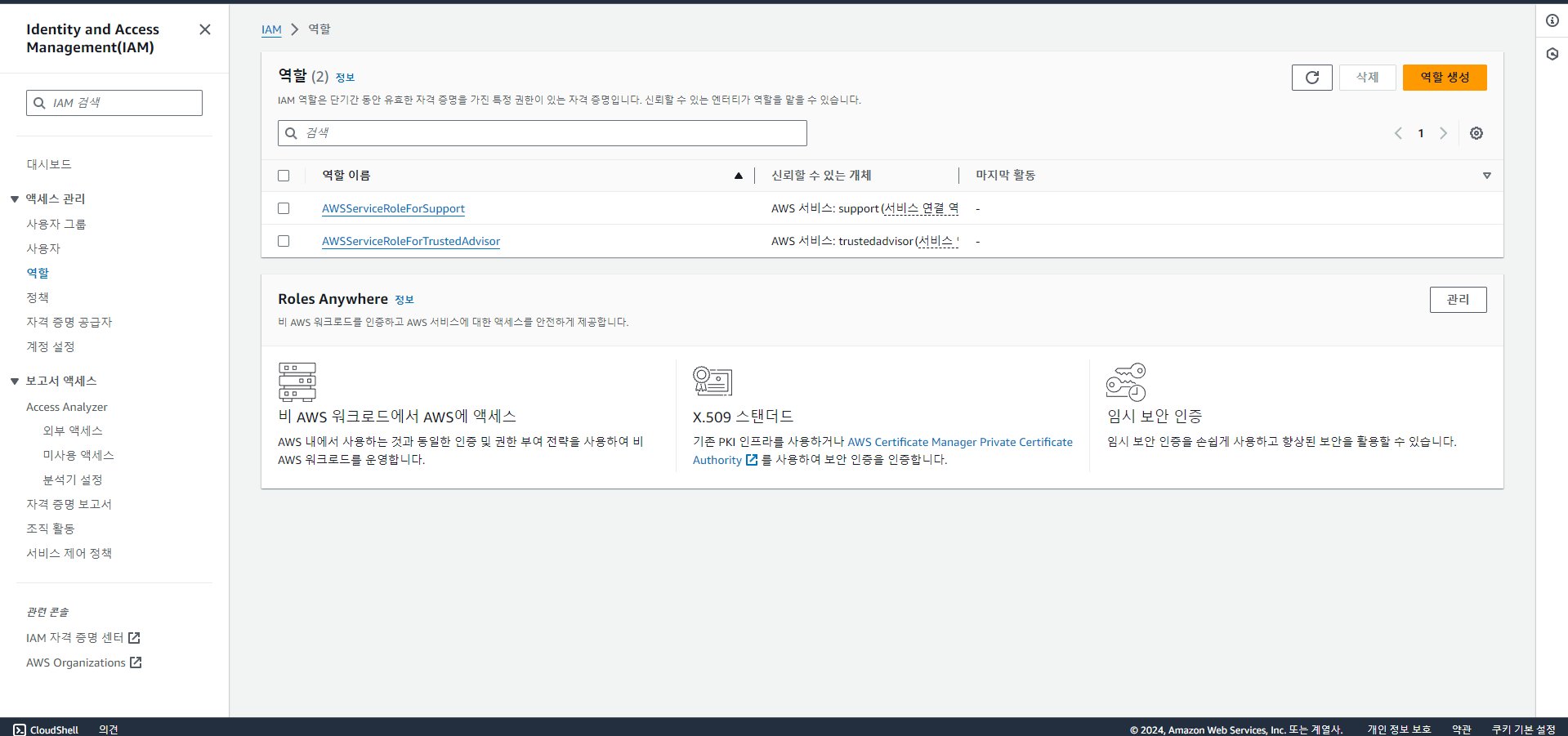
파일을 다운로드, 업로드 등을 할 수 있다.



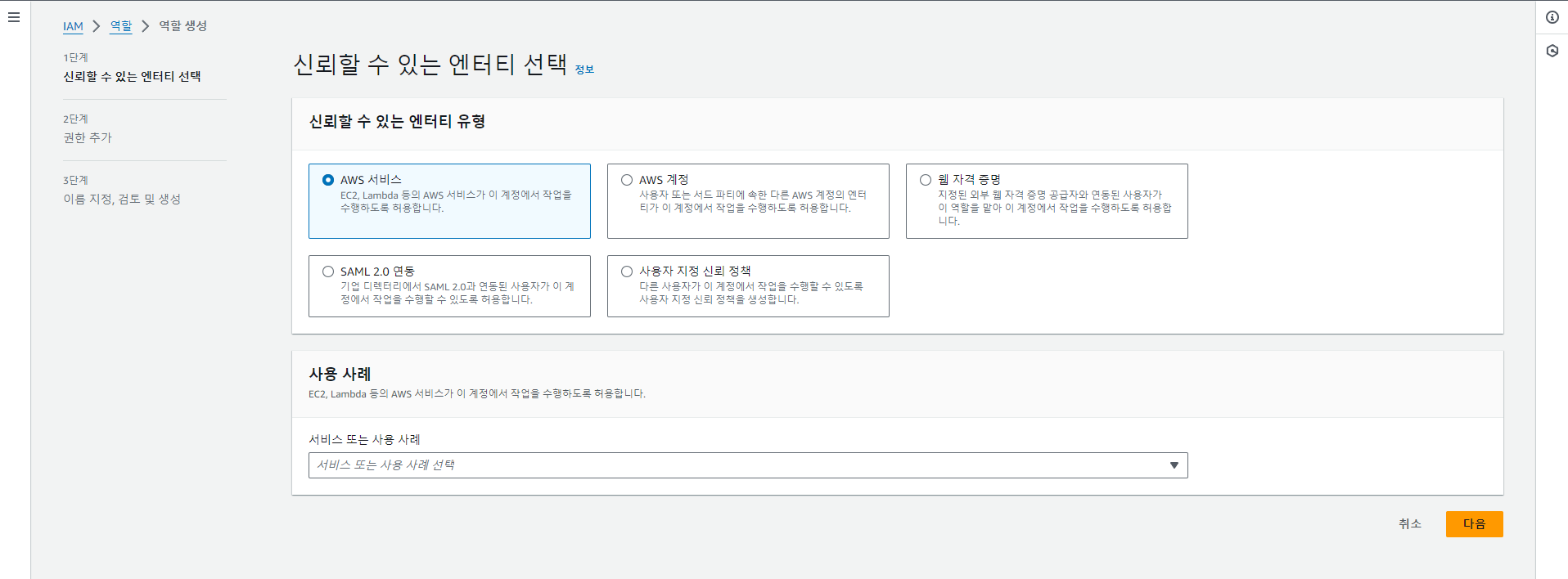
CloudShell에는 별도의 저장소가 따로 있어 파일을 생성한 후 재시작을 한다고 해도 파일이 남아있다.

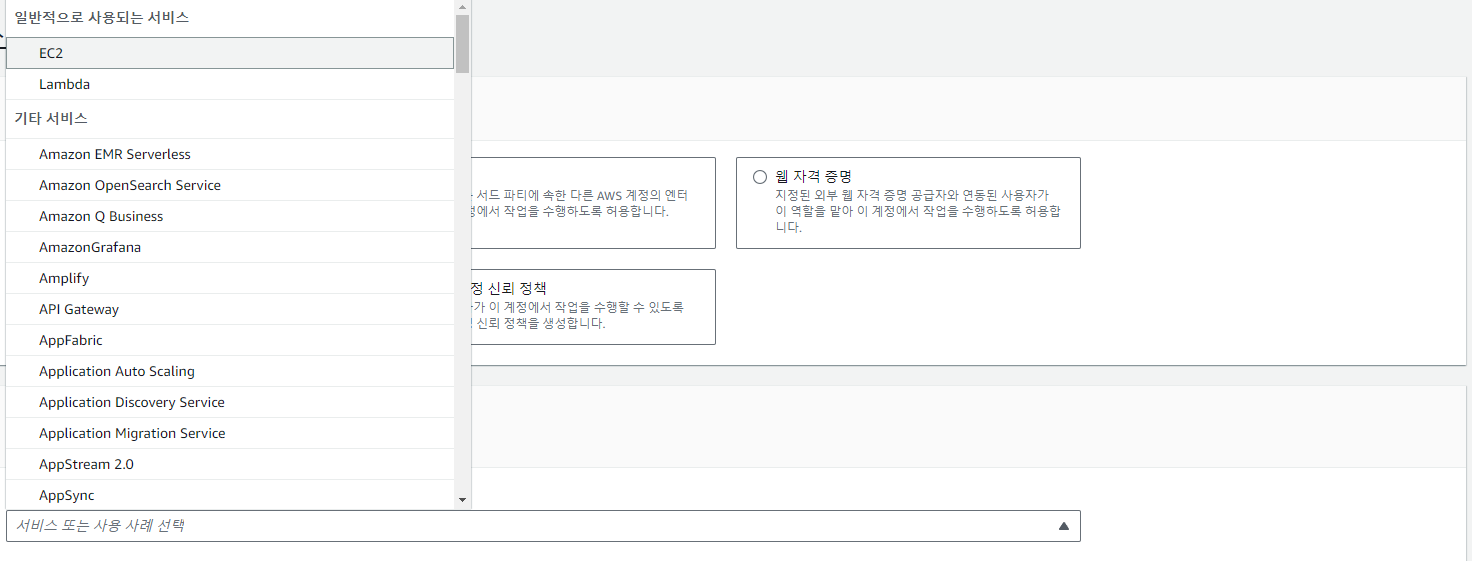
## IAM Role(역할)

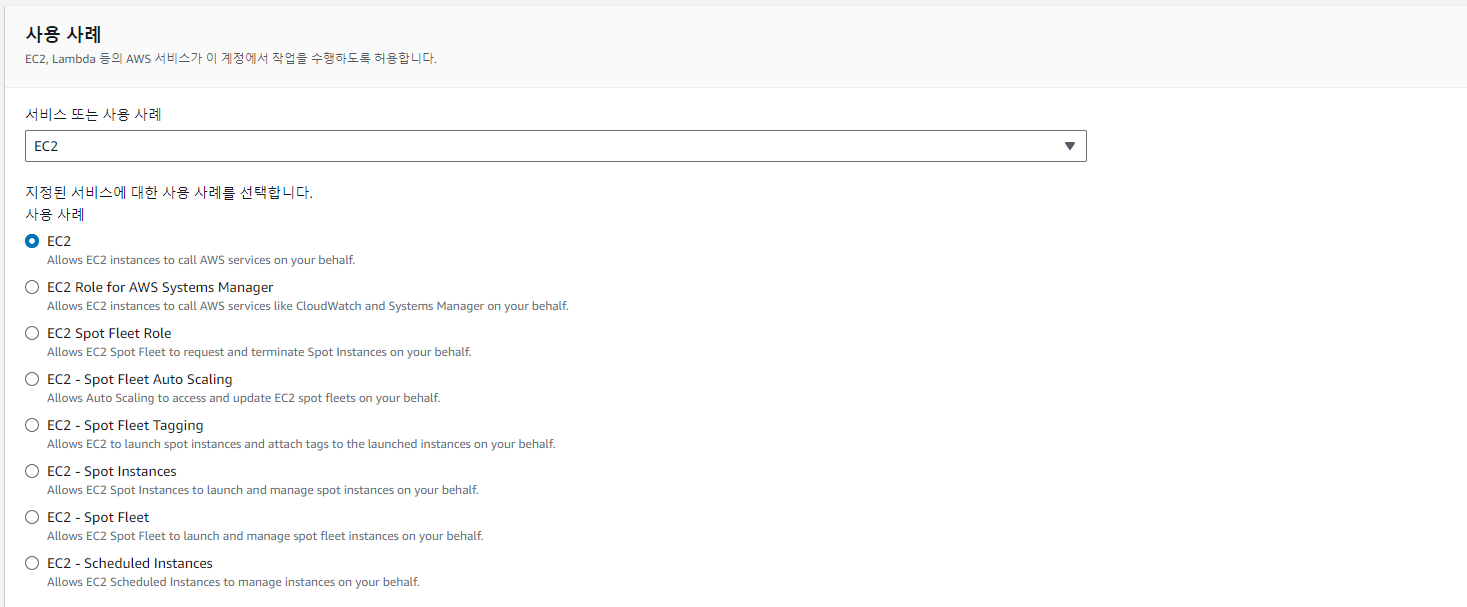
IAM -> 역할 클릭 후 역할 생성 클릭



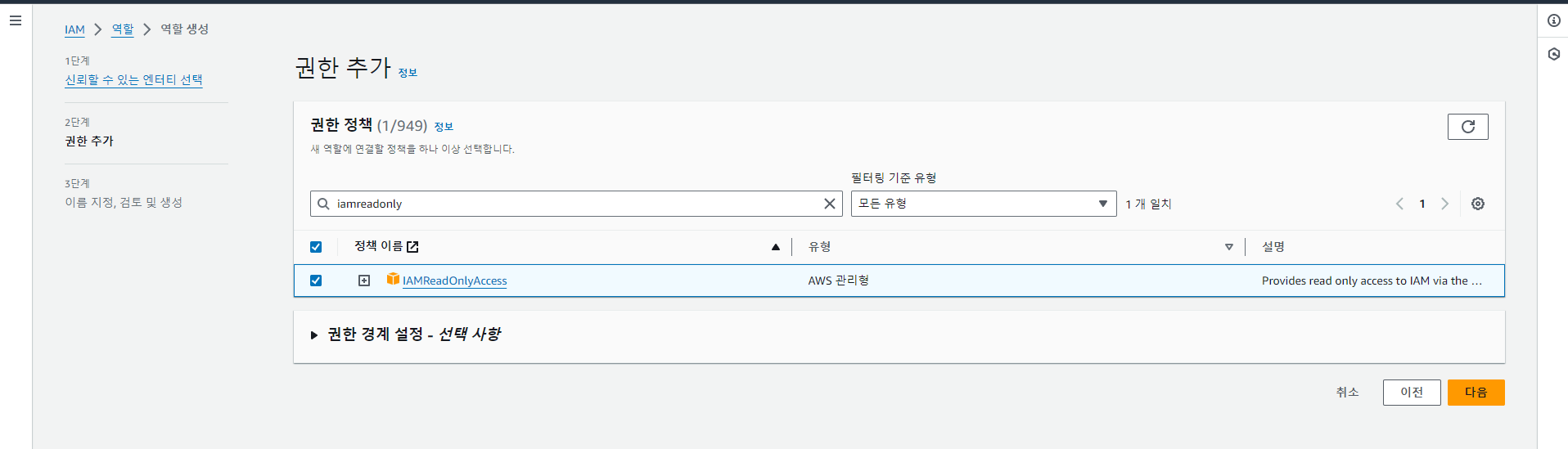
신뢰할 수 있는 엔티티 유형과 사용 사례 선택



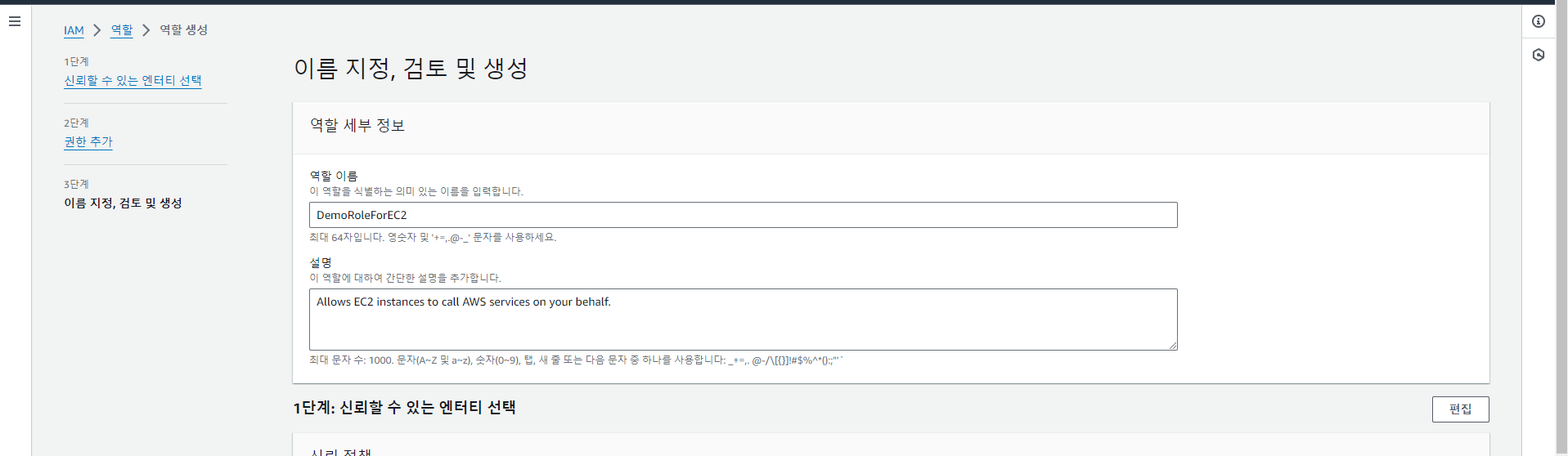


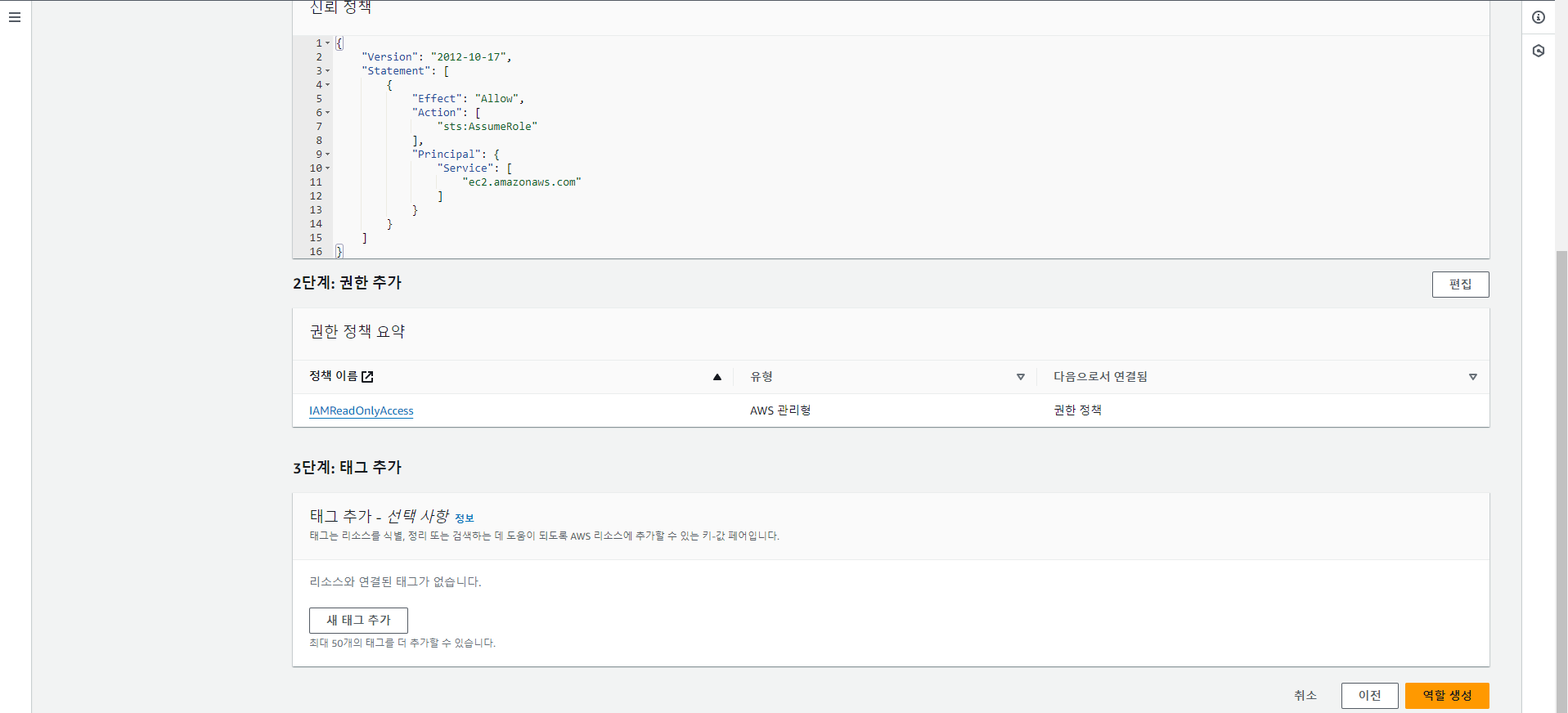


추가할 권한 선택

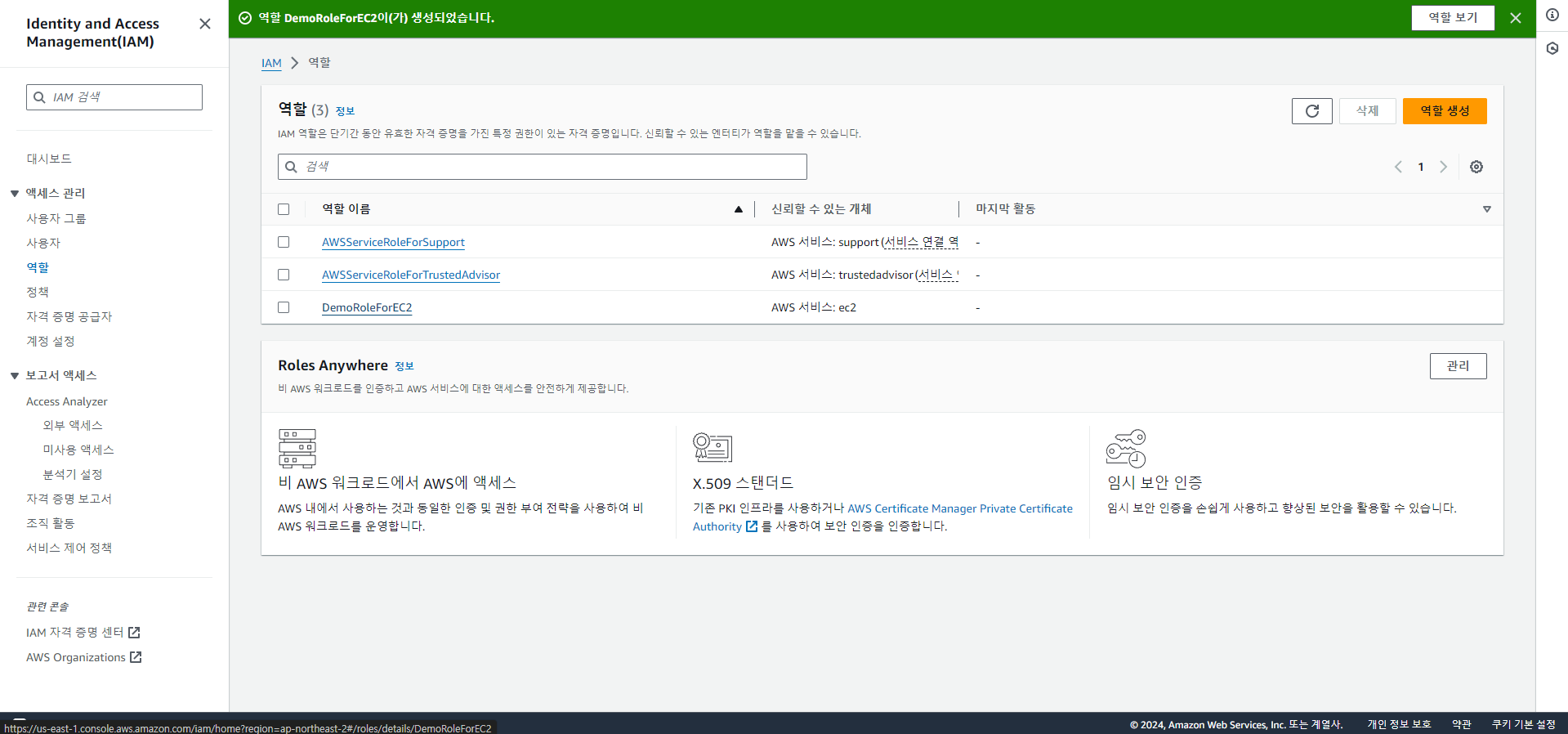


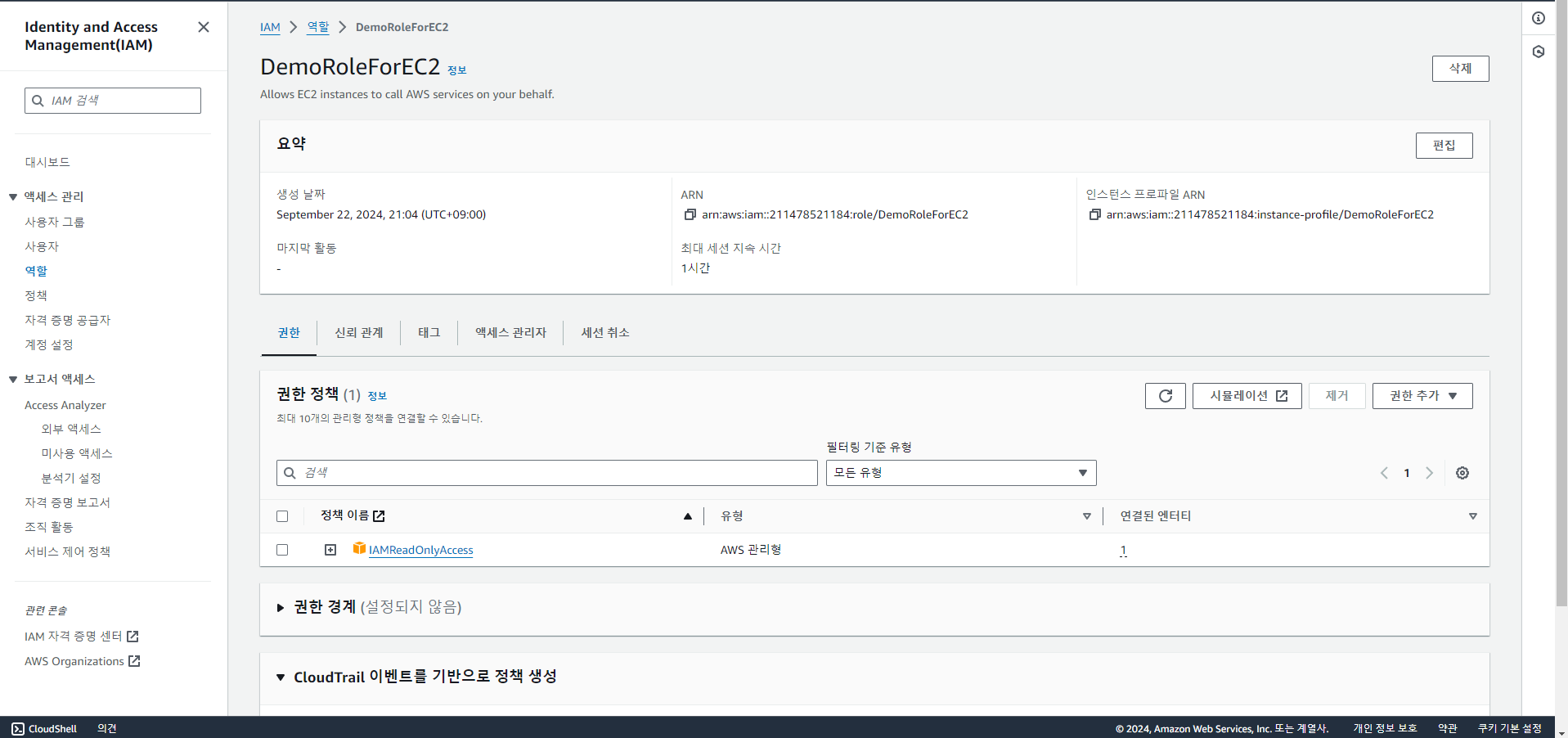
역할 이름 지정 및 검토





생성 후 확인

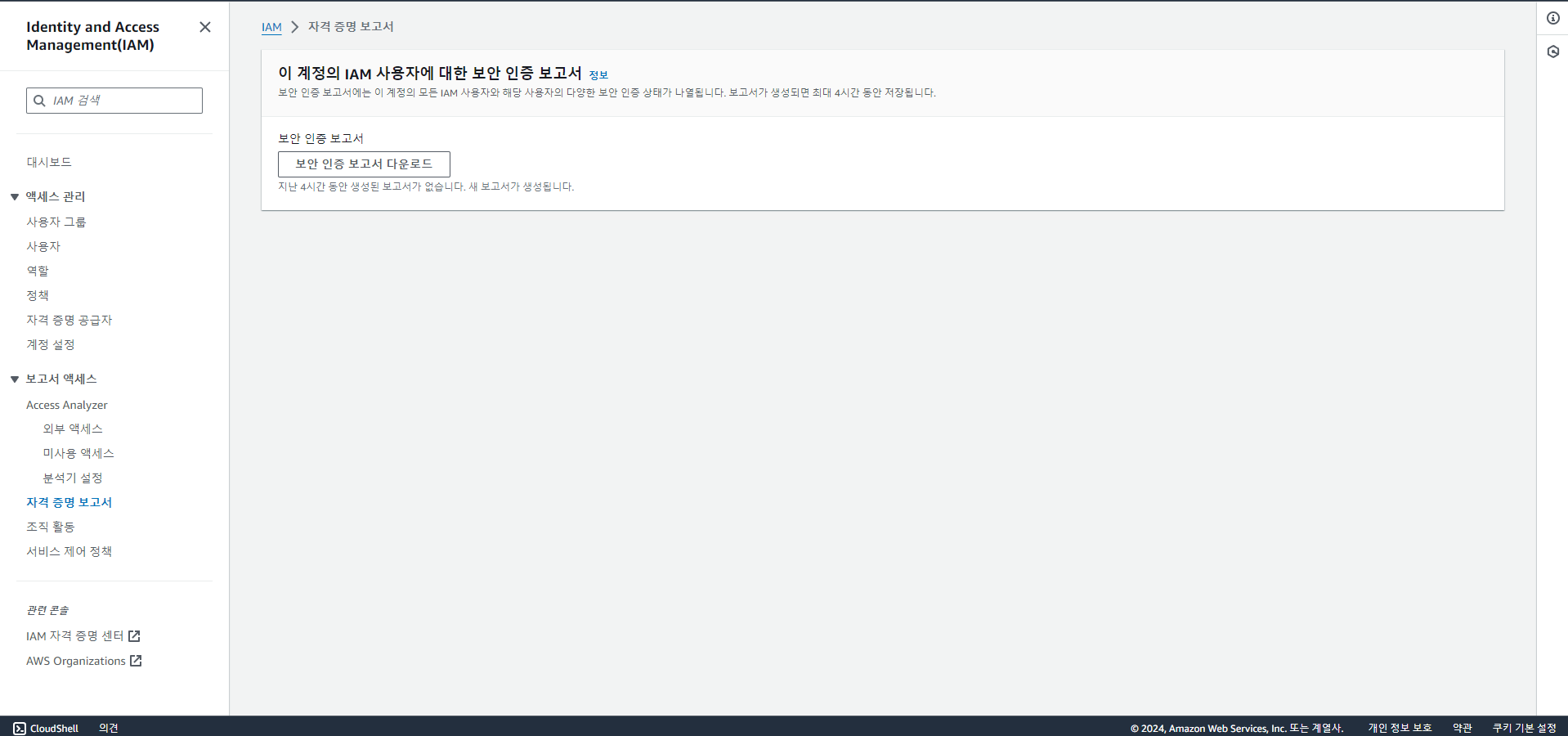




## IAM 보안 도구

### 자격 증명 보고서(Credential report)

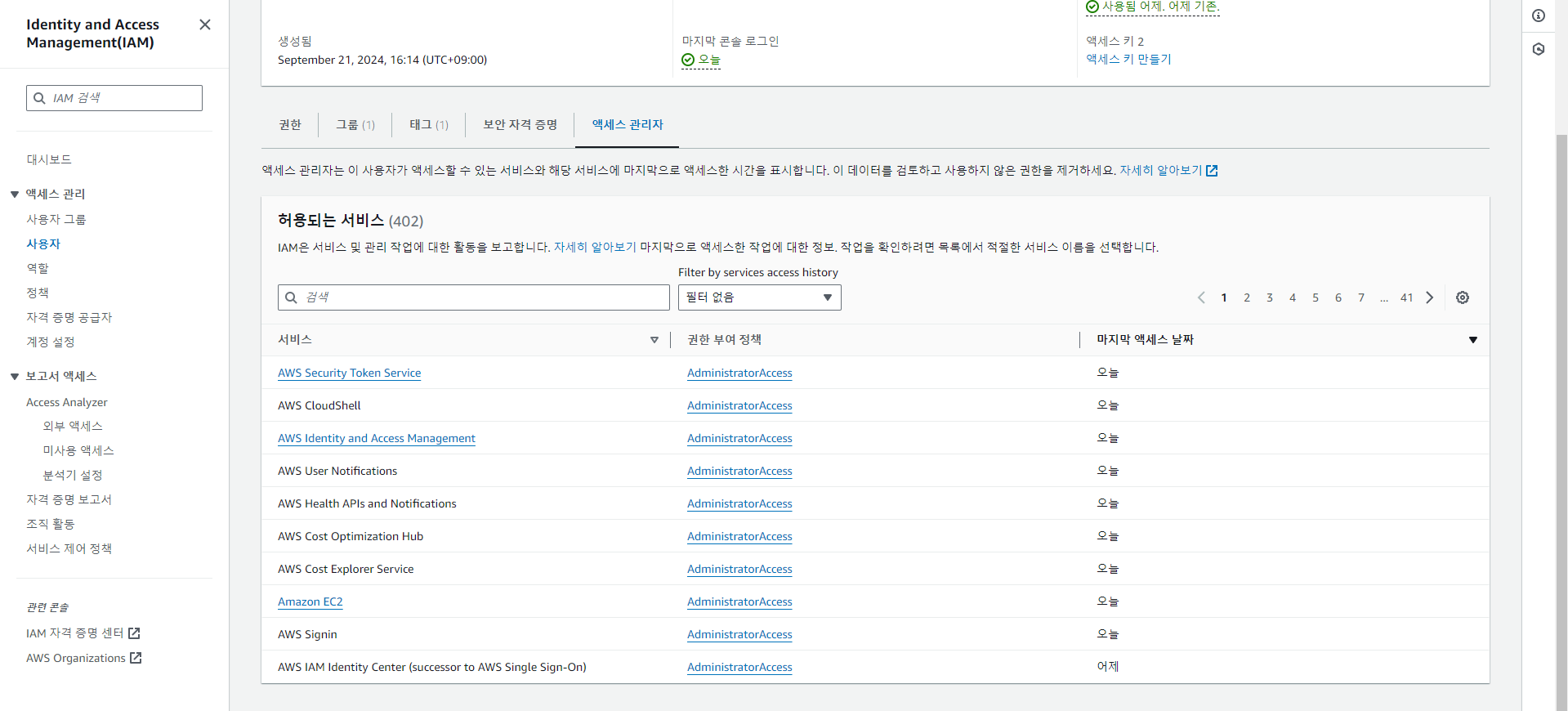
IAM -> 자격 증명 보고서 -> 보안 인증 보고서 다운로드를 클릭하면 .csv 파일이 다운로드 된다.



csv 파일에서는 root 사용자와 일반 사용자에 대한 정보들을 확인할 수 있다.

### 액세스 관리자

사용자 -> 사용자 명 클릭 -> 액세스 관리자로 들어오면 사용자가 올바른 권한을 가지고 있는지 여부를 확인할 수 있다.



## 모범 사례

1. AWS 계정을 설정할 때를 제외하고는 루트 계정을 사용하지 마라.
2. 한 명의 AWS 사용자는 한 명의 물리적 사용자와 동일하다.  
   친구가 AWS를 사용하고 싶어하는 경우 자격 증명 정보를 제공하지 말고 다른 사용자를 생성하라.
3. 사용자를 그룹에 할당하고 그룹에 권한을 할당하여 보안이 그룹 수준에서 관리되도록 하라.
4. 강력한 비밀번호 정책을 만들어라.
5. 다중 인증 또는 MFA를 사용해라.
6. AWS 서비스에 권한을 부여할 때 역할을 생성하고 사용하는 것이 좋다.
7. CLI 또는 일부 SDK에서 액세스 키를 생성해야 한다.
8. IAM 사용자와 액세스 키를 절대로 공유하지 마라.