

[IAM - Identity And Access Management]

-계정 권한 관리

-AWS의 계정 및 권한 관리 서비스이다

-AWS 서비스 + 리소스에 대한 접근 관리

-리전 단위 X

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

- 루트계정 말고, IAM 계정으로 서비스를 사용하고 최소한의 권한만 부여한다(최소권한 원칙)

-루트계정 - 개별사용자 사이 : 강력한 암호 + 멀티팩터인증(MFA)- 다중 인증이라고 생각하면된다 --

적용이 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 액세스 키나 암호, 이메일 주소, 계정 이름 등의 계정 설정을 변경할 때 사용한다
2. AWS 계정을 닫을때
3. AWS 지원플랜을 변경, 취소할때
4. 인스턴스를 팔려고할때 (인스턴스 매매가능하다- 마켓플레이스 판매자로 등록가능)
5. MFA - 멀티팩터인증(다중인증) 삭제 Delete를 활성화하도록 Amazon S3 버킷(오브젝트 데이터 저장서비스) 을 구성할때
6. 잘못된 VPC(AWS 네트워크임) ID 또는 VPC 엔드포인트 ID가 들어있는 Amazon S3 버킷 정책을 편집하거나 삭제할때

[IAM 의 액세스 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 액세스 하는 권한

나아가 **IAM 정책**이라는 용어가 있는데

이는 AWS 리소스에 대한 액세스 권한을 정의 한 것이라고 보면된다.

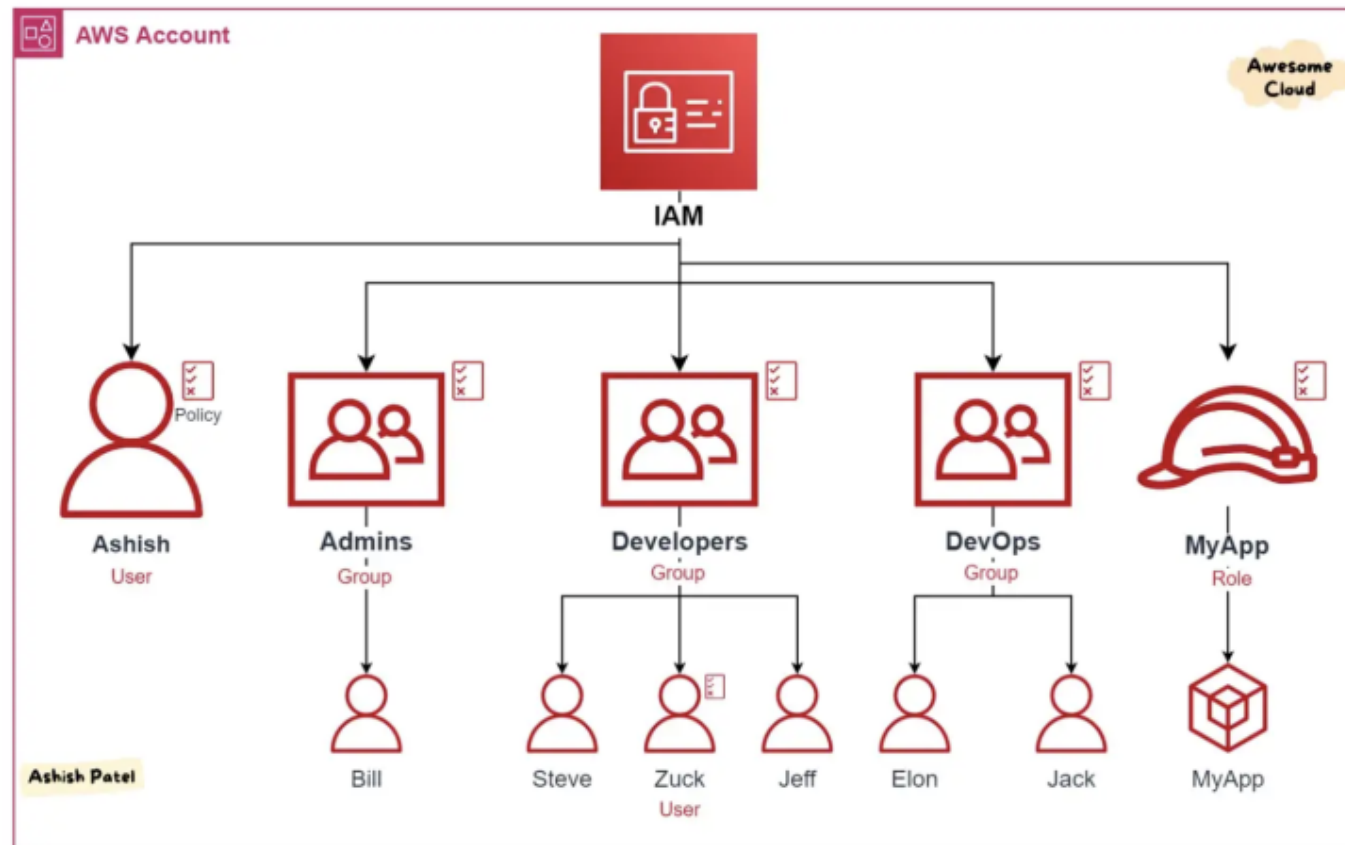
쉽게 말해 권한을 통해 인증되고, 이후 부여된 리소스 라고 생각하면된다.

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 거부가 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 대시보드

보안 권장 사항 **2**

루트 사용자에게 MFA 추가

루트 사용자에게 MFA 추가 - 루트 사용자에게 다중 인증(MFA)을 활성화하여 이 계정의 보안을 강화합니다.

MFA 추가

루트 사용자에게 활성 액세스 키가 없음

루트 사용자 대신 IAM 사용자에게 연결된 액세스 키를 사용하면 보안이 향상됩니다.

AWS 결제, 비용 관리, 계정 콘솔에 대한 액세스 권한 업데이트

결제, 비용 관리 및 계정 콘솔에 대한 IAM 작업을 세분화된 IAM 작업으로 대체하고 있습니다. aws-portal:ViewBilling, aws-portal:ModifyBilling, aws-portal:ViewAccount, aws-portal:ModifyAccount, aws-portal:ViewPaymentMethods, aws-portal:ModifyPaymentMethods, aws-portal:ViewUsage, purchase-orders:ViewPurchaseOrders 및 purchase-orders:ModifyPurchaseOrders. AWS 결제, 비용 관리 및 계정 콘솔 기반 기능에 대한 액세스 권한을 잃지 않으려면 2023년 7월 전에 새로운 IAM 작업을 포함하도록 기존 IAM 정책을 업데이트합니다. 영향을 받는 기능의 예로는 AWS Cost Explorer, AWS Budgets, 결제 콘솔 등이 있습니다. 더 자세한 내용은 [blog](#) (블) 참조하세요.

영향을 받는 정책 보기

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

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

1단계

MFA 디바이스 선택

2단계

디바이스 설정

MFA 디바이스 선택

MFA 디바이스 이름 지정

디바이스 이름

이 디바이스를 식별하는 의미 있는 이름을 입력합니다.

최대 128자입니다. 영숫자 및 '* = , . @ - _' 문자를 사용하세요.

MFA 디바이스 선택 [Info](#)

인증이 필요할 때마다 사용자 이름 및 암호 외에 사용할 MFA 디바이스를 선택합니다.

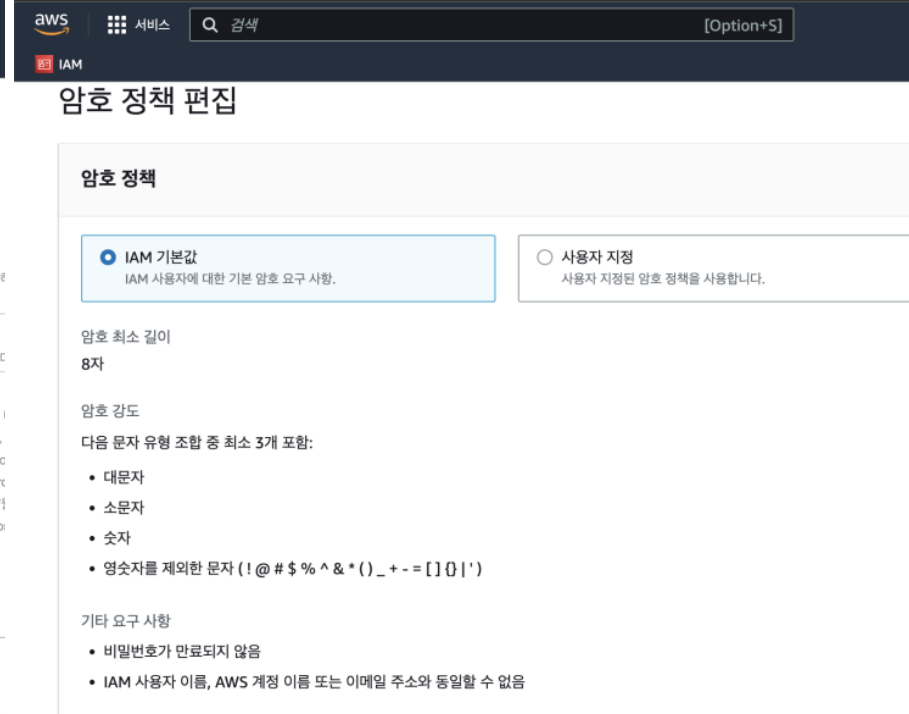
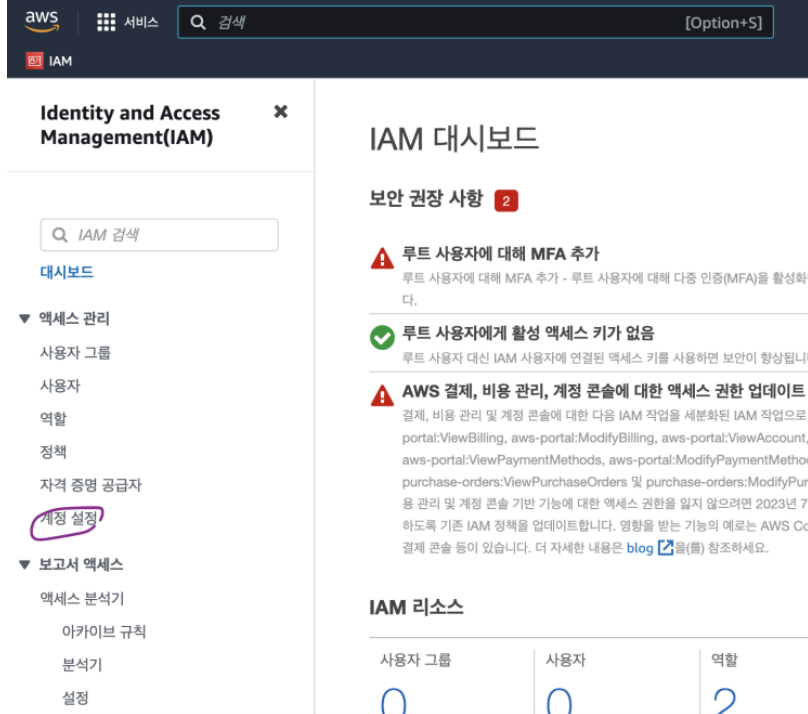


인증 관리자 앱

모바일 디바이스 또는 컴퓨터에 설치된 앱에서 생성된 코드를 사용하여 인증합니다.

MFA 활성화 방법

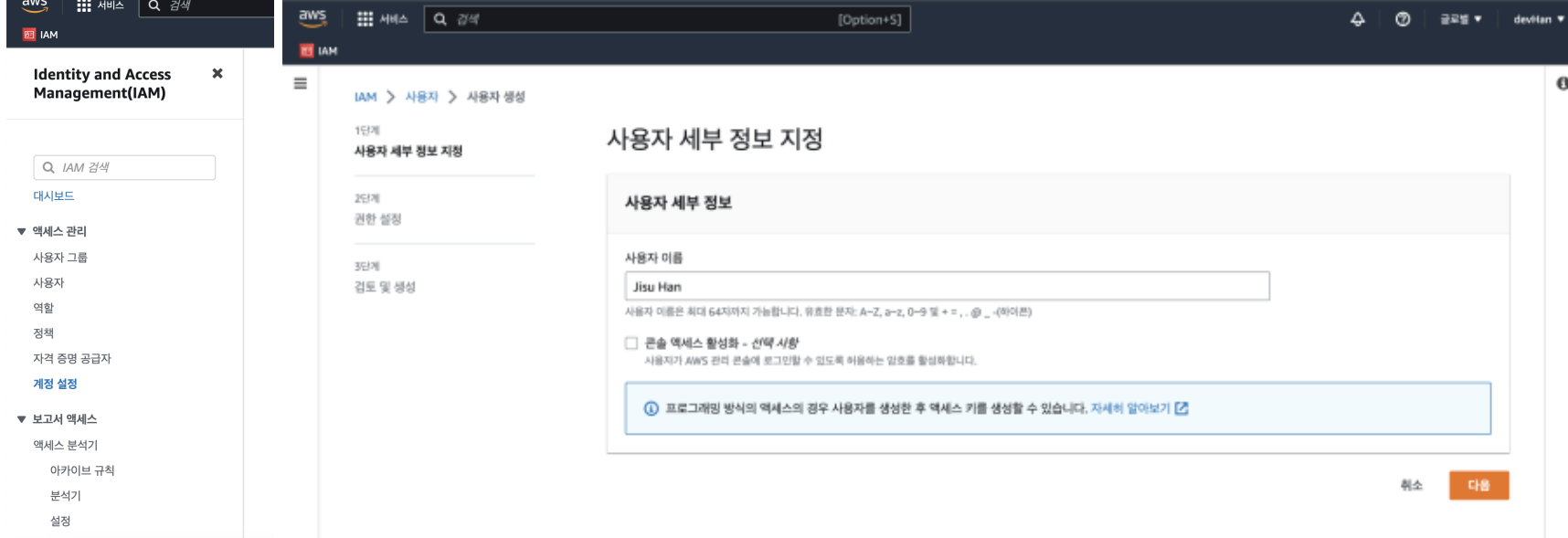
IAM 계정 설정 방법



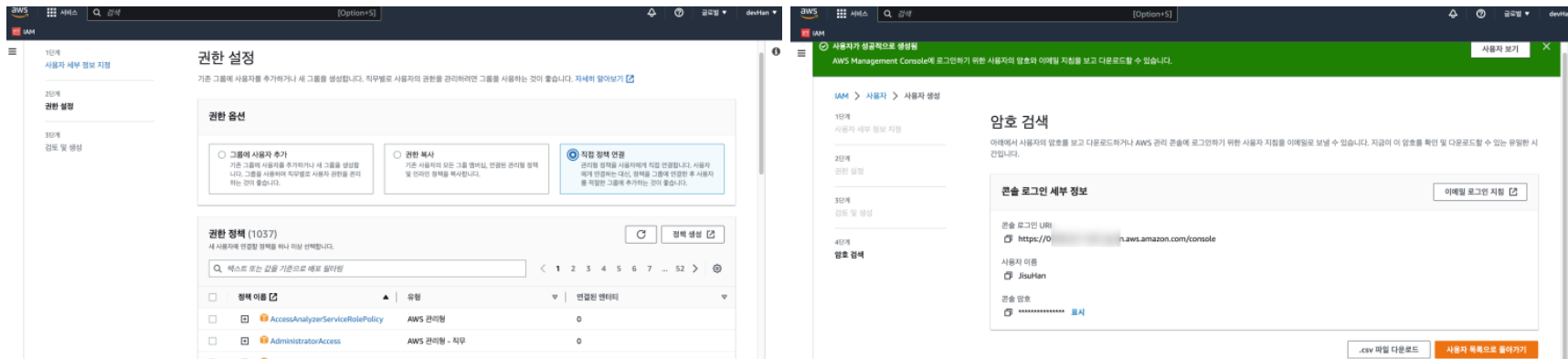
IAM-계정설정 - 암호정책 편집가능

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

[User IAM 설정]

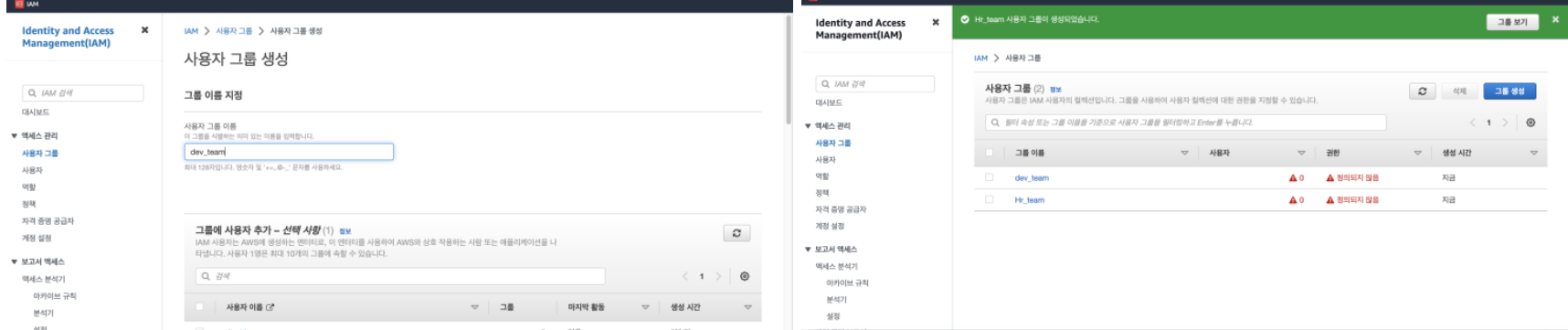


IAM 사용자(User) IAM 설정



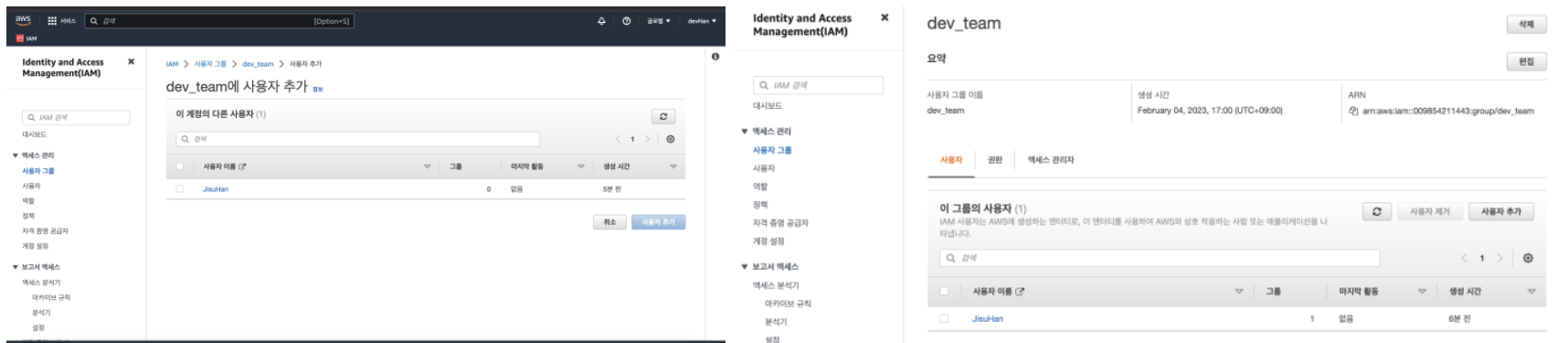
IAM 직접 권한 설정이 가능

[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.



로그인

☐ 루트 사용자

무제한 액세스 권한이 필요한 작업을 수행하는 계정 소유자입니다. 자세히 알아보기

☒ IAM 사용자

일일 작업을 수행하는 계정 내 사용자입니다. 자세히 알아보기

계정 ID(12자리) 또는 계정 별칭

다음

계속 진행하는 경우 [AWS 고객 계약](#) 또는 [AWS 서비스에 대한 기타 계약 및 개인 정보 보호 정책](#)에 동의하게 됩니다. 이 사이트는 필수 쿠키를 사용합니다. 자세한 내용은 [주기](#) [고지](#)를 참조하세요.

————— AWS를 처음 사용하십니까? —————

[AWS 계정 새로 만들기](#)



루트가 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.

The screenshot displays the AWS IAM console interface. On the left, the 'AWS 계정' (AWS Account) page is visible, showing the account ID '009854211443' and the IAM user name 'JisuHan'. Below this, there are input fields for '이전 비밀번호' (Previous Password), '새 비밀번호' (New Password), and '새 비밀번호 재입력' (New Password Confirmation), along with a '비밀번호 변경 확인' (Confirm Password Change) button. On the right, the '암호 정책 편집' (Edit Password Policy) page is shown. It features two radio buttons: 'IAM 기본값' (IAM Defaults) and '사용자 지정' (Custom). The '사용자 지정' option is selected. Below the radio buttons, there are checkboxes for '암호 최소 길이' (Minimum password length), '암호 강도' (Password strength), and '기타 요구 사항' (Other requirements). The '사용자 자신의 암호 변경 허용' (Allow user to change their own password) checkbox is checked, indicated by a purple checkmark.

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.

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

자격 증명 공급자

계정 설정

▼ 보고서 액세스

액세스 분석기

아카이브 규칙

분석기

IAM > 사용자 그룹 > dev_team

dev_team

삭제

편집

요약

사용자 그룹 이름

dev_team

생성 시간

February 04, 2023, 17:00 (UTC+09:00)

ARN

arn:aws:iam::009854211443:group/dev_team

사용자

권한

액세스 관리자

권한 정책 (0) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

Q 속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

정책 연결

인라인 정책 생성

정책 이름

유형

설명

IAM - 사용자 그룹 - dev_team 사용자 그룹에 권한을 추가할 것이다.

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

Identity and Access Management(IAM)

Q IAM 검색

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

자격 증명 공급자

계정 설정

▼ 보고서 액세스

액세스 분석기

아카이브 규칙

분석기

기타 권한 정책 (선택됨 1/809)

이 사용자 그룹에 최대 10개의 관리형 정책을 연결할 수 있습니다. 이 그룹의 모든 사용자는 연결된 권한을 상속합니다.

Q 속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

9 개 일치

"iam" X

필터 지우기

정책 이름

유형

설명

☐

AWSQuickSightListIAM

AWS 관리형

Allow QuickSight to li

☐

IAMSelfManageServiceSpecificCredentials

AWS 관리형

Allows an IAM user tc

☐

IAMFullAccess

AWS 관리형

Provides full access t

☐

IAMUserChangePassword

AWS 관리형

Provides the ability fc

☒

IAMReadOnlyAccess

AWS 관리형

Provides read only ac

☐

IAMUserSSHKeys

AWS 관리형

Provides the ability fc

☐

IAMAccessAdvisorReadOnly

AWS 관리형

This policy grants acc

☐

IAMAccessAnalyzerReadOnlyAccess

AWS 관리형

Provides read only ac

IAMReadOnlyAccess 권한 부여

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

확인해보면 아래와 같다

dev_team

삭제

요약

편집

사용자 그룹 이름

dev_team

생성 시간

February 04, 2023, 17:00 (UTC+09:00)

ARN

arn:aws:iam::009854211443:group/dev_team

사용자

권한

엑세스 관리자

권한 정책 (1) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

검색

속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

< 1 >

설정

정책 이름

유형

설명

IAMReadOnlyAccess

AWS 관리형

Provides read only access to IAM via the AWS Management Console.

dev_team

삭제

요약

편집

사용자 그룹 이름

dev_team

생성 시간

February 04, 2023, 17:00 (UTC+09:00)

ARN

arn:aws:iam::009854211443:group/dev_team

사용자

권한

엑세스 관리자

권한 정책 (1) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

검색

속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

< 1 >

설정

정책 이름

유형

설명

IAMReadOnlyAccess

AWS 관리형

Provides read only access to IAM via the AWS Management Console.

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