aws re/start

AWS Identity 및 Access Management(IAM) 검토

학습 내용

강의의 핵심

배울 내용은 다음과 같습니다.

- AWS Identity 및 Access Management(IAM)를 검토합니다.
- 보안 인증 정보의 유형과 IAM 사용자 및 IAM 역할의 개념을 검토합니다.
- IAM 모범 사례를 설명합니다.

주요 용어:

- IAM
- 인증
- 사용 권한
- AWS 계정 루트 사용자
- 다중 요소 인증(MFA)

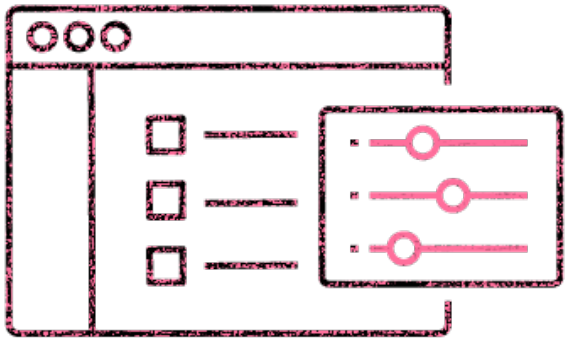
AWS Identity 및 Access Management(IAM)

IAM 검토

AWS Identity 및 Access Management(IAM)

인증과 AWS 리소스에 대한 액세스를 중앙에서 관리할 수 있습니다.

- 추가 비용 없이 AWS 계정의 기능으로 제공됩니다.
- 사용자, 그룹 및 역할을 생성합니다.
- 여기에 정책을 적용하여 AWS 리소스에 대한 액세스를 제어합니다.



AWS 서비스 액세스

프로그래밍 방식 액세스

- 액세스 키 ID와 보안 액세스 키를 인증합니다.
- 애플리케이션 프로그램 인터페이스(API), AWS Command Line Interface(AWS CLI), 소프트웨어 개발 키트(SDK) 및 기타 개발 도구에 대한 액세스를 제공합니다.

콘솔 액세스

- 계정 ID 또는 별칭, IAM 사용자 이름 및 암호를 사용합니다.
- 이 옵션을 활성화하면 MFA에서 인증 코드를 묻습니다.

AWS CLI

SDK

AWS 관리 콘솔

보안 인증 정보의 유형

인증 정보의 유형	설명
이메일 주소 및 암호	AWS 계정(루트 사용자)과 연결됨
IAM 사용자 이름 및 암호	AWS Management Console 액세스에 사용됨
액세스 키	일반적으로 API 및 SDK를 통한 프로그래밍 방식 요청 및 AWS CLI와 함께 사용됨
다중 요소 인증(MFA)	추가 보안 계층 계정 루트 사용자 및 IAM 사용자에 대해 활성화할 수 있음
키 페어	Amazon Elastic Compute Cloud(Amazon EC2)와 같은 특정 AWS 서비스에만 사용됨

정책 및 권한(1/2)

권한 정책	권한 경계	관리형 정책	인라인 정책
		✓	✓
✓			
	✓		
✓			

정책 및 권한(2/2)

IAM 정책 예시:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "MFA-Access",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                },
                "IpAddress": {
                    "aws:SourceIp": "1.2.3.4/32"
                }
            }
        }
    ]
}
```

IAM 역할 사용하기

IAM 역할이 할당된 사용자는 다음을 제공할 수 있습니다.

- AWS 서비스에 다른 AWS 리소스에 액세스할 수 있는 권한
- Security Assertion Markup Language(SAML) 2.0 또는 OAuth 2.0 등의 통합 인증(SSO) 액세스

다음 리소스에 액세스하도록 역할을 전환합니다.

- AWS 계정
- 다른 AWS 계정(교차 계정 액세스)

IAM 사용자 역할 위임

사용자 기반 권한

특정 엔터티가 액세스할 수 있는 것은 무엇입니까?

Xiulan

	읽기	쓰기	나열
리소스 X	✓	✓	✓

Saanvi

	읽기	쓰기	나열
리소스 Y	✓		
리소스 Z	✓		

관리자

	읽기	쓰기	나열
리소스 X			✓
리소스 Y			✓
리소스 Z			✓

리소스 기반 권한

특정 리소스에 액세스할 수 있는 사람은 누구입니까?

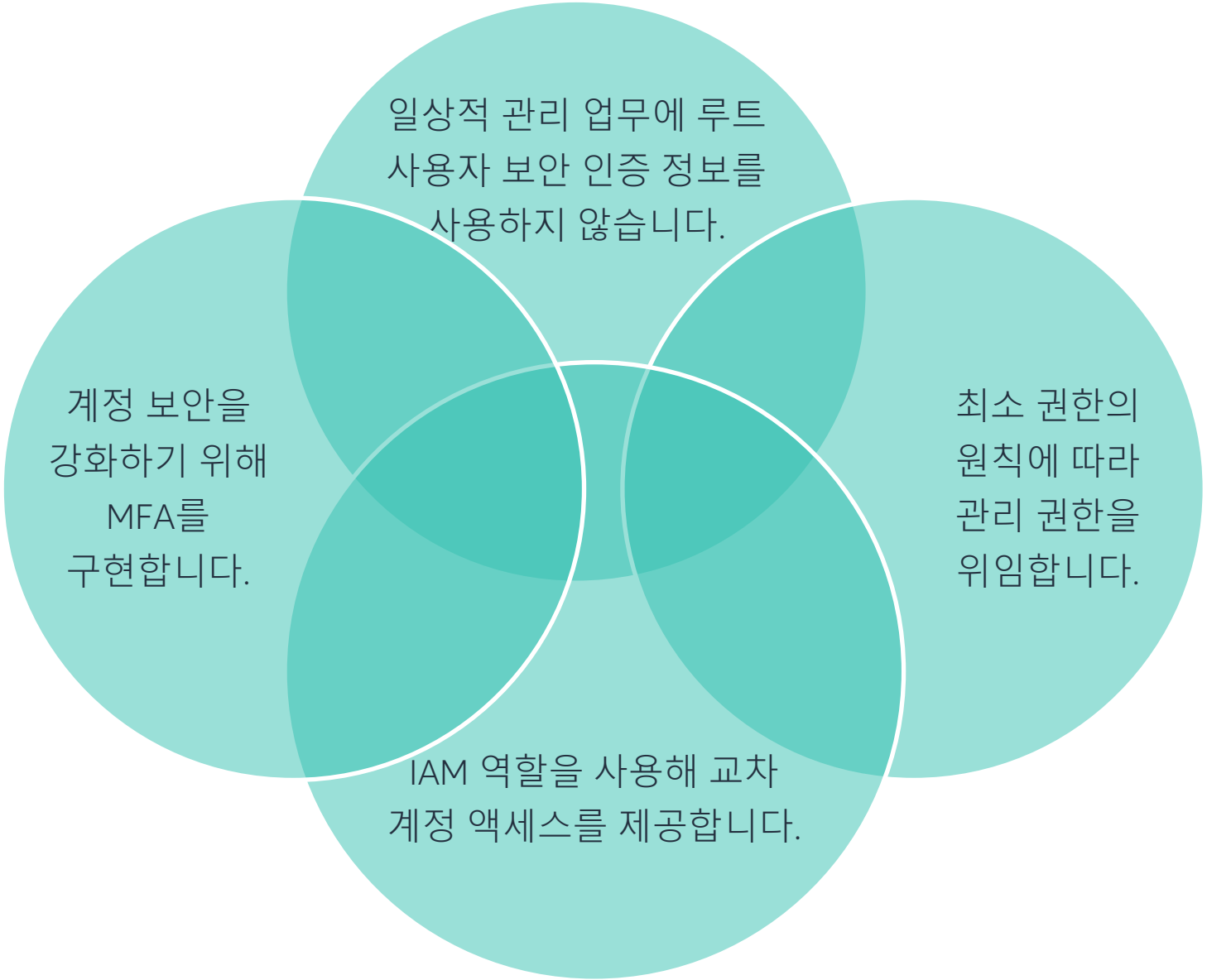
리소스 X

	읽기	쓰기	나열
Bob	✓	✓	✓
Xiulan	✓	✓	✓
Efua	✓		✓
Arnav			✓

리소스 Y

	읽기	쓰기	나열
Bob	✓	✓	✓
Saanvi	✓		
Diego		✓	✓

IAM 모범 사례


일상적 관리 업무에 루트 사용자 보안 인증 정보를 사용하지 않습니다.
계정 보안을 강화하기 위해 MFA를 구현합니다.
최소 권한의 원칙에 따라 관리 권한을 위임합니다.
IAM 역할을 사용해 교차 계정 액세스를 제공합니다.

핵심 사항

- IAM은 세 가지 유형의 아이덴티티를 사용합니다.
  - 사용자
  - 그룹
  - 역할
- AWS 리소스는 콘솔(웹 페이지)이나 AWS CLI를 통해 또는 프로그래밍 방식으로 액세스할 수 있습니다.
- IAM 정책은 권한을 정의하는 JSON 문서입니다. 이 권한은 사용자, 그룹, 역할에 적용됩니다.
- 역할을 통해 사용자는 일시적으로 역할로 정의된 특정 권한을 위임할 수 있습니다.
- 일상적인 관리 태스크에는 계정 루트 사용자를 사용하지 마십시오.
- 권한을 할당할 때 최소 권한의 원칙을 사용하십시오.
- 역할을 사용해 교차 계정 액세스를 제공하십시오.
- 가능한 경우 MFA를 사용하십시오.

aws re/start