

AWS Security

Jae Hyeon Kim

— 목차

1. Identity & Access Management
2. AWS CloudTrail
3. AWS CloudWatch
4. 경보 체계 구성

Identity & Access Management

- 사용자 분류

어플리케이션 사용자
Identities: 어플리케이션 사용자, 어플리케이션 운영자



NETFLIX

운영체제 / 플랫폼 사용자
Identities: 개발자, 시스템 엔지니어, DevOps



AWS 사용자
Identities: 개발자, DevOps 엔지니어, 테스터, 소프트웨어/플랫폼
AWS Identities 간의 상호 작용
EC2 인스턴스와 EBS 스토리지의 프로비저닝
Load Balancer 구성



— AWS Identity and Access Management(IAM)

- AWS Identity and Access Management(IAM)은 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- IAM을 사용하여 리소스를 사용하도록 인증 및 인가된 대상을 제어한다




— IAM 기능

- AWS 계정에 대한 공유 액세스
- 세분화된 권한
- Amazon EC2에서 실행되는 애플리케이션을 위한 보안 AWS 리소스 액세스
- 멀티 팩터 인증(MFA)
- 많은 AWS 서비스와의 통합

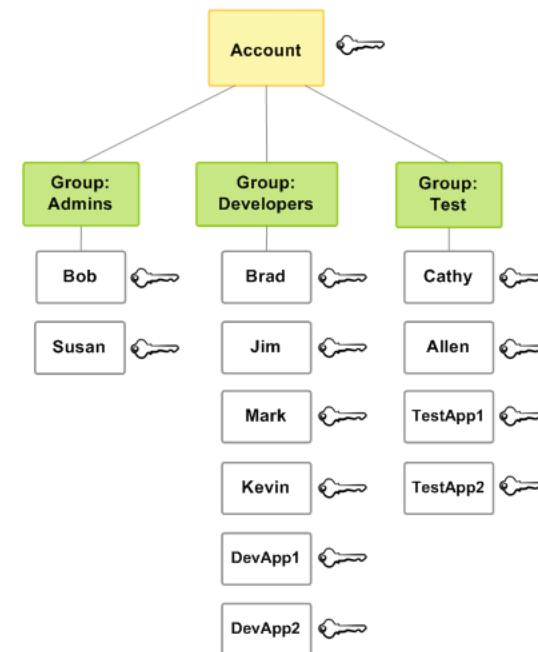
— AWS Identity

- IAM Principal은 AWS 계정 내에 정의된 요청 주체(사람 또는 애플리케이션)를 의미한다


 <p>IAM 사용자</p> <ul style="list-style-type: none">• 실 사용자 기준으로 통제할 때 <p>IAM 사용자(<u>상시</u> 자격증명)으로 인증 주로 IAM Group으로 관리</p>	 <p>IAM 역할</p> <ul style="list-style-type: none">• 자동화된 프로세스에서• AWS 서비스들에서• 인증 연계된 외부 사용자들이 <p>IAM 역할은 <u>임시</u> 자격증명으로 인증</p>
--	--

— IAM User Group

- IAM User Group은 보안 주체가 아니며, IAM 권한을 한꺼번에 주기 위한 용도
- 그룹 간 포함(Nested) 관계는 불가
- 자동 소속되는 기본 그룹은 없음
- IAM 사용자는 복수개의 그룹에 속할 수 있음(최대 10개까지, Hard Limit)

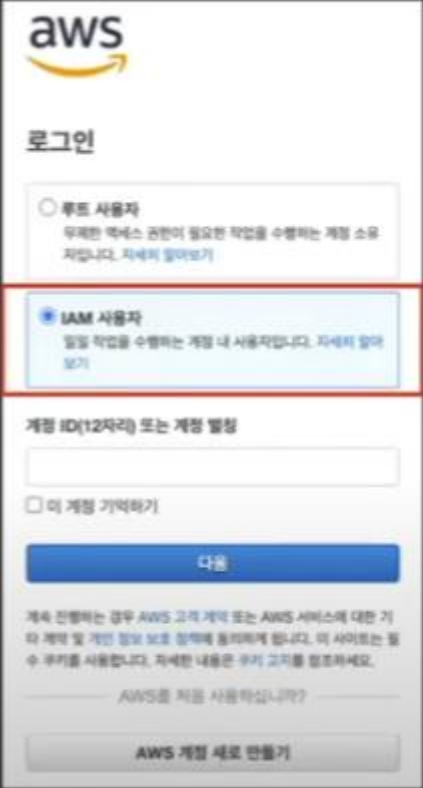


- IAM 사용자 유형



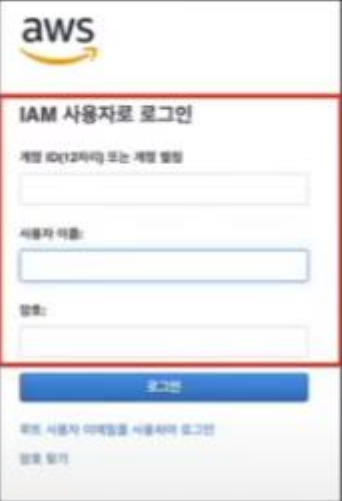
The image shows the AWS Root User Sign In page. It features the AWS logo at the top, followed by the title "Root user sign in". Below this, there are input fields for "Email" (with a placeholder "cc @i nail.net") and "Password". A red rectangular box highlights the "Email" and "Password" fields. At the bottom of the form is a blue "Sign In" button.

Root User



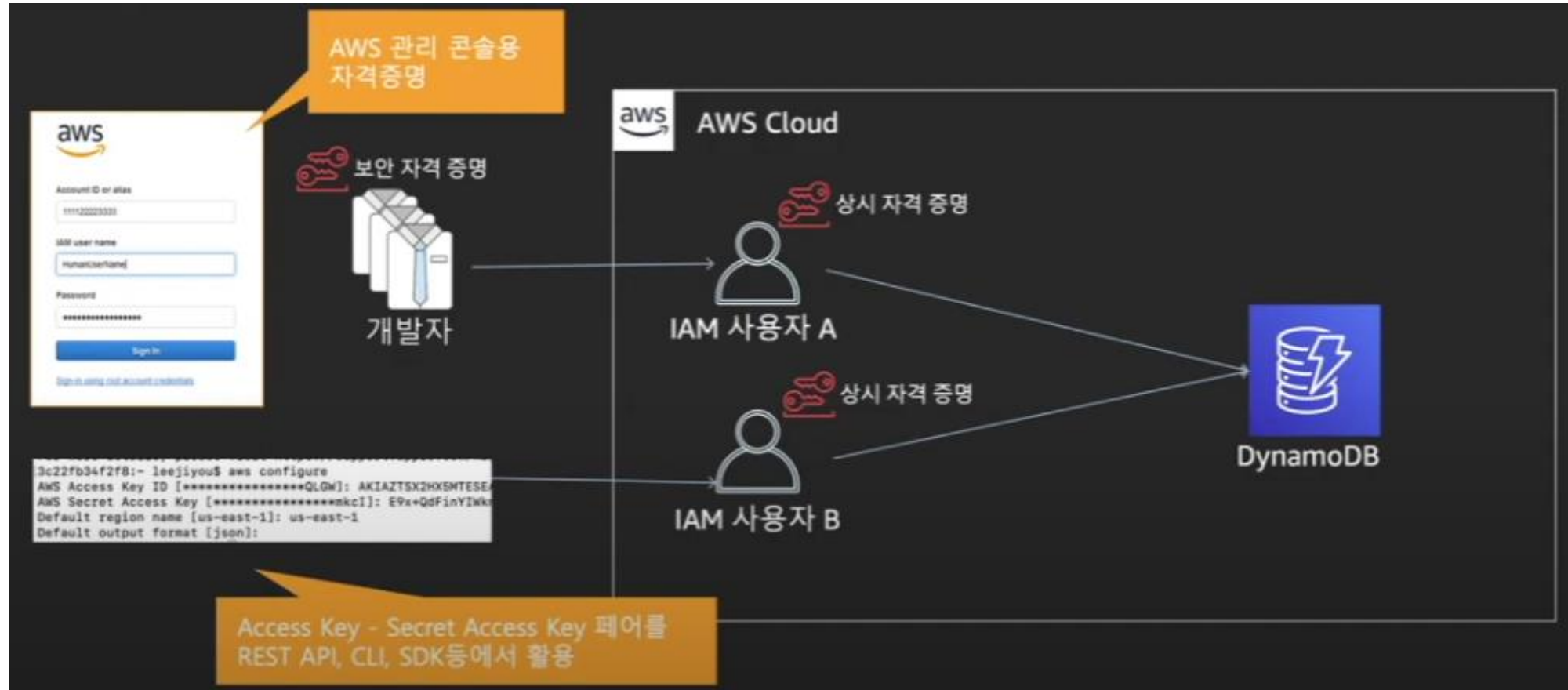
The image shows the AWS IAM User Login page. It features the AWS logo at the top, followed by the title "로그인" (Login). Below this, there are two radio button options: "루트 사용자" (Root User) and "IAM 사용자" (IAM User). The "IAM 사용자" option is selected and highlighted with a red rectangular box. Below the radio buttons, there is a text input field for "계정 ID(12자리) 또는 계정 별칭" (Account ID (12 digits) or Account Alias). A checkbox labeled "이 계정 기억하기" (Remember this account) is also present. At the bottom of the form is a blue "다음" (Next) button.

IAM Users



The image shows the AWS IAM User Login page. It features the AWS logo at the top, followed by the title "IAM 사용자로 로그인" (Log in as IAM user). Below this, there are two text input fields: "계정 ID(12자리) 또는 계정 별칭" (Account ID (12 digits) or Account Alias) and "사용자 이름:" (User name:). A red rectangular box highlights the "계정 ID" field and the "사용자 이름:" field. At the bottom of the form is a blue "로그인" (Login) button.

- IAM 사용자 자격 증명



— AWS Identity

- IAM Principal은 AWS 계정 내에 정의된 요청 주체를 의미한다



IAM 사용자

- 실 사용자 기준으로 통제할 때
IAM 사용자(상시 자격증명)으로 인증
주로 IAM Group으로 관리



IAM 역할

- 자동화된 프로세스에서
• AWS 서비스들에서
• 인증 연계된 외부 사용자들이

IAM 역할은 임시 자격증명으로 인증

IAM Role 생성 메뉴

IAM Role 생성 메뉴

Role for your non-human process

Role for federated (human) identities

2 3 4

Choose the service that will use this role

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

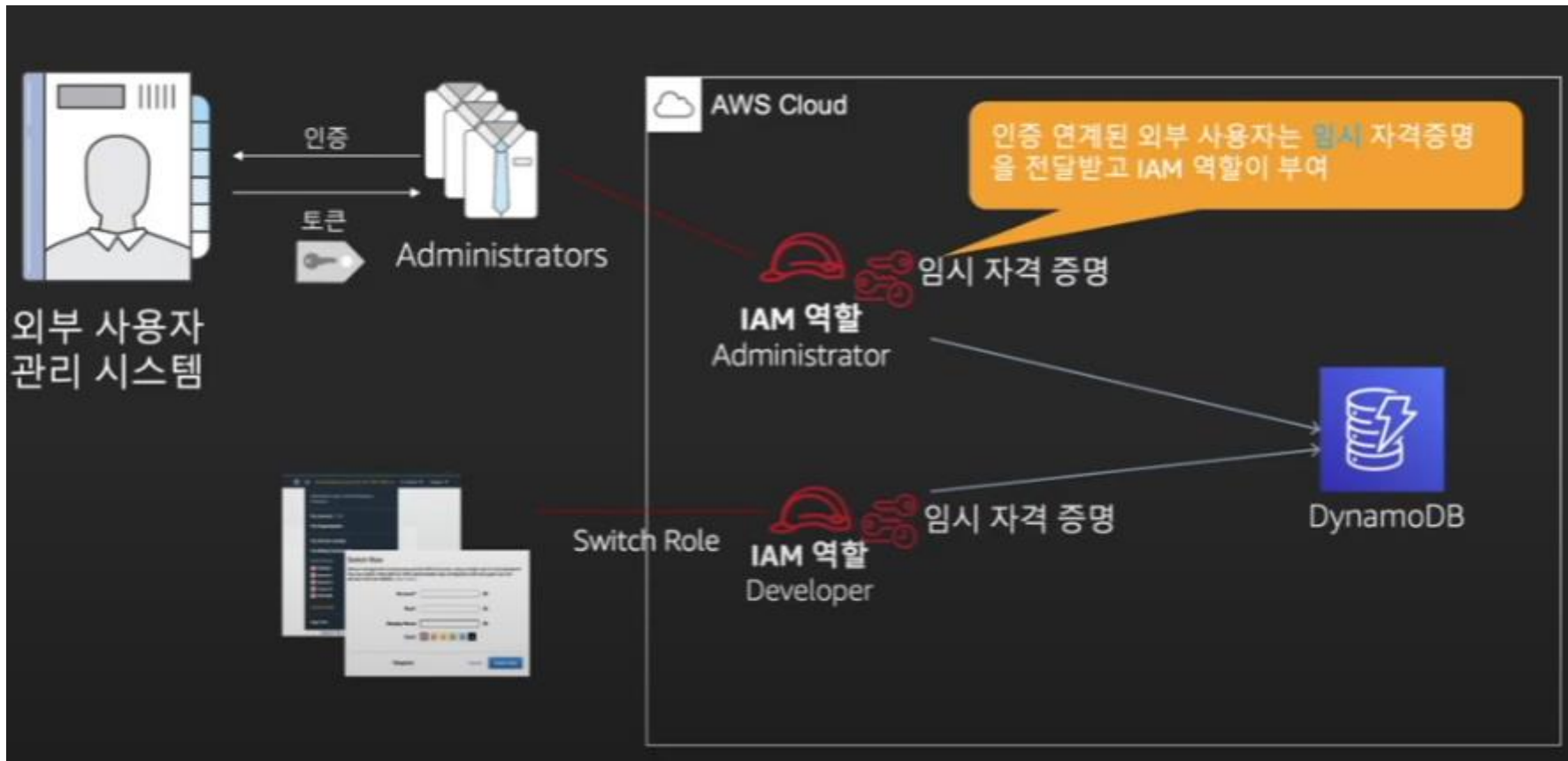
Role for cross-account access

API Gateway	CodeDeploy	EKS	Kinesis	S3
AWS Backup	Comprehend	EMR	Lambda	SMS
AWS Support	Config	ElastiCache	Lex	SNS
Amplify	Connect	Elastic Beanstalk	License Manager	SWF
AppSync	DMS	Elastic Container Service	Machine Learning	SageMaker

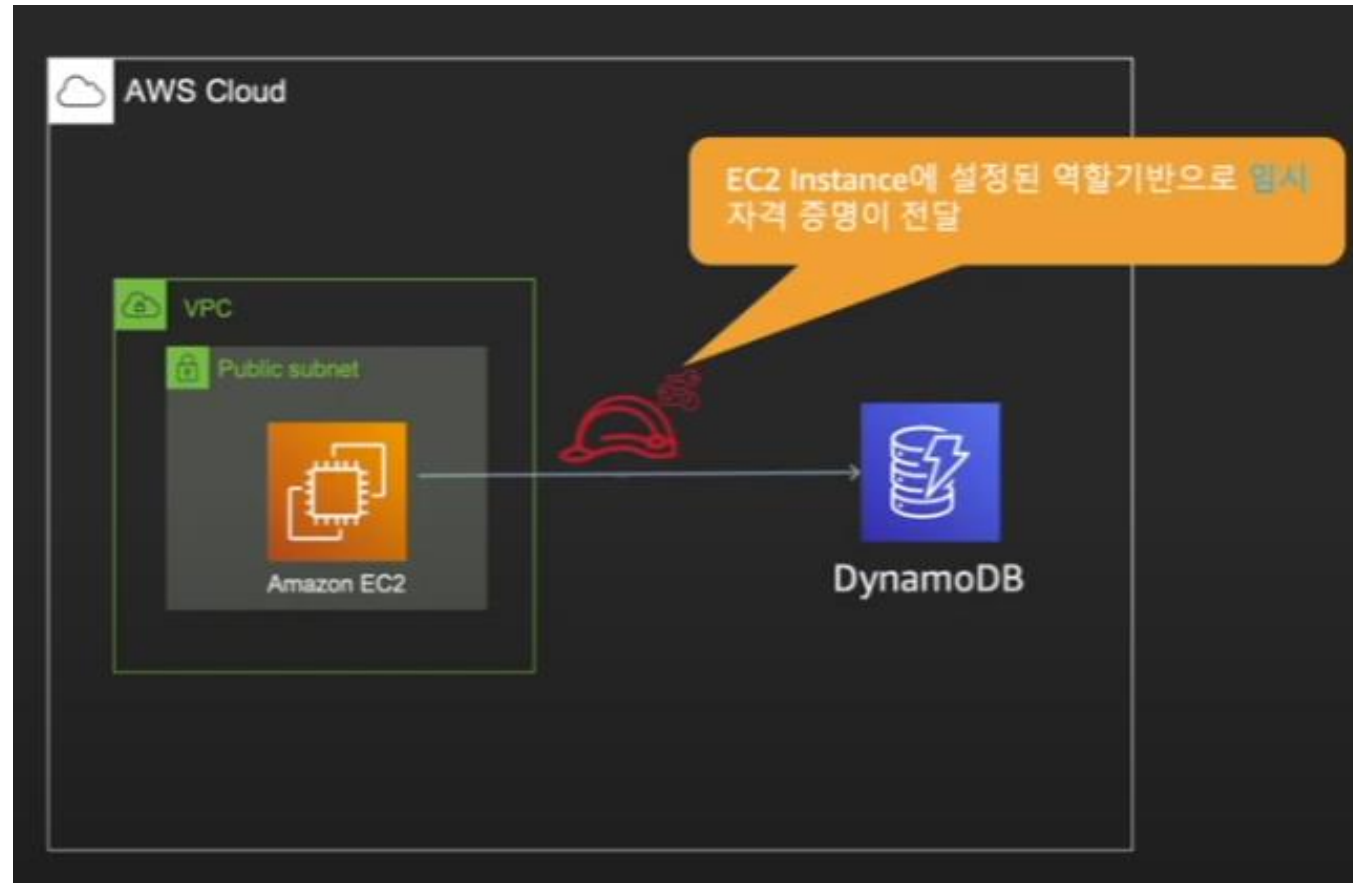
* Required

Cancel Next: Permissions

- IAM Role 자격 증명



— IAM Role 자격 증명



— AWS Access Management

- 모든 AWS 서비스는 접근제어 정책(Policy)을 기반으로 인가됨
- 매 API호출 시, 적용된 정책을 통해 인가 수행
- 정책은 IAM 역할/사용자/그룹, AWS 리소스, 임시 자격증명 세션, OU 등에 적용 가능
- AWS Root 계정은 기본적으로 AWS 리소스에 대한 모든 권한을 가짐
- AWS 정책은 기본 디폴트가 Deny이고, 명시적 Allow < 명시적 Deny의 우선순위



— IAM Policy

- AWS에서 하나의 계정을 관리하려면 정책을 사용하여 해당 계정 내 권한을 정의한다
- IAM 사용자를 생성할 경우, 권한을 부여하지 않는 한 사용자는 계정 내에서 어떠한 것으로도 액세스할 수 없다
- 사용자가 또는 사용자가 속한 그룹에 연결된 정책인 자격 증명 기반 정책을 생성해서 사용자에게 권한을 부여해야 함

— IAM Policy 구성요소

```
{
  "Statement": [{
    "Effect": "Allow or Deny",
    "Principal": "principal",
    "Action": "action",
    "Resource": "arn",
    "Condition": {
      "condition": {
        "key": "value"
      }
    }
  ]
}
```

Effect – 명시된 정책에 대한 허용 혹은 차단

Principal – 접근을 허용 혹은 차단하고자 하는 대상

"Principal": "AWS": "arn:aws:iam::123456789012:user/username"

Action – 허용 혹은 차단하고자하는 접근 타입

"Action": "s3:GetObject"

Resource – 요청의 목적지가 되는 서비스

"Resource": "arn:aws:sqs:us-west-2:123456789012:queue1"

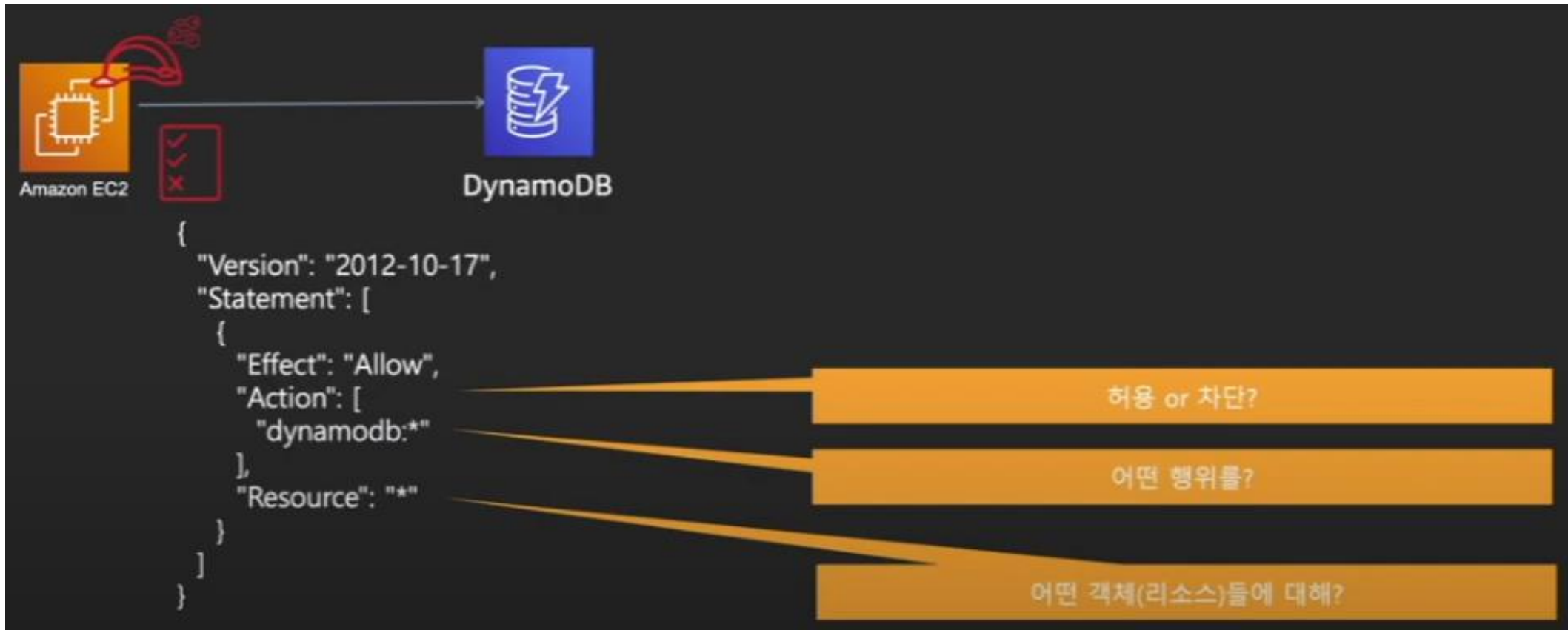
Condition – 명시된 조건 유효하다고 판단될 수 있는 조건

"StringEqualsIfExists": {"aws:RequestTag/project": ["Pickles"]}

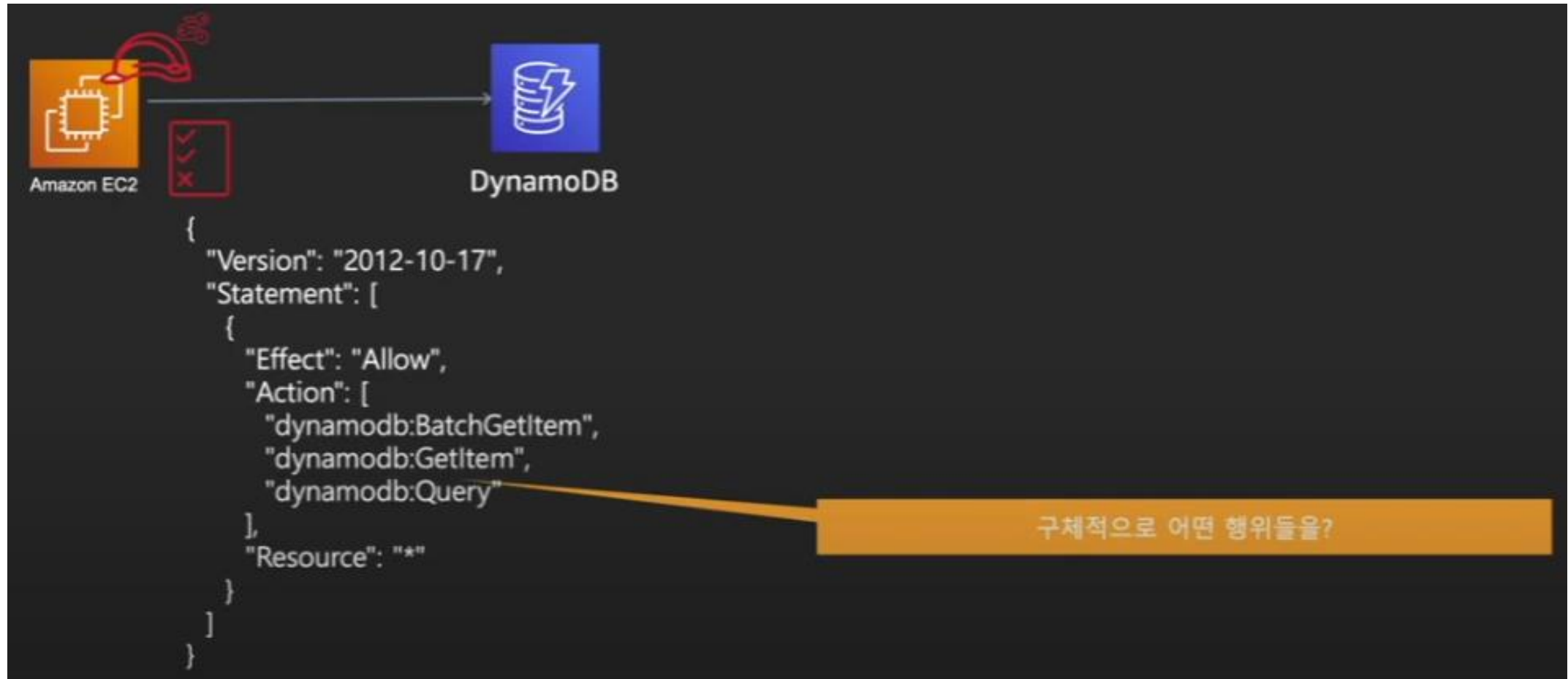
— IAM 요청의 성공 조건

- IAM 보안 주체의 적법한 서명값이 포함되어 있고(인증)
- 정책(Policy)에 의해 해당 요청이 정확하게 인가되어야 함

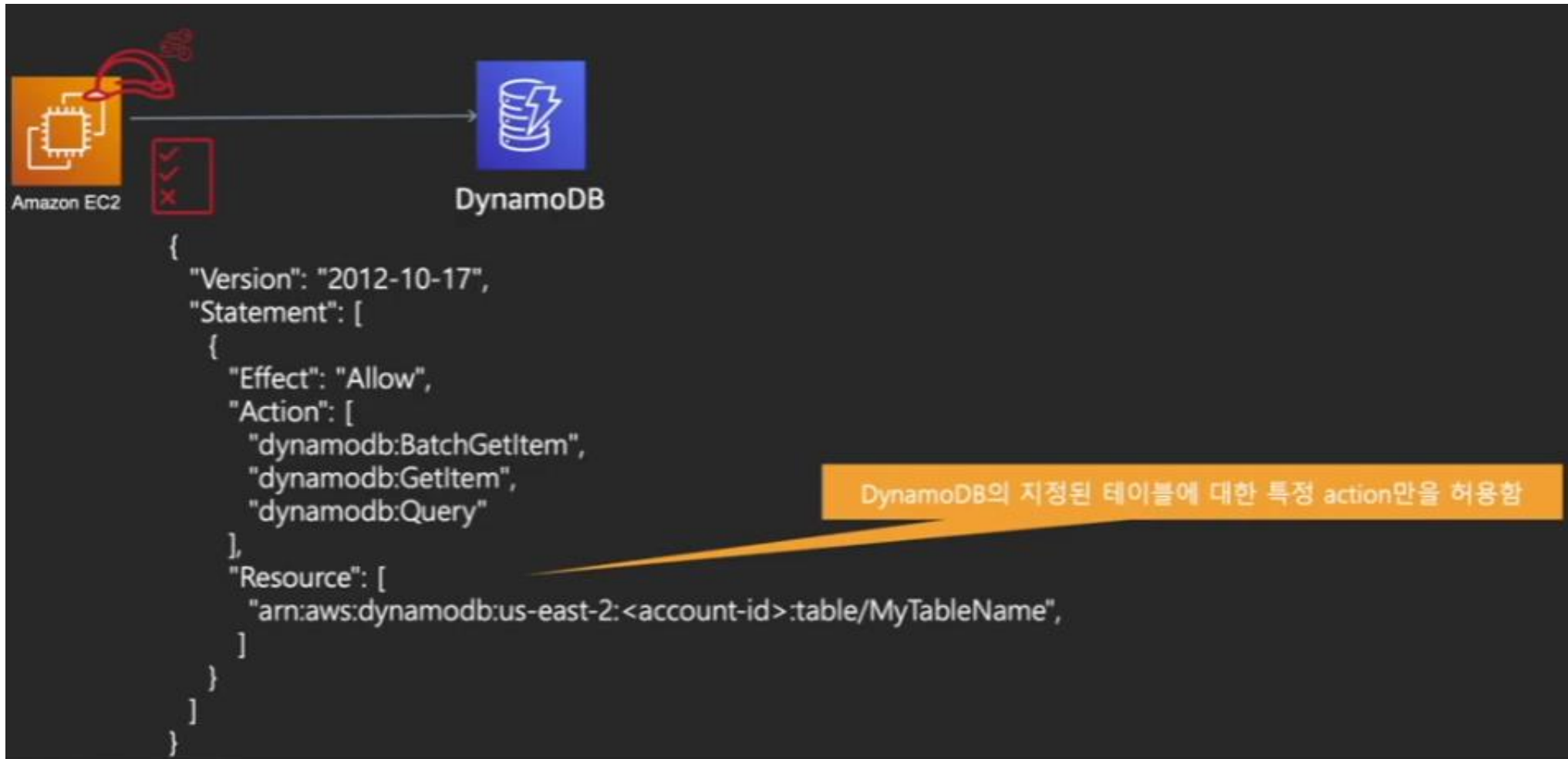
- DynamoDB로 부터 데이터 읽기



– DynamoDB로 부터 데이터 읽기



– DynamoDB로 부터 데이터 읽기



— AWS 정책의 분류



Identity-Based 정책과 Resource-Based 정책 비교

- IAM 보안주체에 할당되어 해당 주체의 권한을 규정
- IAM 사용자, 그룹, 역할

Identity-based 정책

```
{
  "Statement": [{
    "Effect": "effect",
    "Action": "action",
    "Resource": "arn",
    "Condition": {
      "condition": {
        "key": "value"
      }
    }
  }]
}
```

Action
Resource
Condition

Resource-based 정책

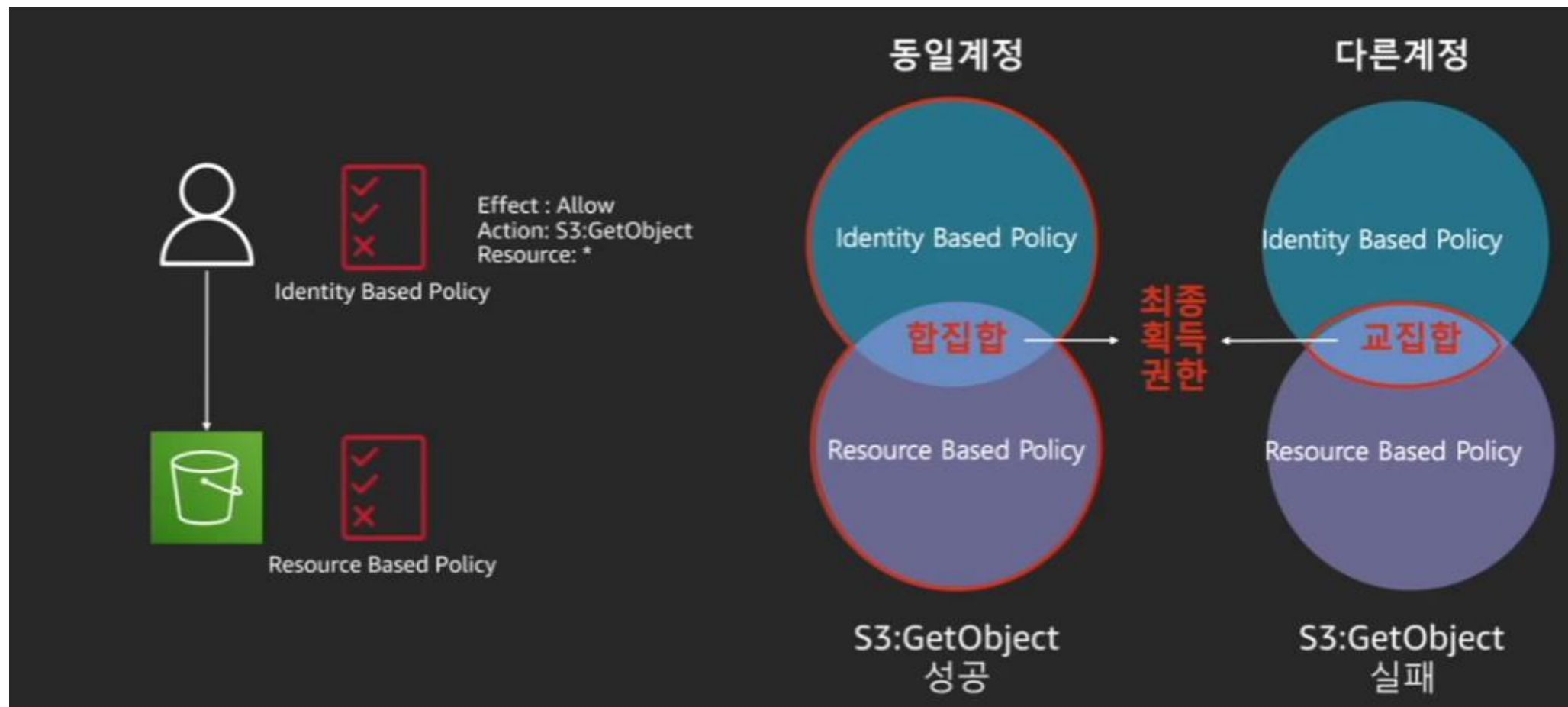
```
{
  "Statement": [{
    "Effect": "effect",
    "Principal": "principal",
    "Action": "action",
    "Resource": "arn",
    "Condition": {
      "condition": {
        "key": "value"
      }
    }
  }]
}
```

Principal
Action
Resource
Condition

- 지정된 보안 주체 (Principal)가 해당 리소스에 대해 수행할 수 있는 작업 및 이에 관한 조건을 규정
- Amazon S3 버킷, Amazon SQS 대기열 및 AWS Key Management Service 암호화 키 등

필수

Identity-Based 정책과 Resource-Based 정책 예시



- 다른 계정의 경우 정책 설정

다른 계정의 경우 정책 설정



```
"Effect": "Allow",  
"Action": "s3:GetObject",  
"Resource": "arn:aws:s3:::AccountABucket/*"
```

```
"Effect": "Allow",  
"Principal": {  
  "AWS": "arn:aws:iam::AccountB:user/AccountBUser"  
},  
"Action": "s3:GetObject",  
"Resource": [  
  "arn:aws:s3:::AccountABucket/*"  
]
```

다른계정

Identity Based Policy

교집합

Resource Based Policy

S3:GetObject
성공

— Deny 정책 예시



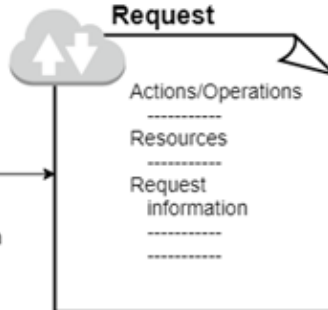


Account ID 123456789012

Principal



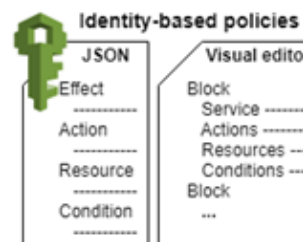
Request



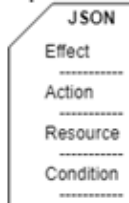
Authentication



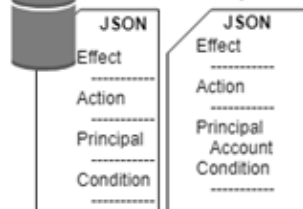
Authorization



Other policies



Resource-based policies



Actions (Console) or Operations (API/CLI)



Resources



Account ID 012345012345



Account ID 112233445566



— AWS IAM 모범 사례

1. AWS 계정 루트 사용자 액세스 키 잠금
2. 개별 IAM 사용자 생성
3. 자격 증명을 정기적으로 교체
4. 액세스 키를 공유하지 마십시오
5. 불필요한 자격 증명 삭제
6. 강력한 비밀번호 정책
7. 권한 있는 사용자에게 대해 MFA 활성화
8. 그룹을 사용한 권한 관리

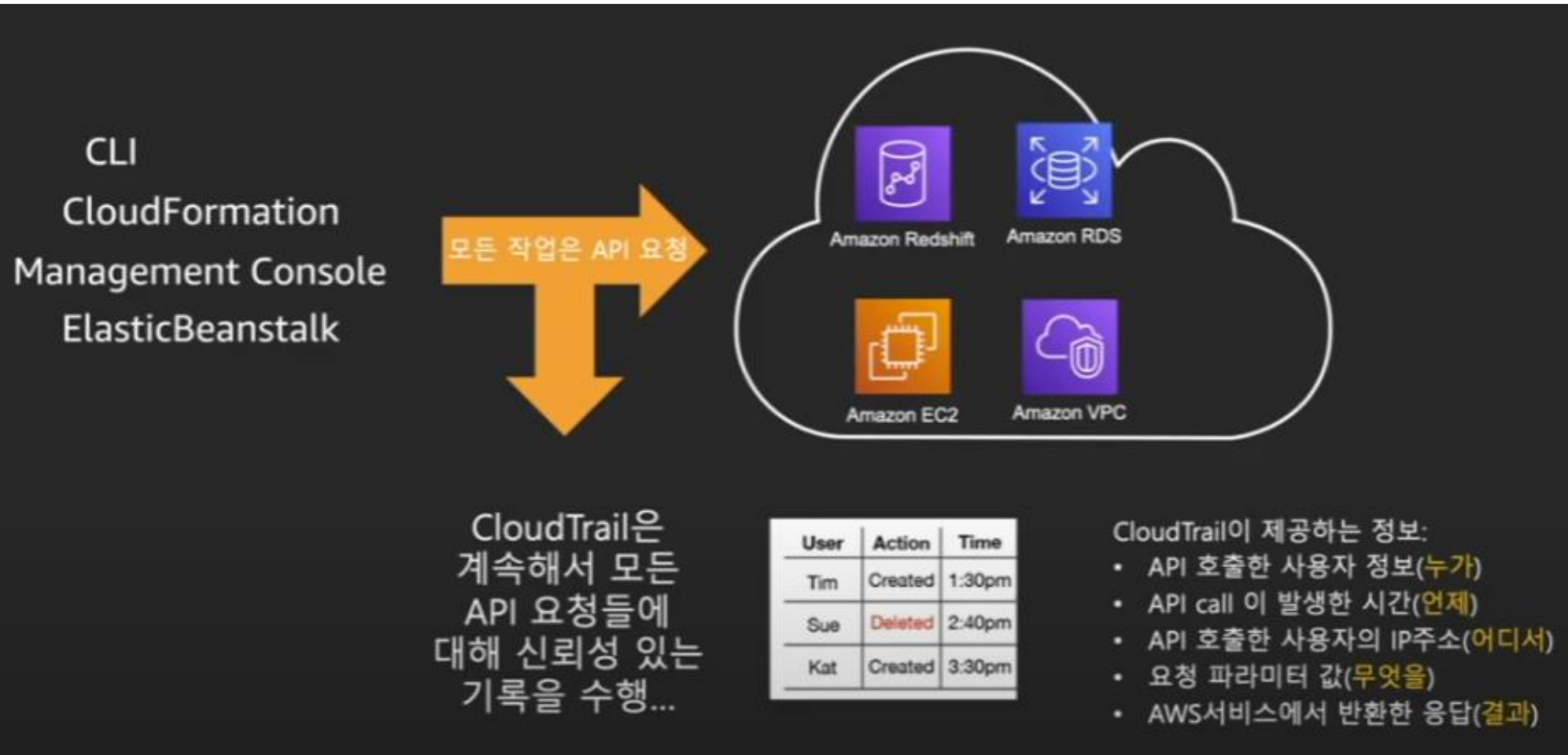
9. 최소 권한 부여
10. AWS 관리형 정책으로 권한 사용 시작
11. 인라인 정책 대신 고객 관리형 정책 사용
12. 조건(Condition) 사용
13. 인스턴스에서 실행되는 애플리케이션에 역할 사용
14. 역할을 사용하여 권한 위임
15. AWS 계정의 활동 모니터링
16. 액세스 레벨을 이용한 IAM 권한 검토

AWS CloudTrail

— AWS CloudTrail

- AWS CloudTrail은 AWS 계정의 운영 및 위험 감사, 거버넌스 및 규정 준수를 지원하는 AWS 서비스
- 사용자, 역할 또는 AWS 서비스가 수행한 작업은 CloudTrail에 이벤트로 기록
- 이벤트에는 AWS Management Console, AWS Command Line Interface, AWS SDK 및 API에서 수행된 작업이 포함된다.

— AWS CloudTrail



— AWS CloudTrail



AWS CloudTrail

- 사용자 및 리소스 활동에 대한 가시성
 - AWS 관리 콘솔 작업 및 API 호출을 기록
- Amazon CloudWatch Logs와의 통합
 - 간편하게 로그 데이터를 수집 및 검색
- 규정 준수 간소화
 - 이벤트 로그를 자동으로 기록하고 저장
 - CloudWatch Events와 통합하여 알람 설정

CloudTrail 로그 샘플

• Who

• When

• What

• Where

• Which

```
{
  "eventVersion": "1.01",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJDPLRKL7UEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-03-18T14:29:23Z"
      }
    }
  },
  "eventTime": "2020-03-18T14:30:07Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "StartLogging",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "72.21.198.64",
  "userAgent": "AWSConsole, aws-sdk-java/1.4.5 Linux/x.xx.fleetxen Java_HotSpot(TM)_64-Bit_Server_VM/xx",
  "requestParameters": {
    "name": "Default"
  },
  ...
}
```

— CloudTrail 추적

- 로그를 파일 형태로 지정된 S3버킷 또는 CloudWatch Log Group에 전달하는 설정
- API 호출 후 15분 정도 소요, 5분마다 파일 생성, SNS 알림 설정
- 단일 리전 또는 글로벌 전체에 설정
- AWS KMS 관리형 키를 사용한 서버 측 암호화
- 로그 파일 무결성 활성화 가능

— CloudTrail 이벤트의 종류

- 관리 이벤트

EC2 상에서 업데이트, 삭제 등과 같은 리소스 통제 행위
거의 모든 AWS 서비스를 지원(130+)

- 데이터 이벤트

S3의 단일 객체에 대한 읽기와 같은 상세 레벨의 행위
관리 이벤트에 비해 굉장히 많은 빈도
S3와 Lambda에 대해 지원

- Insight 이벤트

Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#) [↗](#)

Event type

Choose the type of events that you want to log.

☒ Management events

Capture management operations performed on your AWS resources.

☐ Data events

Log the resource operations performed on or within a resource.

☐ Insights events

Identify unusual activity, errors, or user behavior in your account.

AWS CloudWatch

— CloudWatch



AWS 클라우드 리소스와
온프레미스 상의
애플리케이션에 대한
모니터링



Collect

로그 저장
매트릭



Monitor

Dashboard
중앙모니터링



Act

규칙 기반 경보/대응



Analyze

분석 및 원인파악

— CloudWatch Logs

- 로그 보존 기간
 - **Never Expire**(디폴트)
 - 보존 기간 설정 – 지나면 자동 삭제
- 로그 암호화
 - **KMS 기반** 암호화 지원 – 로그 그룹 별 CMK 지정
 - CMK 분실 시, 접근 불가
- 로그 연계
 - S3로 로그 데이터 덤프 지원 : 실시간 아님
 - Subscription을 이용한 실시간 Stream 연계 : Elastic Search로 바로 연계하거나, Lambda로 Kinesis Stream, Kinesis Data Firehorse 등을 활용하여 기타 환경과 실시간 연계

경보 체계 구성

경보 체계 구성

중요 API 활동에 대한 통보 체계



CloudWatch Alarm

The screenshot displays the AWS CloudWatch Alarm configuration interface. It is divided into two main sections: 'Event selector' and 'Targets'.

Event selector: This section is used to build a pattern that selects events for processing. It shows 'AWS API call' as the event type. Under 'Service name', 'CloudTrail' is selected. The 'Any operation' radio button is unselected, and the 'Specific operation(s)' radio button is selected. A list of specific operations is shown, with 'StopLogging' selected and highlighted by an orange callout.

Targets: This section is used to select the targets to receive the events that match the rule. It shows 'Lambda function' as the target type. Under 'Function', 'RevertCloudTrailOff' is selected and highlighted by an orange callout. Below this, there is a 'Configure input' link and an 'Add target' button.

Annotations:

- An orange callout points to the 'StopLogging' event, with the text: 'CloudTrail에서 StopLogging 이벤트가 발생 하는 경우를 알람 설정' (Set alarm when StopLogging event occurs in CloudTrail).
- An orange callout points to the 'RevertCloudTrailOff' function, with the text: 'Detect malicious API and automate response. If trail.delete { trail.enable & email.security_team}' (Detect malicious API and automate response. If trail.delete { trail.enable & email.security_team}).