

IAM 역할, 정책 세팅

☰ Tags	2020 DT 교육
▼ 상태	완료
📅 시작	@Sep 2, 2020
📅 종료	@Sep 2, 2020

개념

- 역할(Role): 사용자, 서비스에 부여하는 업무적인 역할
 - 사용자나 서비스에 여러개의 역할을 부여할 수 있음
- 정책(Policy): 역할에 부여되는 권한
 - 역할에 여러개의 정책을 부여할 수 있음

CodeBuild 역할 생성

1. IAM 에서 역할 만들기 버튼 클릭

Identity and Access Management(IAM)

대시보드

▼ 액세스 관리

그룹

사용자

역할

정책

자격 증명 공급자

계정 설정

▼ 보고서 액세스

액세스 분석기

아카이브 규칙

분석기

설정

자격 증명 보고서

역할

IAM 역할이란 무엇입니까?

IAM 역할은 신뢰하는 개체에 권한을 부여하는 방법입니다.

- 다른 계정의 IAM 사용자
- AWS 리소스에서 작업을 수행해야 하는
- 계정 내 리소스에서 작업을 수행하여 기
- SAML을 통해 인증 연동을 사용하는 사

IAM 역할은 권한을 부여하는 더욱 안전한 방법입니다.

추가 리소스:

- IAM 역할 FAQ
- IAM 역할 설명서
- 자습서: AWS 계정 간 액세스 권한 위임
- 역할에 대한 일반적인 시나리오

역할 만들기

역할 삭제

2. AWS 서비스 > CodeBuild 선택 후 다음 버튼 클릭

CloudFormation	EC2	IAM Access Analyzer	Purchase Orders	Transfer
CloudHSM	EC2 - Fleet	Inspector	QLDB	Trusted Advisor
CloudTrail	EC2 Auto Scaling	IoT	RAM	VPC
CloudWatch Application Insights	EC2 Image Builder	IoT SiteWise	RDS	WorkLink
CloudWatch Events	EKS	IoT Things Graph	Redshift	WorkMail
CodeBuild				

사용 사례 선택

CodeBuild

Allows CodeBuild to call AWS services on your behalf.

* 필수

취소

다음: 권한

3. 기존의 권한 정책들을 선택을 해도 되고 안해도 됨

4. 태그 추가는 안할것이니 다음 버튼 클릭

5. 이름과 설명 추가 후 생성

역할 만들기

1 2 3 4

검토

생성하기 전에 아래에 필요한 정보를 입력하고 이 역할을 검토하십시오.

역할 이름*	<input type="text" value="CodeBuildForEveryone"/>
<small>영숫자 및 '+', '@', '-' 문자를 사용합니다. 최대 64자입니다.</small>	
역할 설명	<input type="text" value="CodeBuild Role for ECR, EKS deployment"/>
<small>최대 1000자입니다. 영숫자 및 '+', '@', '-' 문자를 사용합니다.</small>	

6. 검색을 하여 생성되었는지 확인

역할 이름 ▼

☐ CodeBuildForEveryone

CodeBuild 정책 생성

1. 정책 생성 클릭





Identity and Access Management(IAM)

- 대시보드
- ▼ 액세스 관리
 - 그룹
 - 사용자
 - 역할
 - 정책

정책 생성

정책 필터 ▾

정책

- ☐ ▶  A
- ☐ ▶  A
- ☐ ▶  A
- ☐ ▶  A

2. 시각적 편집기에서 선택하여 생성해도 되나, JSON으로 생성하겠음

정책 생성

정책은 사용자, 그룹, 또는 역할에 할당할 수 있는 AWS 권한

시각적 편집기

JSON

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": []  
4 }
```

3. Statement 안에 리소스 별 권한을 입력

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Resource": [  
        "arn:aws:logs:ap-northeast-2:052937454741:log-group:/aws/codebuild/"
```

```

],
  "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ]
},
{
  "Effect": "Allow",
  "Resource": [
    "arn:aws:s3:::codepipeline-ap-northeast-2-"
  ],
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "codebuild:CreateReportGroup",
    "codebuild:CreateReport",
    "codebuild:UpdateReport",
    "codebuild:BatchPutTestCases",
    "codebuild:BatchPutCodeCoverages"
  ],
  "Resource": [
    "arn:aws:codebuild:ap-northeast-2:052937454741:report-group/"
  ]
},
{
  "Action": [
    "ecr:BatchCheckLayerAvailability",
    "ecr:CompleteLayerUpload",
    "ecr:GetAuthorizationToken",

```

```

    "ecr:InitiateLayerUpload",
    "ecr:PutImage",
    "ecr:UploadLayerPart",
    "eks:DescribeCluster"
  ],
  "Resource": "",
  "Effect": "Allow"
}
]
}

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:logs:ap-northeast-2:052937454741:log-group:/aws/codebuild/"
      ],
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    },
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::codepipeline-ap-northeast-2-"
      ],
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ]
    }
  ]
}

```

```

"Effect": "Allow",
"Action": [
"codebuild:CreateReportGroup",
"codebuild:CreateReport",
"codebuild:UpdateReport",
"codebuild:BatchPutTestCases",
"codebuild:BatchPutCodeCoverages"
],
"Resource": [
"arn:aws:codebuild:ap-northeast-2:052937454741:report-group/"
]
},
{
"Action": [
"ecr:BatchCheckLayerAvailability",
"ecr:CompleteLayerUpload",
"ecr:GetAuthorizationToken",
"ecr:InitiateLayerUpload",
"ecr:PutImage",
"ecr:UploadLayerPart",
"eks:DescribeCluster"
],
"Resource": "*",
"Effect": "Allow"
}
]
}

```

- Resource에 권한을 부여할 AWS 자원의 ARN(Amazon Resource Name), Action에는 해당 자원에서 호출을 허용할 AWS API를 입력
- 마지막에 ECR과 EKS에 대한 권한이 부여되어 있음
- 정책 검토 버튼 클릭

4. 정책 이름, 설명 입력 후 원하는 서비스의 권한이 부여되었는지 요약 내역 확인

정책 검토

이름*

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

설명

최대 1000자입니다. 영숫자 및 '*=, @ _.' 문자를 사용합니다.

요약

Q 필터:

서비스 ▼	액세스 레벨	리소스	요청 조건
허용 (5 / 238 서비스) 나머지 233 표시			
CloudWatch Logs	제한: 쓰기	LogGroupName string like /aws/codebuild/*	없음
CodeBuild	제한: 쓰기	arn:aws:codebuild:ap-northeast-2:052937454741:report-group/*	없음
EKS	제한: 읽기	모든 리소스	없음
Elastic Container Registry	제한: 읽기, 쓰기	모든 리소스	없음
S3	제한: 읽기, 쓰기	BucketName string like codepipeline-ap-northeast-2-*	없음

* 필수

취소 이전 **정책 생성**

5. 생성 확인

Identity and Access Management(IAM)

대시보드

▼ 액세스 관리

그룹

사용자

✔ **CodeBuildPolicyForEveryone** 이(가) 생성되었습니다.

정책 생성 정책 작업 ▼

정책 필터 ▼

역할에 정책 연결

1. 검색창에 생성한 역할 이름을 입력하고 클릭

Identity and Access Management(IAM)

대시보드

▼ 액세스 관리

그룹

사용자

역할

정책

자격 증명 공급자

계정 연결

역할 만들기

역할 삭제

CodeBuildFor

역할 이름 ▼

☐

CodeBuildForEveryone

2. 권한 탭에서 정책 연결 클릭

권한

신뢰 관계

태그

액세스 관리자

세션 취소

▼ Permissions policies



권한 시작하기

이 역할은(는) 아직 권한이 없습니다. 이 역할에 정책을 1개 이상

정책 연결

3. 앞서 생성한 연결할 정책을 검색하여 체크한 후 정책 연결 버튼 클릭

CodeBuildForEveryone에 권한 추가

권한 연결

정책 생성 ↺

정책 필터 2 결과 표시

	정책 이름	유형	사용 용도
<input checked="" type="checkbox"/>	CodeBuildPolicyForEveryone	고객 관리형	없음
<input type="checkbox"/>	CodeBuildPolicyForTeamE	고객 관리형	Permissions policy (1)

취소 정책 연결

4. 연결된 정책 확인

역할 > CodeBuildForEveryone

요약

정책 CodeBuildPolicyForEveryone이 CodeBuildForEveryone에 대해 연결되었습니다.

역할 ARN `arn:aws:iam::052937454741:role/CodeBuildForEveryone` [🔗](#)
 역할 설명 CodeBuild Role for ECR, EKS deployment | [편집](#)
 인스턴스 프로파일 ARN [🔗](#)
 경로 /
 생성 시간 2020-09-02 10:32 UTC+0900
 마지막 활동 추적 기간에 액세스되지 않음
 최대 세션 지속 시간 1 시간 [편집](#)

권한 신뢰 관계 태그 액세스 관리자 세션 취소

▼ Permissions policies (1 정책이 적용됨)

정책 연결

정책 이름	정책 유형
CodeBuildPolicyForEveryone	관리형 정책

서비스에 역할 연결

1. CodeBuild 생성 또는 환경 편집으로 역할 선택 가능

환경				편집
이미지 aws/codebuild/standard:4.0	환경 유형 Linux	컴퓨팅 3GB 메모리, vCPU 2개	권한이 있음 True	
서비스 역할 arn:aws:iam::052937454741:role/ CodeBuildServiceRoleForTeamE	제한 시간 1시간 0분	대기 중인 제한 시간 8시간 0분	인증서 -	

2. X를 눌러 기존 서비스 역할을 삭제하고 dropdown list에서 앞서 생성한 역할을 클릭

환경

현재 환경 이미지

aws/codebuild/standard:4.0

이미지 재정의

서비스 역할

계정에서 기존 서비스 역할 선택

Q

codebuild-gateway-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-gateway-service-role

codebuild-hospitalmanage-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-hospitalmanage-service-role

codebuild-mypage-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-mypage-service-role

codebuild-r-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-r-service-role

codebuild-screeningmanage-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-screeningmanage-service-role

codebuild-TeamE-bookinglist-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-TeamE-bookinglist-service-role

codebuild-TeamE-gateway-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-TeamE-gateway-service-role

codebuild-TeamE-notification-service-role
arn:aws:iam::052937454741:role/service-role/codebuild-TeamE-notification-service-role

CodeBuildForEveryone
arn:aws:iam::052937454741:role/CodeBuildForEveryone

CodeBuildServiceRoleForTeamE
arn:aws:iam::052937454741:role/CodeBuildServiceRoleForTeamE

3. 체크박스 해제 후, 환경 업데이트 버튼 클릭

개발자 도구 > CodeBuild > 빌드 프로젝트 > TeamE-booking > 환경 편집

환경 편집

환경

현재 환경 이미지
aws/codebuild/standard:4.0

이미지 재정의

서비스 역할
계정에서 기존 서비스 역할 선택

arn:aws:iam::052937454741:role/CodeBuildForEveryone

☐ 이 서비스 역할을 이 빌드 프로젝트에 사용할 수 있도록 AWS CodeBuild에서 수정하도록 허용

▶ 추가 구성
제한 시간, 인증서, VPC, 컴퓨팅 유형, 환경 변수, 파일 시스템

취소 환경 업데이트

4. 변경된 역할 확인

Success

빌드 프로젝트 TeamE-booking의 환경이 업데이트되었습니다.

환경

이미지	환경 유형
aws/codebuild/standard:4.0	Linux
서비스 역할	제한 시간
arn:aws:iam::052937454741:role/CodeBuildForEveryone	1시간 0분
레지스트리 자격 증명	