<u>≔</u> Tags	2020 DT 교육
☑ 상태	완료
를 시작	@Sep 2, 2020
를 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 부여?

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

IAM 역할은 권한을 부여하는 더욱 안전한

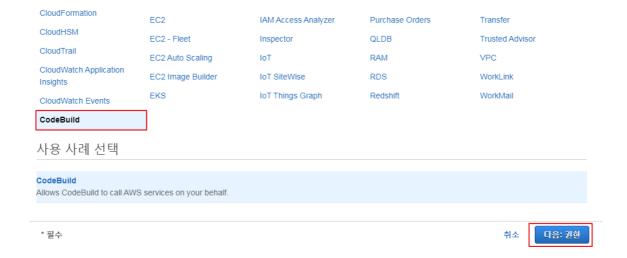
#### 추가 리소스:

- 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



- 3. 기존의 권한 정책들을 선택을 해도 되고 안해도 됨
- 4. 태그 추가는 안할것이니 다음 버튼 클릭

### 5. 이름과 설명 추가 후 생성



#### 6. 검색을 하여 생성되었는지 확인



# CodeBuild 정책 생성

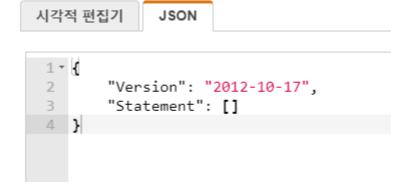
1. 정책 생성 클릭



2. 시각적 편집기에서 선택하여 생성해도 되나, JSON으로 생성하겠음

# 정책 생성

정책은 사용자, 그룹, 또는 역할에 할당할 수 있는 AWS 권한·



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/"
```

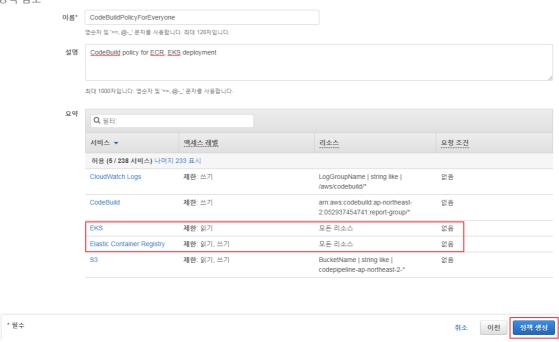
```
],
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:PutLogEvents"
},
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::codepipeline-ap-northeast-2-"
],
"Action": [
"s3:PutObject",
"s3:GetObject",
"s3:GetObjectVersion",
"s3:GetBucketAcl",
"s3:GetBucketLocation"
]
},
"Effect": "Allow",
"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"
1
}
"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

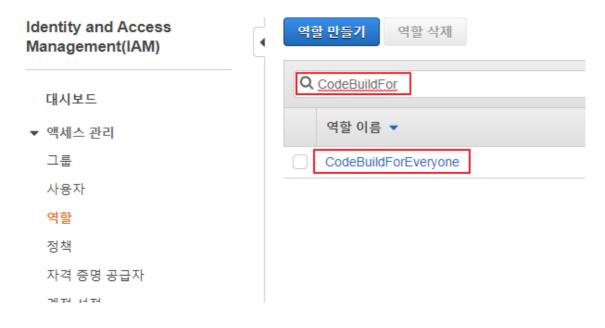


### 5. 생성 확인

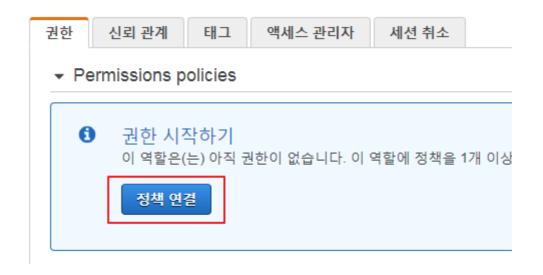


# 역할에 정책 연결

1. 검색창에 생성한 역할 이름을 입력하고 클릭



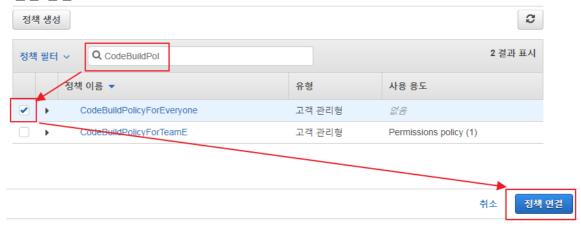
2. 권한 탭에서 정책 연결 클릭



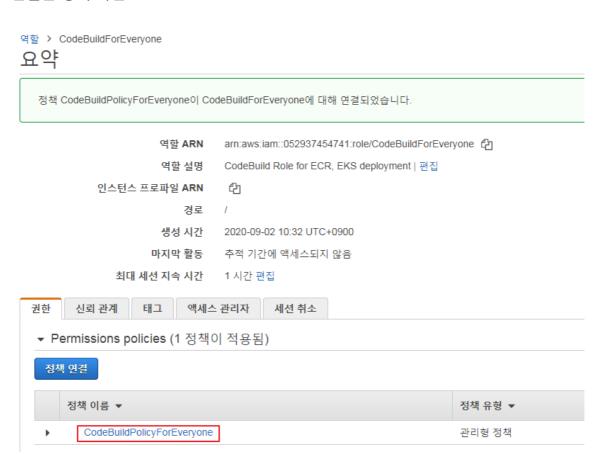
3. 앞서 생성한 연결할 정책을 검색하여 체크한 후 정책 연결 버튼 클릭

## CodeBuildForEveryone에 권한 추가

#### 권한 연결



#### 4. 연결된 정책 확인

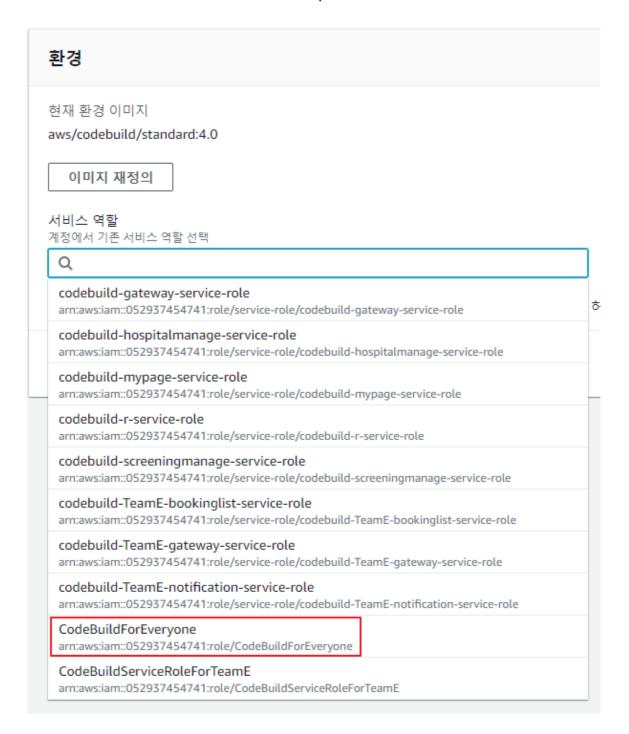


### 서비스에 역할 연결

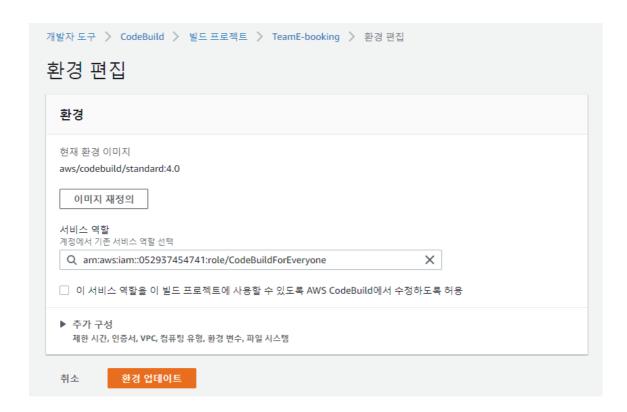
1. CodeBuild 생성 또는 환경 편집으로 역할 선택 가능



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



### 3. 체크박스 해제 후, 환경 업데이트 버튼 클릭



#### 4. 변경된 역할 확인

