



AWS기반 리눅스 서버 구축

AWS 기초 강의

● 박 예 원

Digital learning Team

Cloud Developer

목차

- 1 IAM
- 2 리눅스(Linux)
- 3 EC2
- 4 클라우드 네트워크 세팅
- 5 AWS Storage (S3)

IAM (Identity and Access Management)



- **AWS 서비스 및 리소스에 대한 액세스 관리**
- **AWS 사용자 및 그룹 단위로 액세스 권한 관리**

IAM (Identity and Access Management)

- **AWS Account / Resource / User / Service 권한 제어**
 - 서비스 사용을 위한 인증 정보 부여
- **사용자 생성 및 계정 보안 관리**
 - 서비스 사용을 위한 인증 정보 부여

글로벌 서비스

IAM 구성

- **Policy / 정책**
 - 권한을 정의하는 AWS 객체
 - Json 형식으로 정의
- AWS 제공 정책 (AWS 관리형)
- Custom 정책 (고객 관리형)

The screenshot displays two AWS IAM policies in the console. The top policy, **AmazonEC2RoleforDataPipelineRole**, is a managed policy with the description "Default policy for the Amazon EC2 Role for Data Pipeline service role." Its JSON content is partially visible, showing a version of "2012-10-17" and a statement with an "Allow" effect. The bottom policy, **Denied-drun_resource**, is a custom policy with the description "Denied-drun_resource". Its JSON content is fully visible, showing a version of "2012-10-17" and two statements. The first statement, "DenyALL", has a "Deny" effect and denies all actions on all resources, with a condition that restricts it to resources with the tag "aws:ResourceTag/drun" set to "alpain". The second statement has an "Allow" effect and allows all EC2 actions on all resources.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
```

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "DenyALL",
6       "Effect": "Deny",
7       "Action": "*",
8       "Resource": "*",
9       "Condition": {
10        "StringEquals": {
11          "aws:ResourceTag/drun": "alpain"
12        }
13      }
14    },
15    {
16      "Effect": "Allow",
17      "Action": "ec2:*",
18      "Resource": "*"
19    }
20  ]
21 }
```

IAM 구성

- **Policy / 정책**

Version : IAM 정책 언어 버전

Id : 정책 식별 ID (opt)

Statement : 권한 정의 영역

Sid : Statement id로써 문장 식별 id (opt)

Effect : 허용/거부 여부

Principal : 정책이 적용될 주체

- User, account, role 등

Action : 허용하거나 거부할 AWS 작업

Resource : 작업이 적용되는 대상의 정보

- ARN으로 표현

```
{  
  "Version": "2012-10-12",  
  "Id": "...",  
  "Statement": [  
    {  
      "Sid": "1",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": ["arn:aws:iam:12345:root"]  
      },  
      "Action": ["s3:GetObject", "s3:PutObject"],  
      "Resource": ["arn:aws:s3::mybucket/"]  
    }  
  ]  
}
```

IAM 구성

- Roles / 역할
 - 사용자나 리소스에 할당
 - 최소 권한 원칙
 - 권한(Policy) 부여
 - 신뢰 관계 부여

aws-elasticbeanstalk-ec2-role 정보

Allows EC2 instances to call AWS services on your behalf.

요약

생성 날짜

April 24, 2024, 11:35 (UTC+09:00)

ARN

arn:aws:iam::
elasticbeans

마지막 활동

1개월 전

최대 세션 지속 시간

1시간

권한

신뢰 관계

태그

액세스 관리자

세션 취소

권한 정책 (3) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

검색

☐

정책 이름

☐

AWSElasticBeanstalkMulticontainerDo...

☐

AWSElasticBeanstalkWebTier

☐

AWSElasticBeanstalkWorkerTier

▶ 권한 경계 (설정되지 않음)

권한

신뢰 관계

태그

액세스 관리자

세션 취소

신뢰할 수 있는 엔터티

지정된 조건에서 이 역할을 수입할 수 있는 엔터티입니다.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": "ec2.amazonaws.com"
8       },
9       "Action": "sts:AssumeRole"
10    }
11  ]
12 }
```

- Root 계정과 최소 권한의 원칙
 - 최초 생성된 계정은 Root 계정
 - Root 계정은 사용자를 생성하는 용도 (공유 금지)
 - 많은 권한은 비용이나 보안 문제를 야기함
 - 필요 이상의 권한은 제공하지 않기

IAM

AWS 액세스 관리

정책(Policy)

권한을 정의하는 AWS 객체

역할(Role)

권한을 임시로 부여 받는 AWS 객체

IAM 관리 원칙

Root 계정 보호 / 최소 권한의 원칙



감사합니다.

Thank You
