

AWS IAM 실습

목차

- IAM로 사용자 및 그룹에 권한 부여
- IAM 계정 ECS 생성 테스트

IAM로 사용자 및 그룹에 권한 부여

사용자 그룹 생성

- 사용자 그룹 생성

사용자 그룹 (1) [정보](#)

사용자 그룹은 IAM 사용자의 컬렉션입니다. 그룹을 사용하여 사용자 컬렉션에 대한 권한을 지정할 수 있습니다.

삭제

그룹 생성

필터 속성 또는 그룹 이름을 기준으로 사용자 그룹을 필터링하고 Enter를 누릅니다.

< 1 >

<input type="checkbox"/>	그룹 이름	사용자	권한	생성 시간
<input type="checkbox"/>	delivery_project_managers	3	로드 중	4시간 전

그룹에 사용자 추가

- 그룹에 사용자 추가

사용자 (4) 정보

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

🔄

삭제

사용자 추가

🔍 사용자 이름 또는 액세스 키로 사용자 찾기





< 1 > ⚙️

<input type="checkbox"/>	사용자 이름	그룹	마지막 활동	MFA	암호 수명
<input type="checkbox"/>	manager_poland	delivery_project_managers	✓ 27분 전	가상	✓ 3시간 전
<input type="checkbox"/>	manager_sona	delivery_project_managers	✓ 18분 전	가상	✓ 3시간 전

그룹에 권한 추가

- 권한 추가를 누르면 정책 연결과 인라인 정책 생성 선택지가 나온다.
- 정책 연결을 누르면 기존에 있던 정책을 끼워넣을 수 있음.
- 인라인 정책 생성을 누르면 해당 그룹 또는 사용자에 게만 사용할 수 있는 정책을 생성할 수 있다.
- 프로젝트에 필요한 모든 기능을 가져와서 정책에 추가. 정책은 최대 10개까지 허용됨.



<input type="checkbox"/>	 AmazonSNSFullAccess	AWS 관리형	Provides full access to Amazon SNS via the AWS Management Con...
<input type="checkbox"/>	 AmazonSQSFullAccess	AWS 관리형	Provides full access to Amazon SQS via the AWS Management Con...
<input type="checkbox"/>	 AmazonVPCFullAccess	AWS 관리형	Provides full access to Amazon VPC via the AWS Management Con...
<input type="checkbox"/>	 AmazonCognitoPowerUser	AWS 관리형	Provides administrative access to existing Amazon Cognito resource...
<input type="checkbox"/>	 AmazonAPIGatewayAdministra...	AWS 관리형	Provides full access to create/edit/delete APIs in Amazon API Gatew...
<input type="checkbox"/>	 AmazonECS_FullAccess	AWS 관리형	Provides administrative access to Amazon ECS resources and enabl...

IAM 계정 ECS 생성 테스트

IAM 계정 ECS 생성 에러 – not authorized

- IAM 계정으로 로그인 하여 ECS 클러스터를 생성하려 했으나, 클러스터만 정상적으로 생성되고, Task definition은 진행되지 않았다.
- IAM 권한 설정 관련 에러가 발생

서비스 준비 중 : 1 / 9 완료

ECS 리소스 생성	대기 중
클러스터 default	완료
작업 정의	User: arn:aws:iam::453043152051:user/manager_poland is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::453043152051:role/ecsTaskExecutionRole because no identity-
서비스	대기 중
추가 AWS 서비스 통합	대기 중

arn:aws:iam::453043152051:role/ecsTaskExecutionRole because no identity-based policy allows the iam:CreateRole action (Service: AmazonIdentityManagement; Status Code: 403)

대기 중

해결 방법 – IAM Role을 추가

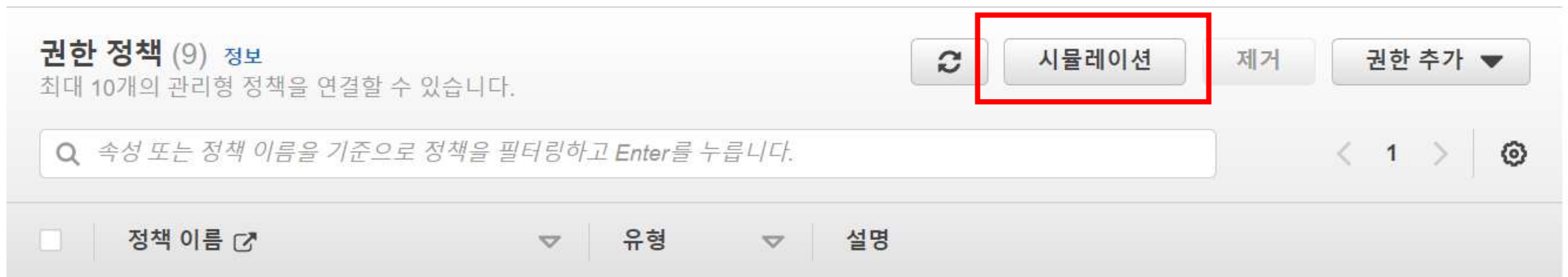
- IAM에서 정책 생성을 눌러서 IAM 서비스의 CreateRole을 추가해준다.



```
"Sid": "VisualEditor0",  
"Effect": "Allow",  
"Action": [  
    "iam:DeleteAccessKey",  
    "iam:UntagRole",  
    "iam:TagRole",  
    "iam:CreateRole",  
    "iam:TagMFADevice",  
    "iam:AttachRolePolicy",  
    "iam:CreateVirtualMFADevice",  
    "iam:ListMFADevices"
```

IAM 활용 팁 - 시뮬레이션

- IAM 계정에서 정상작동 되는지 확인하려면 루트를 로그아웃하고, IAM 계정으로 로그인을 했어야 했다.
- 귀찮게 로그인 반복하지 말고 그냥 시뮬레이션 들어가면 됨



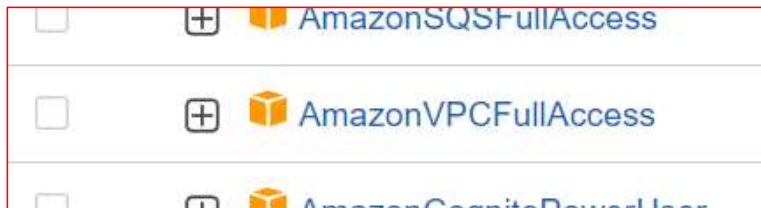
또 다시 에러 발생

- 이번엔 시뮬레이션에선 Create cluster, Create Service, Create task definition 모두 멀쩡하게 동작했는데 실제 클러스터 생성 테스트에서는 한 군데에서 에러가 났다.
- VPC 관련해서 에러가 발생

ECS 리소스 생성	대기 중
클러스터 <code>docker-test</code>	완료
작업 정의 <code>first-run-task-definition:2</code>	완료
서비스	대기 중
추가 AWS 서비스 통합	대기 중
로그 그룹 <code>[/ecs/first-run-task-definition]</code> 로그 그룹이 이미 존재합니다.	완료
CloudFormation 스택	대기 중
VPC Resource handler returned message: "You are not authorized to perform this operation. Encoded authorization failure message: HNSEg4D8Gakm6LvHcKZz3eLJ8Lve_BACYbGsvQv3BR9sFkZGAL"	

해결방법 – VPC Role을 추가

- VPC full access를 권한에 추가하면 문제 해결



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions"
      ]
    }
  ]
}
```

ECS 서비스 실행 테스트

- IAM 계정으로 접속해서 ECS에 클러스터 생성하여 서비스 실행 테스트
- 컨테이너 동작 확인

작업 상태: Running Stopped		
이 페이지의 필터		
작업	작업 정의	마지막 상태
238aeba584b7487...	first-run-task-definiti...	RUNNING

manager_poland @ millwheel-forest ▼

← → ↺ ⚠ 주의 요함 | 43.201.116.165

YouTube 프로그래머스 Cambridge Dictionary

Docker test! This has been updated