2024년도 전국기능경기대회 과제

직 종 명	클라우드컴퓨팅	과제명	Small Challenge	과제번호	제 2과제
경기시간	4시간	비번호		심사위원 확 인	(인)

1. 선수 유의사항

1) 기계 및 공구 등의 사용 시 안전에 유의하시고, 필요 시 안전장비 및 복장등을 착용하여 사고를 예방하여 주시기 바랍니다.

2) 작업 중 화상, 감전, 찰과상 등 안전사고 예방에 유의하시고, 공구나작업도구 사용 시 안전보호구 착용 등 안전수칙을 준수하시기 바랍니다.

3) 작업 중 공구의 사용에 주의하고, 안전수칙을 준수하여 사고를 예방하여주시기 바랍니다.

4) 경기 시작 전 가벼운 스트레칭 등으로 긴장을 풀어주시고, 작업도구의 사용시 안전에 주의하십시오.

5) 선수의 계정에는 비용제한이 존재하며, 이보다 더 높게 과금될 시 계정사용이 불가능할 수 있습니다.

6) 문제에 제시된 괄호박스 는 변수를 뜻함으로 선수가 적절히 변경하여사용해야 합니다.

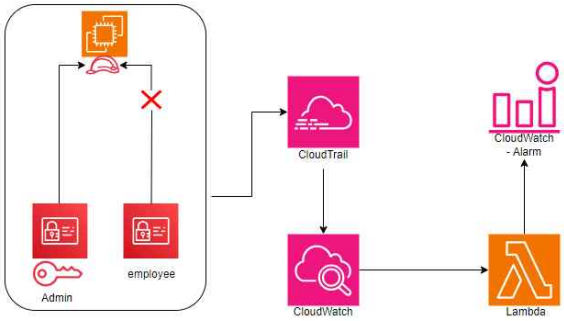
7) EC2 인스턴스의 TCP 80/443 outbound 는 anyopen 하여 사용할 수 있도록합니다.

8) 과제 종료 시 진행 중인 테스트를 모두 종료하여 서버에 부하가 발생 하지않도록 합니다.

9) 별도 언급이 없는 경우, ap-southeast-1 리전에 리소스를 생성하도록 합니다.

o Dynamic IAM Role Authorization Enforcement

Module: 8) Cloud governance



EC2 보안을 위해 관리자만 EC2 역할에 권한을 추가할 수 있어야 합니다.
두 개의 IAM 사용자를 생성합니다. AdministratorAccess 권한을 가진 관리자 사용자와 IAMFullAccess 권한을 가진 직원 사용자입니다.

모든 IAM 활동은 CloudTrail을 통해 관찰되며 로그는 모두 CloudWatch로 전송되어야 합니다.
기본적으로 EC2가 가지고 있는 역할의 권한은 AmazonSSMManagedInstanceCore 권한입니다.

직원 사용자가 EC2 역할에 권한을 추가하면 Lambda 함수가 해당 권한을 3분 이내에 자동으로 삭제하고, CloudWatch에서 경고 알림이 발생해야 합니다.
채점을 위해 기본 VPC를 이용하여 AdministratorAccess 권한을 가진 Bastion을 생성합니다.

- EC2 Role Name: wsc2024-instance-role
- IAM User Name: Admin, Employee
- CloudTrail Name: wsc2024-CT
- CloudTrail LogGroup Name: wsc2024-gvn-LG
- CloudWatch Alarm Name: wsc2024-gvn-alarm
- Lambda Name: wsc2024-gvn-Lambda
- Lambda runtime:python:3.9

S/W stack

AWS services	Other S/W
- VPC - EC2 - CloudWatch - Lambda - IAM	