

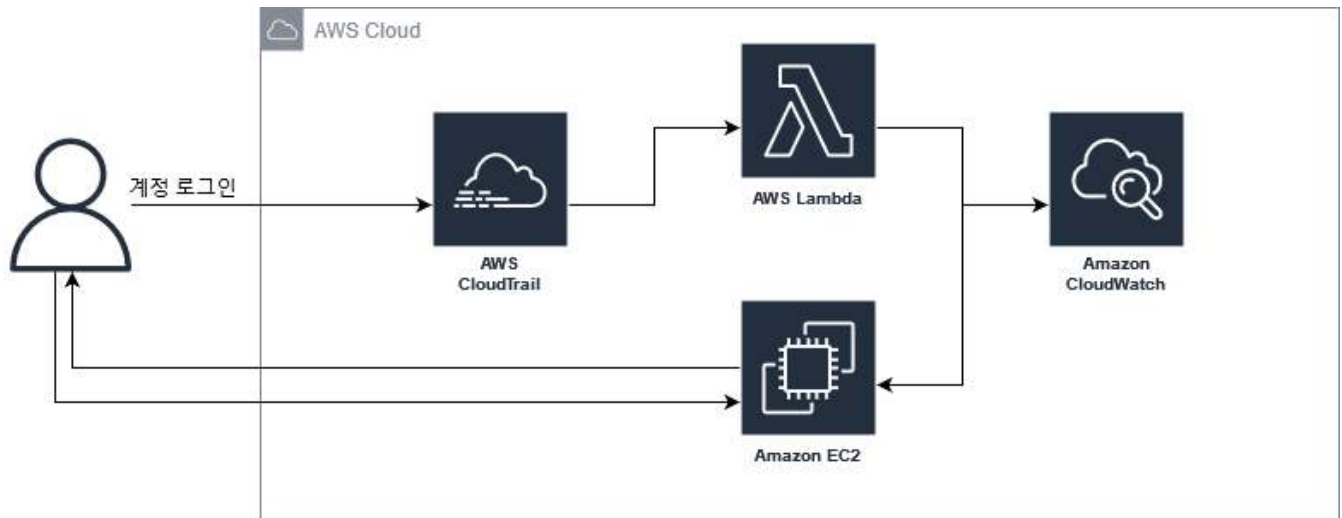
2024년도 전국기능경기대회

직 종 명	클라우드컴퓨팅	과 제 명	Governance	과제번호	제 2과제
경기시간	30분	비 번 호		심사위원 확 인	(인)

1. 요구사항

IAM 사용자 로그인 하면 로그인 기록이 저장되는 간편한 인프라를 구성합니다.

다이어그램



Software Stack

AWS

- CloudTrail
- CloudWatch
- Lambda
- EC2
- VPC
- IAM

2. 선수 유의사항

- 1) 기계 및 공구 등의 사용 시 안전에 유의하시고, 필요 시 안전장비 및 복장 등을 착용하여 사고를 예방하여 주시기 바랍니다.
- 2) 작업 중 화상, 감전, 찰과상 등 안전사고 예방에 유의하시고, 공구나 작업도구 사용 시 안전보호구 착용 등 안전수칙을 준수하시기 바랍니다.
- 3) 작업 중 공구의 사용에 주의하고, 안전수칙을 준수하여 사고를 예방하여 주시기 바랍니다.
- 4) 경기 시작 전 가벼운 스트레칭 등으로 긴장을 풀어주시고, 작업도구의 사용 시 안전에 주의하십시오.
- 5) 선수의 계정에는 비용의 제한이 존재하며, 이보다 더 높게 요금이 부과될 시 계정 사용이 불가능할 수 있습니다.
- 6) 문제에 제시된 괄호 박스 ◇는 변수를 뜻함으로 선수가 적절히 변경하여 사용해야 합니다.
- 7) EC2 인스턴스의 TCP 80/443 outbound는 anyopen하여 사용할 수 있도록 합니다.
- 8) 과제의 Bastion 서버에서 대부분의 채점이 이루어짐으로 인스턴스를 생성하지 않았거나 종료된 상태면 채점이 불가능하니 각별히 주의하도록 합니다.
- 9) 과제 종료 시 진행 중인 테스트를 모두 종료하여 서버에 부하가 발생하지 않도록 합니다.
- 10) 별도 언급이 없는 경우, ap-northeast-2 리전에 리소스를 생성하도록 합니다.
- 11) 1페이지의 다이어그램은 구성을 추상적으로 표현한 그림으로, 세부적인 구성은 아래의 요구사항을 만족시킬 수 있도록 합니다. (ex. 서브넷이 2개 이상 존재할 수 있습니다.)
- 12) 모든 리소스의 이름, 태그, 변수와 변수는 대소문자를 구분합니다.
- 13) 문제에서 주어지지 않는 값들은 AWS Well-Architected Framework 6 pillars를 기준으로 적절한 값을 설정해야 합니다.
- 14) 불필요한 리소스를 생성한 경우, 감점의 요인이 될 수 있습니다. (e.g. VPC 추가 생성)
- 15) Bastion 서버로 ssh 접속시 22번 포트 외에 다른 포트를 사용하세요.
- 16) Bastion은 비밀번호 설정 시 비밀번호를 Skills2024**로 설정합니다.

3. EC2

EC2를 활용해 Bastion 서버를 구성합니다. Bastion 서버의 접근을 위해서 TCP 2220를 사용합니다.

- Instance 이름: wsi-bastion-ec2
- Subnet: Public subnet
- 설치 패키지: AWS CLI v2, jq, curl
- Instance Type: t3.small
- EC2 IAM Role: 모든 리소스에 대해 full access를 가지는 role을 생성하여 붙입니다.

4. IAM

IAM 사용자를 생성 후 계정에 로그인시 자동으로 CloudWatch로 로그인 로그를 저장 할 수 있게 구성합니다. IAM 사용자는 모든 서비스를 사용할 수 있게 관리자 권한을 연동 시킵니다.

- IAM 사용자 이름: wsi-project-user
- IAM 권한: AdministratorAccess Policy
- AWS Management Console 접속 허용

5. CloudTrail

IAM 사용자가 콘솔로 로그인시 CloudWatch로 로그인 로그를 저장 할 수 있게 위해 계정 활동을 모니터링을 할 수 있는 서비스인 CloudTrail를 생성합니다.

- Tag: Name=wsi-project-trail

6. CloudWatch

CloudWatch는 아래에 있는 요구사항을 참고하여 로그 그룹을 생성합니다.

CloudWatch 로그 스트림에는 로그인 로그를 제외한 다른 로그들은 존재해서는 안됩니다.

- Tag: Name=wsi-project-login
- 로그 스트림 이름 : wsi-project-login-stream
- 로그 포맷: { USER: "<로그인한 IAM 사용자 이름> has logged in!" }
- 예시): { USER: "wsi-project-user has logged in!" }

7. Lambda

람다를 이용해서 Cloudtrail에 로그인 트리거가 발생되면 자동으로 cloudwatch로 로그 저장할 수 있게 구성합니다.

- Tag: Name=wsi-project-log-function