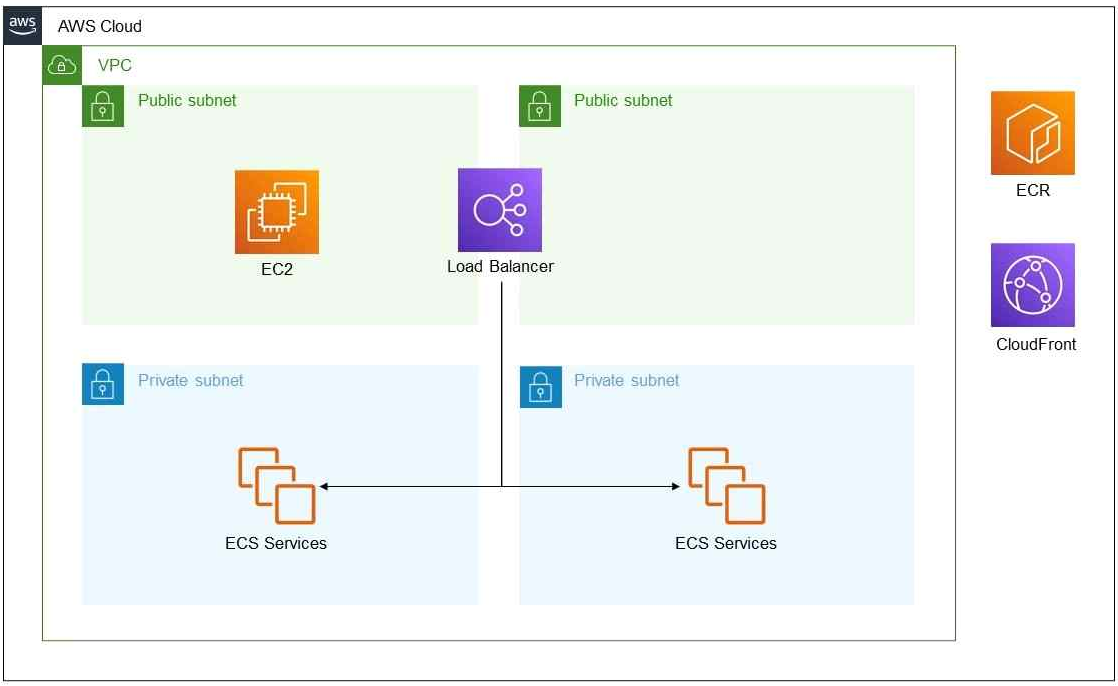
2023 지방기능경기대회 과제

직 종 명	클라우드컴퓨팅	과 제 명	Web Service Provisioning	과제번호	제1과제
경기시간	4시간	비 번 호		심사위원 확 인	(인)

1. 요구사항

AWS 서비스를 이용하여 웹서비스를 운영할 수 있는 클라우드 플랫폼을 구성하고자 합니다. 주어진 아키텍처를 바탕으로 고가용성과 성능 등 여러 가지 요소를 고려하여 웹 어플리케이션이 구동할 수 있는 클라우드 플랫폼을 구축하여야 합니다. AWS에서 제공하는 솔루션을 통해 더욱 빠르고 안정성 있게 구축하는 것이 당신의 업무입니다.

다이어그램



Software Stack

AWS	개발언어/프레임워크
- VPC	- Python / Flask
- EC2	
- ECS	
- ELB	
- ECR	
- CloudFront	

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 비용제한이 존재하며, 이보다 더 높게 과금될 시 계정 사용이 불가능할 수 있습니다.
6) 문제에 제시된 괄호박스 <>는 변수를 뜻함으로 선수가 적절히 변경하여 사용해야 합니다.
7) 문제의 효율을 위해 Security Group의 80/443 outbound는 anyopen하여 사용할 수 있도록 합니다.
8) Bastion EC2는 채점시 사용되기 때문에 종료되어 불이익을 받지 않도록 주의해 주시기 바랍니다.
9) 모든 리소스는 서울(ap-northeast-2) 리전에 구성합니다.

3. Cloud Netowkring

클라우드 인프라에 대해 네트워크 레벨의 격리 및 분리가 가능하도록 아래 요구사항을 참고하여 VPC를 구성합니다. Name 태그 가장 뒤에 붙은 알파벳은 ZONE을 의미합니다.

VPC 정보

- VPC CIDR : 10.0.0.0/16
- VPC Tag : Name=wsi-vpc

Public A subnet 정보

- CIDR : 10.0.1.0/24
- Tag : Name=wsi-public-a
- 외부 통신 : Internet G/W 를 구성하여 인터넷을 접근
- Route table Tag : Name=wsi-public-rtb

Public B subnet 정보

- CIDR : 10.0.2.0/24
- Tag : Name=wsi-public-b
- 외부 통신 : Internet G/W를 구성하여 인터넷을 접근
- Route table Tag : Name=wsi-public-rtb

Private A subnet 정보

- CIDR : 10.0.3.0/24
- Tag : Name=wsi-private-a
- 외부 통신 : NAT G/W를 구성하여 인터넷 접근이 가능하도록 구성
- Route table Tag : Name=wsi-private-rtb-a

Private B subnet 정보

- CIDR : 10.0.4.0/24
- Tag : Name=wsi-private-b
- 외부 통신 : NAT G/W를 구성하여 인터넷 접근이 가능하도록 구성
- Route table Tag : Name=wsi-private-rtb-b

4. Bastion 서버

EC2를 활용해 Bastion 서버를 구성합니다. 해당 서버는 public 존에 위치하고 stop 후 재시작하더라도 public ip가 변경돼서는 안 됩니다. 외부에서 Bastion 서버에 SSH로 접속할 수 있도록 구성합니다. 채점 시에도 사용함으로 인스턴스가 종료되어 불이익을 받지 않도록 합니다. Bastion 서버 내 어떤 사용자에서 awscli 명령어를 호출하여도 PowerUserAccess policy 권한을 갖도록 설정해야 합니다. 아래 요구사항에 따라 Bastion 서버를 구성합니다.

- EC2 type : t3.small
- 이미지 : Amazon Linux2
- Subnet : wsi-public-a
- 권한 : AWS PowerUser policy
- 설치 패키지 : awscli, curl
- Tag : Name=wsi-bastion
- Security Group : 모든 트래픽, 모든 IPv4 대상에 대해 outbound 허용

5. 웹 어플리케이션

해당 과제에서 도커 이미지로 배포하여 사용할 웹 어플리케이션에 대한 정보입니다.
Listen Port는 모두 5000으로 설정합니다. 배포파일은 수정하지 않습니다.

about 어플리케이션 정보

- 개발언어 및 프레임워크 : Python3.8 / Flask
- 도커 컨테이너에서 http://localhost:5000/about 접속 시 "The about page" 출력

projects 어플리케이션 정보

- 개발언어 및 프레임워크 : Python3.8 / Flask
- 도커 컨테이너에서 http://localhost:5000/projects 접속 시 "The projects page" 출력

6. ECR

ECS 컨테이너에서 사용할 도커 이미지를 생성합니다. 아래 요구사항에 따라 프라이빗 리포지토리를 구성하고 도커 이미지를 업로드합니다. 이미지는 업로드 시 자동으로 스캔하도록 하며 태그는 모두 latest로 설정합니다. 모든 이미지에 Low 레벨 이상의 취약성이 없도록 합니다.

about 도커 이미지 정보

- 리포지토리 이름 : wsi-about
- 해당 도커 이미지 실행 시 about 어플리케이션이 실행되어야 합니다.

projects 도커 이미지 정보

- 리포지토리 이름 : wsi-projects
- 해당 도커 이미지 실행 시 projects 어플리케이션이 실행되어야 합니다.

7. ECS

아래 요구사항에 따라 ECS 서비스를 구성합니다. 모든 컨테이너는 EC2에서 실행되어야 합니다. ALB를 통해서 들어오는 요청만 허용해야 합니다. 모든 서비스의 호스트 포트는 5000으로 설정하며 컨테이너 포트를 적절히 매핑합니다. 가용영역 하나에 문제가 생겨도 서비스가 정상적으로 이루어져야 합니다. 모든 서비스는 Fargate(Linux)에서 실행되어야 하며 Private Subnet에 구성합니다.

클러스터 정보

- 클러스터 이름 : wsi-ecs

about 서비스 정보

- 서비스 이름 : wsi-about-svc
- 작업 정의 : about-task-def
- 컨테이너 이미지 : about 도커 이미지
- Security Group : wsi-about-sg

projects 서비스 정보

- 서비스 이름 : wsi-projects-svc
- 작업 정의 : projects-task-def
- 컨테이너 이미지 : projects 도커 이미지
- Security Group : wsi-projects-sg

8. ALB

ALB가 요청을 수신하면 요청을 ECS 서비스로 보낸 다음 응답을 클라이언트에 반환합니다. Target Group을 통해 대상을 선택하도록 구성합니다. ALB는 CloudFront를 통해서 들어오는 요청만 허용해야 합니다. 아래 요구사항에 따라 ALB를 구성합니다.

- ALB 이름 : wsi-alb
  - HTTP 80 /about 경로로 들어오는 요청은 about 서비스로 전달되어야 합니다.
    Target Group : wsi-about-tg
  - HTTP 80 /projects 경로로 들어오는 요청은 projects 서비스로 전달되어야 합니다.
    Target Group : wsi-projects-tg

9. CloudFront

CloudFront를 통하여 웹서비스 접근이 가능하도록 합니다. 캐싱을 통해 유저가 브라우저를 통해 CloudFront의 주소에 접근하여 보다 빠른속도로 웹서비스를 이용할 수 있도록 합니다. about 서비스로의 요청에 대해서는 캐싱이 되어야 하고 projects 서비스로의 요청에 대해서는 캐싱하지 않도록 설정합니다.

- 프로토콜 : CloudFront에 접근시 HTTPS를 통하여 접근 가능하도록 구성
- Origin : ALB
- Edge : 한국뿐만 아니라 전 세계의 유저가 빠른 속도로 접근 가능하도록 구성
- 기타 : 채점 시 오동작 예방으로 IPv6는 비활성화하고, 하나의 CloudFront만 생성
- /about 경로로 들어오는 요청은 ALB를 통해 about 서비스로 전달되어야 합니다.
- /projects 경로로 들어오는 요청은 ALB를 통해 projects 서비스로 전달되어야 합니다.