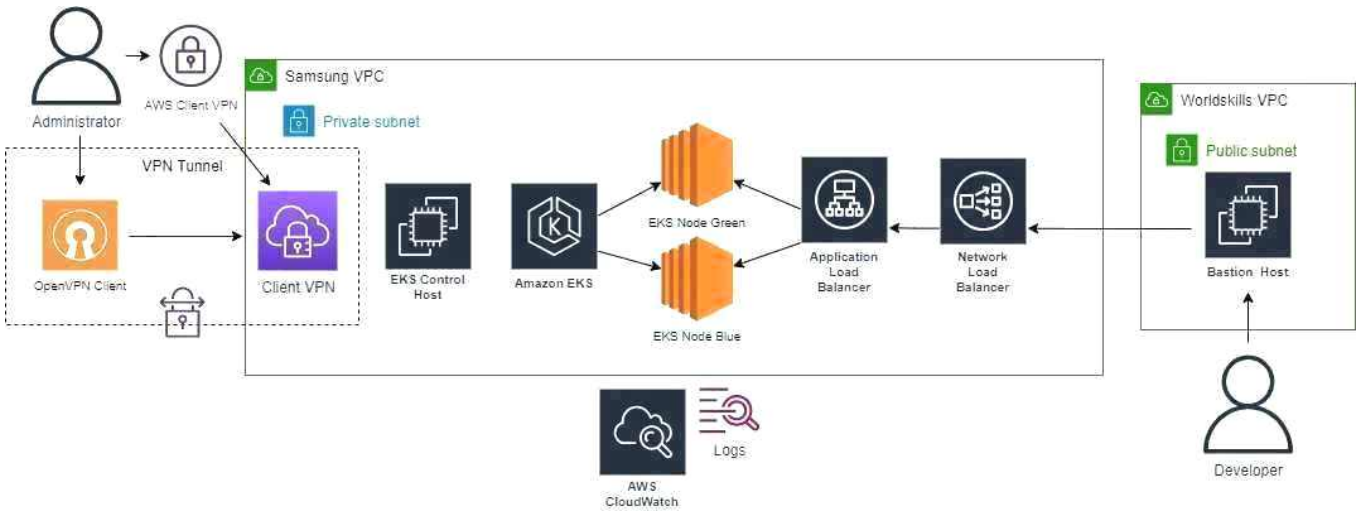
2023년도 클라우드컴퓨팅 친선경기대회

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

1. 요구 사항

당신은 현재 S/W 회사에서 DevOps 엔지니어로 근무중입니다. S/W 회사는 코로나 때문에 모든 직원들이 재택근무를 시작했습니다. 재택근무를 하는 직원들의 원활한 재택근무를 위해 AWS 내부망에 접근할 수 있는 VPN 구축 및 S/W 회사의 회원 등록 및 조회할 수 있는 서비스를 S/W 회사 회원 들만 접근이 가능하도록 구성합니다.



S/W stack

AWS

VPC VPN

EKS ALB

EC2 NLB

CloudWatch

Route53

Application

Golang net/http

2. 선수 유의사항

※ 다음 유의사항을 고려하여 요구사항을 완성하시오.

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 비용 제한이 존재합니다. 비용 제한 이상 사용 시 계정의 사용이 불가능 할 수 있습니다.
6) 문제에 제시된 괄호는 변수를 뜻함으로 선수가 적절히 변경하여 사용하도록 합니다.
7) 문제의 효율을 위해 Security Group의 80/443 outbound는 anyopen하여 사용하도록 합니다.
8) 과제 종료 시 진행 중인 테스트를 모두 종료하여 서버에 부하가 발생하지 않도록 합니다.
9) 채점 시 Bastion EC2를 사용하오니 종료되어 불이익을 받지 않도록 합니다.
10) 비밀번호가 따로 명시되지 않을 경우 “Skills53##”을 사용합니다.
11) 모든 Resource 및 Instance의 Instance Type은 “t3.small”을 사용합니다.

3. 인증서(Certificate & Key)

Client VPN을 사용하기 위해서 인증서(.crt & .key)를 필요합니다. 인증서를 사용하기 위해 ACM(Amazon Certificate Manager)를 이용합니다. ACM을 이용해서 인증서를 Client VPN로 사용하도록 합니다.

Certificates:

- server.crt (Self-Signed Certificate)
- server.key (Self-Signed RSA Private Key)
- ca.crt (Selft-Signed Chain)

Client Certificates:

- client.worldskills-korea.int.crt (Client Certificate)
- client.worldskills-korea.int.key (Client RSA Private Key)
- ca.crt (Selft-Signed Chain)

4. 네트워킹

Worldskills

VPC를 생성하여 클라우드 네트워킹을 구성합니다. HA를 고려하여 최소 3개의 az를 가지도록 VPC를 설계합니다. 구성 시 이름(Name)은 Key를 Name으로 갖는 Tag를 의미합니다. 서브넷 구성 시 zero subnet을 허용하며, 서브넷 마스크는 모두 24bit을 사용합니다.

Name	CIDR	Route Table
worldskills-korea.vpc	10.44.0.0/16	Default
worldskills-korea.pub-a	위 VPC CIDR의 101번째 Network 주소	worldskills-korea.pub-rt
worldskills-korea.pub-c	위 VPC CIDR의 103번째 Network 주소	worldskills-korea.pub-rt
worldskills-korea.priv-a	위 VPC CIDR의 201번째 Network 주소	worldskills-korea.priv-a-rt
worldskills-korea.priv-c	위 VPC CIDR의 203번째 Network 주소	worldskills-korea.priv-c-rt

또한 아래의 표를 참고해 DHCP 서비스를 구성합니다.

Name	Domain	DNS Server	NTP
worldskills-korea-dhcp	worldskills.internal	Route53의 DNS 서버 주소	Amazon Time Sync Service

Samsung

Name	CIDR	Route Table
samsung-korea.vpc	192.168.0.0/16	Default
samsung-korea.pub-a	위 VPC CIDR의 101번째 Network 주소	samsung-korea.pub-a-rt

5. VPN

현재 재택근무중인 직원들이 VPC 내부에 접근하기 위해 Client VPN을 사용해 접근이 되도록 구성합니다. Client VPN은 worldskills-korea.vpc에 생성된 모든 Private Subnet만 접근이 가능해야 하고, 해당 VPN은 UDP 1194번로 Listen되도록 구성합니다. 배포파일로 제공된 client 인증서를 사용하여 사용자 인증이 가능하도록 구성합니다. VPN으로 접근하기 위한 발급 된 Client Configuration(.opvn) 파일은 S3 Bucket에 /vpn-config/라는 경로에 worldskills.opvn이라는 이름으로 업로드 되어 있어야합니다. VPN으로 접근 시 내부 DNS 주소에 DNS Query가야 가능해야합니다.

VPN Name: worldskills-korea-vpn
VPN IP 대역: 172.29.8.0/22
VPN Login Banner: Welcome to Worldskills Korea VPN
Split Tunnel: enable
VPN Link Download: https://aws.amazon.com/ko/vpn/client-vpn-download/

6. Container Orchestration

클라우드 환경에서 운영되는 수많은 컨테이너 및 워크로드를을 일일이 관리하기에는 너무 불편합니다. 이러한 불편한 사항을 해결하고자, Kubernetes를 사용해서 수많은 컨테이너, 워크로드들을 관리 및 운영하고자 합니다. 아래의 요구사항을 참고하여 구성합니다.

A.) Control Host (EC2)

- Name Tag: worldskills-korea-control-ec2
- Subnet: 가용영역 A에 위치한 Private Subnet
- Instance Type: t3.medium
- Essential Software: curl, jq, awscliv2, eksctl, kubectl, wget
- Operating System: AmazonLinux 2
- Private IP 주소: 10.44.200.8
- SSH 접근할 때 사용하는 포트 번호는 “2220”
- IAM Role Name: worldskills-korea-control-role

B.) EKS

Kubernetes에서 생성되는 Pod와 같은 Object를 운영하려면 노드가 필요합니다. Kubernetes 제어 영역이나 작업자 노드를 설치 및 운영할 필요 없이 AWS에서 Kubernetes를 손쉽게 실행할 수 있게 EKS를 사용하도록 합니다. Fargate Profile을 사용해서 EKS on Fargate를 구성합니다. 아래의 표를 참고하여 Fargate Profile을 구성합니다.

Cluster:

- EKS Cluster Name: worldskills-korea-eks-cluster
- Kubernetes 버전: 1.23
- 해당 Cluster는 외부에서 접근이 불가능하도록 구성합니다.

Fargate Profile:

- Fargate Profile Name: worldskills-korea-fargate-profile
- Namespace: worldskills-api

EC2 Profile:

- Node Group 이름: worldskills-korea-node
- EC2 Node들의 Name Tag: worldskills-korea-ec2
- EC2 Node들의 Instance Type: t3.micro
- Operating System: Amazon Linux 2
- 해당 EC2 Node들은 SSH 접근 불가능하도록 구성합니다.

7. Kubernetes

Pod & Deployment

- Deployment Name: worldskills-korea-dp
- Container Name: worldskills-cnt
- 해당 Pod는 최소 2개 이상 운영 중이여야 합니다.
- 해당 Pod는 Deployment를 통해서 관리가 되어야 됩니다.

Limit Range

- CPU: min - 1, max - 2
- Memory: min - 256Mi, max - 512Mi

Service

- Service Name: worldskills-korea-svc

AutoScaling

- Pod들의 평균 CPU 사용률이 30%이상 증가할 경우 자동으로 Scale-out & Scale-in이 되도록 구성합니다.

Namespace: worldskills-api

8. LB

웹 서버를 운영하면서 생기는 트래픽에 대해 처리하기 위해 LB를 구축합니다. 어플리케이션의 K8s Ingress 생성 시 자동으로 AWS ALB가 생성되어야 합니다. ALB는 수동으로 생성하지 않고 kubectl 명령어를 통해서 생성되어야 합니다.

사용자가 접근하면 아래와 같은 방식으로 라우팅이 되어야 합니다 :

```
End User -> Network Load Balancer -> Application Load Balancer -> Web Server
```

Application Load Balancer(ALB)

- ALB Name: worldskills-korea-alb
- LB의 scheme: Internal
- Kubernetes를 사용해 운영중인 API 서버를 Routing 타켓으로 설정합니다.
- ALB는 80번을 Listen 하도록 구성합니다.

Network Load Balancer(NLB)

- NLB Name: worldskills-korea-nlb
- LB의 scheme: Internal
- Application Load Balancer를 Routing 타켓으로 설정합니다
- NLB는 80번을 Listen 하도록 구성합니다.

Load Balancer Security(보안)

- NLB 통하지 않고 직접적으로 ALB의 /users에 접근 할 경우 403 에러코드와 함께 “Only Authorized Person is Allowed” 이라는 message를 출력합니다.
- NLB 통하지 않고 wget 명령어를 직접적으로 ALB의 /users에 접근하면 500 에러코드와 함께 “Only accessible using VPN” 라는 message를 출력 합니다.

9. Application Description

- Image URL: jeonilshin/wsi-skills(Docker Hub)
- Listen Port: 8080
- Sample API Requests

User를 추가하는 명령어

```
$ curl -XPOST -d '{"nickname": "player101", "email": "admin@user.local"}' localhost:8080/users
```

User를 조회하는 명령어

```
$ curl localhost:8080/users
```

- Log: 따로 저장되지 않습니다. 하지만 Log들은 STDOUT과 STDERR 형식으로 출력됩니다.

10. DNS

내부에서 운영 중인 서비스에 내부 Domain을 사용해 접근을 하기위해 Route53을 구축합니다.

- Domain Name: worldskills.internal(Private Zone)
- 아래의 표를 참고하여 Record를 구성합니다.

Record Name	Value
control	10.44.200.8
api	<NLB의 주소>

11. Logs

애플리케이션에서 발생하는 log들을 효과적으로 관리하기 위해서 CloudWatch를 사용해 중앙 집중 식 관리이 가능하도록 구성합니다. Kubernetes의 모든 Pod에서 사용자가 요청한 API에서 발생하는 모든 Log들을 CloudWatch Logs에 아래의 정보를 참고하여 구성하세요.

- Log Group: /cloud/worldskills/korea
- Stream: api_<Instance Id>

12. Storage

여러 가지 파일들을 효율적으로 관리하기 위해 S3 Bucket을 생성해 관리하기이해서 S3 Bucket을 구성합니다.

- S3 Bucket Name: worldskills-korea-s3-<AWS Account ID>

13. Remote Host(Samsung)

- 해당 Instance의 Name Tag는 samsung-korea-remote로 지정합니다.
- 해당 Instance의 Type은 t3.micro
- OS는 Amazon Linux 2
- 해당 Instance는 재부팅 하도 공인 IP가 바뀌어서는 안됩니다.
- 해당 Instance에게는 PowerUser 권한을 부여합니다.
- VPN이 연결되어 있지 않은 상태에서는 Worldskills 항목에서 구축한 서비스에 접근이 되어서는 안 됩니다.