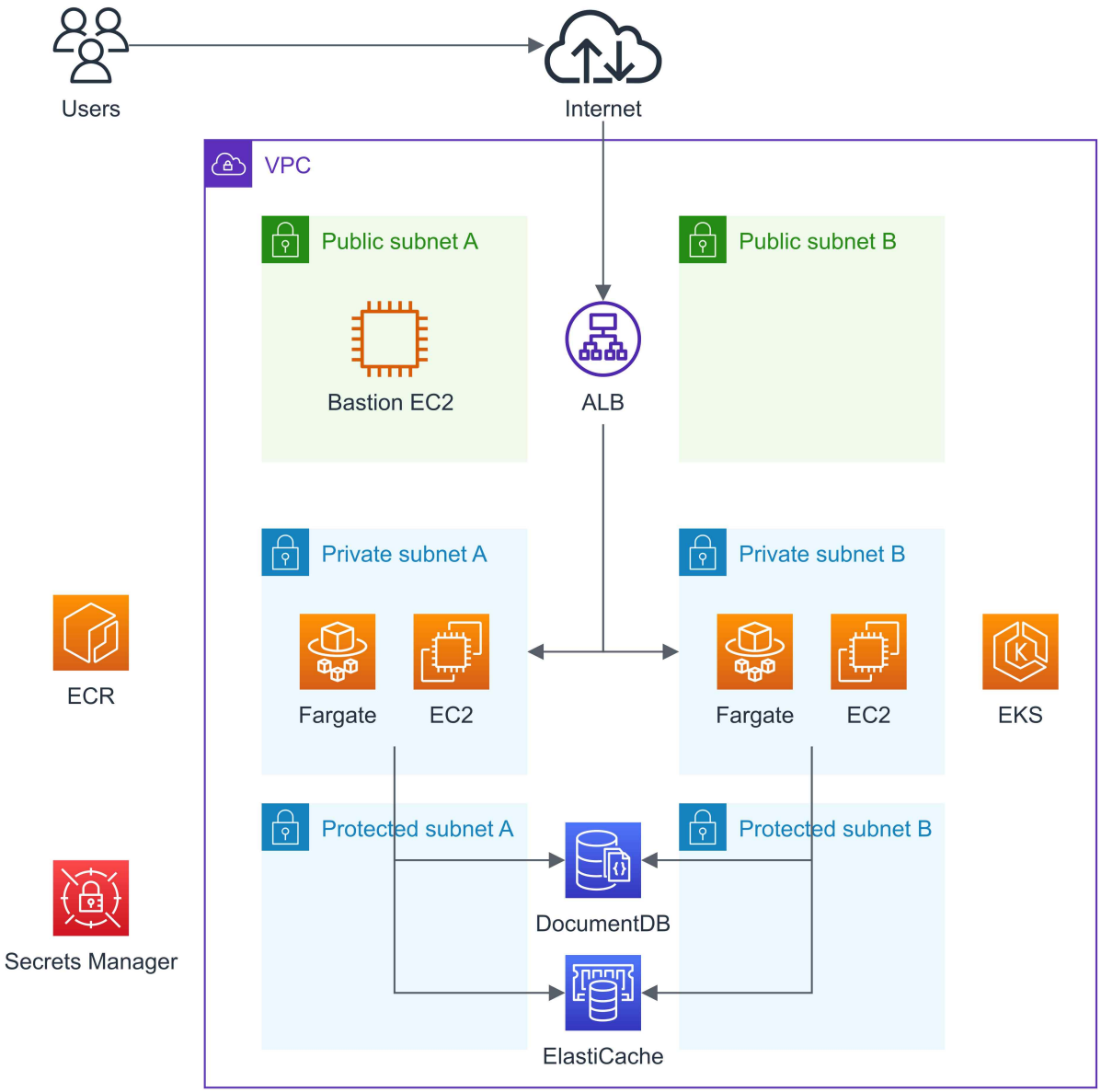
2024년도 지방기능경기대회 과제

직 종 명	클라우드컴퓨팅	과제명	Web Service Provisioning	과제번호	제1과제
경기시간	4시간	비번호		심사위원 확 인	(인)

1. 요구사항

당신은 WorldSkills의 시스템 중 인증 시스템에 대한 Infrastructure 설계와 운영을 담당하는 업무를 맡았습니다. 인증 시스템은 MSA로 구성되어 있습니다. 주어진 요구사항과 클라우드의 설계원칙인 고가용성, 확장성, 비용, 보안 등을 잘 고려하여 인프라를 구축해야 합니다.

다이어그램



Software Stack

AWS	개발언어/프레임워크
- VPC	- Golang
- EC2	
- ELB	
- Fargate	
- EKS	
- ECR	
- DocumentDB	
- ElastiCache	
- Secrets Manager	

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) 문제에 제시된 괄호박스 < > 는 변수를 뜻함으로 선수가 적절히 변경하여 사용해야 합니다.
6) 문제 풀이와 채점의 효율을 위해 Security Group의 80/443 Outbound는 Anyopen하여 사용할 수 있도록 합니다.
7) Bastion EC2는 채점 시 사용되기 때문에 종료되거나 연결 문제, 권한 문제 등으로 발생할 수 있는 불이익을 받지 않도록 주의하시기를 바랍니다.
8) 모든 리소스는 서울(ap-northeast-2) 리전에 구성합니다.
9) 제공자료는 수정 없이 사용합니다. 제공자료를 수정해서 사용하면 불이익을 받을 수 있습니다.

3. Networking

클라우드 인프라 구성을 위하여 기본적인 네트워크 구성을 시행합니다. 부록 1의 정보를 참고하여 AWS VPC를 생성합니다.

4. Bastion Server

EC2를 사용하여 Bastion 서버를 생성합니다. Bastion 서버의 IP는 재부팅 후에도 변경되어서는 안 되며, 종료하지 않도록 특히 주의합니다. 또한 SSH를 사용해 서버에 접속하므로 SSH로 접근할 수 있어야 하며, 포트는 반드시 SSH 기본 포트를 사용해서는 안 됩니다. 해당 인스턴스의 root 계정에서 AWS CLI를 사용하면 AWS의 모든 권한을 사용할 수 있어야 하며, kubectl을 사용하면 해당 EKS Cluster의 모든 권한을 사용할 수 있어야 합니다. 패키지들은 반드시 버전과 권한 등의 문제가 없어야 합니다.

- Instance Type : t4g.large
- OS Image : Amazon Linux 2023
- Name Tag : skills-bastion-ec2
- Packages : AWS CLI v2, cURL, jq, kubectl

5. NoSQL Database

user 애플리케이션은 데이터베이스로 MongoDB를 사용합니다. AWS에서 사용할 수 있는 Managed MongoDB Service인 DocumentDB를 활용해 user 애플리케이션이 사용할 수 있도록 합니다. MongoDB의 포트는 기본 포트에서 다른 포트로 반드시 변경해야 합니다. DocumentDB option을 사용하여 고가용성을 보장해야 하고, 암호화와 로깅(audit, profiler), 백업 등을 활성화해야 합니다. 보안을 위해 인터넷과 연결되지 않는 환경에 구성합니다.

- Cluster Name : skills-mongodb-cluster
- Engine Version : 5.0.0
- Instance Class : db.t4g.medium

6. In-Memory Database

token 애플리케이션은 데이터베이스로 Redis를 사용합니다. AWS에서 사용할 수 있는 Managed Redis Service 중 하나인 ElastiCache를 활용해 token 애플리케이션이 사용할 수 있도록 합니다. Redis의 포트는 기본 포트에서 다른 포트로 반드시 변경해야 합니다. 고가용성을 보장해야 하고, 암호화(AtRest Encrytion, Transit Encnytion), 로깅, 백업 등을 활성화해야 합니다. Sharding 또한 활성화함으로써 token 애플리케이션이 문제없이 동작할 수 있도록 해야 합니다.

- Cluster Name : skills-redis-cluster
- Engine Version : 7.0
- Instance Type : t4g.small

7. Application

제공자료로 주어진 애플리케이션은 Golang으로 개발된 바이너리입니다. token 바이너리는 x86_64 기반에서 빌드되었으며, user 바이너리는 ARM64 기반에서 빌드되었습니다. user 애플리케이션은 token 애플리케이션의 REST API 사용이 가능해야 합니다. 부록 2에 명시된 바이너리 사용 방법을 충분히 숙지하고, 애플리케이션을 운용해야 합니다. 또한, 컨테이너 이미지 내에서 curl 사용이 가능해야 합니다. 제공자료에 API 문서가 있습니다.

8. Secrets Store

JWT를 발행할 수 있게 user 애플리케이션에서 Secrets Manager에 접근할 수 있어야 합니다. Secret은 JSON 형식으로 {"secretValue": "secret"} 와 같은 형태로 저장해야 합니다.
(ex. {"secretValue":"test12345678"})

9. Container Image Registry

AWS ECR를 사용해 애플리케이션의 컨테이너 이미지를 저장합니다. user와 token 애플리케이션에 대해 각각 하나씩 레포지토리를 생성합니다. 두 레포지토리 모두 KMS 암호화와 취약점 분석 등이 가능해야 하며, 같은 태그를 가진 이미지가 업로드되지 않도록 구성합니다.

- user 애플리케이션 레포지토리 이름 : user
- token 애플리케이션 레포지토리 이름 : token

10. Container Orchestration

EKS 기반의 Kubernetes로 Container Orchestration을 구성합니다. Kubernetes Cluster의 Control Plane에서 발생하는 모든 로그를 CloudWatch Logs에서 확인할 수 있어야 하며, Kubernetes의 Secret 리소스들은 반드시 KMS로 암호화해야 합니다. Private 형태의 EKS 클러스터를 생성하고, Kubernetes API는 외부에서 접근 불가능해야 하며, Bastion Server에서만 접근할 수 있어야 합니다. token은 명시된 Fargate에서 운용하고, user는 명시된 Nodegroup에서 운용하며, 다른 Addon들은 반드시 Addon Nodegroup에서 운용해야 합니다. 단, DaemonSet 리소스는 Fargate를 제외한 모든 Node에서 운용되어야 합니다.

- Clsuter Name : skills-eks-cluster
- Kubernetes Version : EKS 최신버전

Addon Nodegroup

애플리케이션을 제외한 다른 모든 Addon들은 반드시 Addon Nodegroup에서 운용해야 합니다. 최소 2개 이상 운용하여야 하며, 평상시에는 2개를 유지해야 합니다.

- Nodegroup Name : skills-eks-addon-nodegroup
- Node EC2 Instance Tag : Name=skills-eks-addon-node
- Node EC2 Instance Type : t4g.large

App Nodegroup

user 애플리케이션은 반드시 App Nodegroup에서 운용해야 하며, user 애플리케이션을 제외한 다른 리소스들은 App Nodegroup에 존재해서는 안 됩니다. 최소 2개 이상 운용하여야 하며, 평상시에는 2개를 유지해야 합니다.

- Nodegroup Name : skills-eks-app-nodegroup
- Node EC2 Instance Tag : Name=skills-eks-app-node
- Node EC2 Instance Type : m6g.large

App Fargate Profile

token 애플리케이션은 반드시 App Fargate Profile에서 운용해야 하며, token 애플리케이션을 제외한 다른 리소스는 App Fargate Profile에 존재해서는 안 됩니다.

- Fargate Profile Name : skills-eks-app-profile
- Fargate Resource : 0.5vCPU, 1GB Memory

Kubernetes Resource

user 애플리케이션과 token 애플리케이션은 *skills* Namespace에 생성해야 하며, user 애플리케이션의 Deployment 이름은 *user*, token 애플리케이션의 Deployment 이름은 *token*이어야 합니다. *user*와 *token* Deployment의 Pod는 각각 최소 2개 이상 운용하여야 하며, 평상시에는 2개를 유지해야 합니다.

11. Load Balancing

user 애플리케이션을 외부에서 접근할 수 있으면서, 부하를 분산할 수 있도록 Load balancer를 사용합니다.

- Load Balancer Type : Application Load Balancer
- Load Balancer Name : skills-user-alb
- Load Balancer Scheme : internet-facing
- Load Balancer Protocol : HTTP
- Load Balancer Port : 80

12. Auto Scaling

user 애플리케이션과 token 애플리케이션이 많은 리소스를 사용하면, Auto Scaling이 수행되도록 구성합니다. user 애플리케이션이 Auto Scaling이 수행되면 Pod가 늘어나면서, Node도 늘어나야 합니다. Pod 개수가 줄어들면, Node 개수도 줄어들어야 합니다. token 애플리케이션이 Auto Scaling이 수행되면 Fargate Pod가 늘어나야 하고, 리소스 사용량이 적으면 Fargate Pod 개수가 줄어들어야 합니다. Pod의 CPU 사용량이 10% 이상일 때 Scale-out, 10% 미만일 때 Scale-in되어야 하며, Scale-out은 5분 이내, Scale-in은 20분 이내에 이루어져야 합니다.

13. Logging

user 애플리케이션과 token 애플리케이션은 표준 출력과 표준 에러로 로그를 출력하고 있습니다. 이 로그들을 CloudWatch에 저장할 수 있도록 구성합니다.

- user 애플리케이션 Log Group 이름 : /aws/app/user
- token 애플리케이션 Log Group 이름 : /aws/app/token

부록 1

VPC 정보

Name Tag	CIDR
skills-vpc	10.100.0.0/16

Subnets 정보

Name Tag	CIDR	Availability Zone
skills-public-subnet-a	10.100.1.0/24	ap-northeast-2a
skills-public-subnet-b	10.100.2.0/24	ap-northeast-2b
skills-private-subnet-a	10.100.11.0/24	ap-northeast-2a
skills-private-subnet-b	10.100.12.0/24	ap-northeast-2b
skills-protected-subnet-a	10.100.21.0/24	ap-northeast-2a
skills-protected-subnet-b	10.100.22.0/24	ap-northeast-2b

Route Tables 정보

Name Tag	Subnet	Gateway
skills-public-rtb	skills-public-subnet-a skills-public-subnet-b	Internet Gateway (Name Tag : skills-igw)
skills-private-rtb-a	skills-private-subnet-a	NAT Gateway (Name Tag : skills-nat-a)
skills-private-rtb-b	skills-private-subnet-b	NAT Gateway (Name Tag : skills-nat-b)
skills-protected-rtb	skills-protected-subnet-a skills-protected-subnet-b	NO INTERNET ACCESS

부록 2

user 애플리케이션

애플리케이션 설명

사용자 데이터(email, password)를 입력받아 새로운 사용자를 생성하거나, 사용자 데이터를 입력받아 JWT를 발행합니다. 데이터베이스는 MongoDB를 사용합니다. 하단의 환경 변수를 설정해야 애플리케이션이 문제없이 동작할 수 있습니다. MongoDB 데이터베이스 이름을 지정하면, 해당 데이터베이스 내부에는 user라는 컬렉션이 자동으로 생성되게 됩니다. AWS Secrets Manager에서 secret을 가져와 JWT 발행에 사용합니다.

REST API는 TCP 8080에서 접속할 수 있습니다.

환경 변수

- MONGODB_HOST : MongoDB 주소
- MONGODB_PORT : MongoDB 포트
- MONGODB_USERNAME : MongoDB 사용자
- MONGODB_PASSWORD : MongoDB 사용자 비밀번호
- AWS_REGION : Secrets Manager Secret이 위치한 리전
- AWS_SECRET_NAME : Secrets Manager Secret 이름
- TOKEN_ENDPOINT : token 애플리케이션 엔드포인트 URL
  (ex. http://token-endpoint:8080)

token 애플리케이션

애플리케이션 설명

user 애플리케이션에서 생성된 JWT를 전달받아 In-Memory Database에 저장합니다. 데이터베이스는 Redis를 사용합니다. 하단의 환경 변수를 설정해야 애플리케이션이 문제없이 동작할 수 있습니다.

REST API는 TCP 8080에서 접속할 수 있습니다.

환경 변수

- REDIS_HOST: Redis Configuration 주소
- REDIS_PORT : Redis Configuration 포트