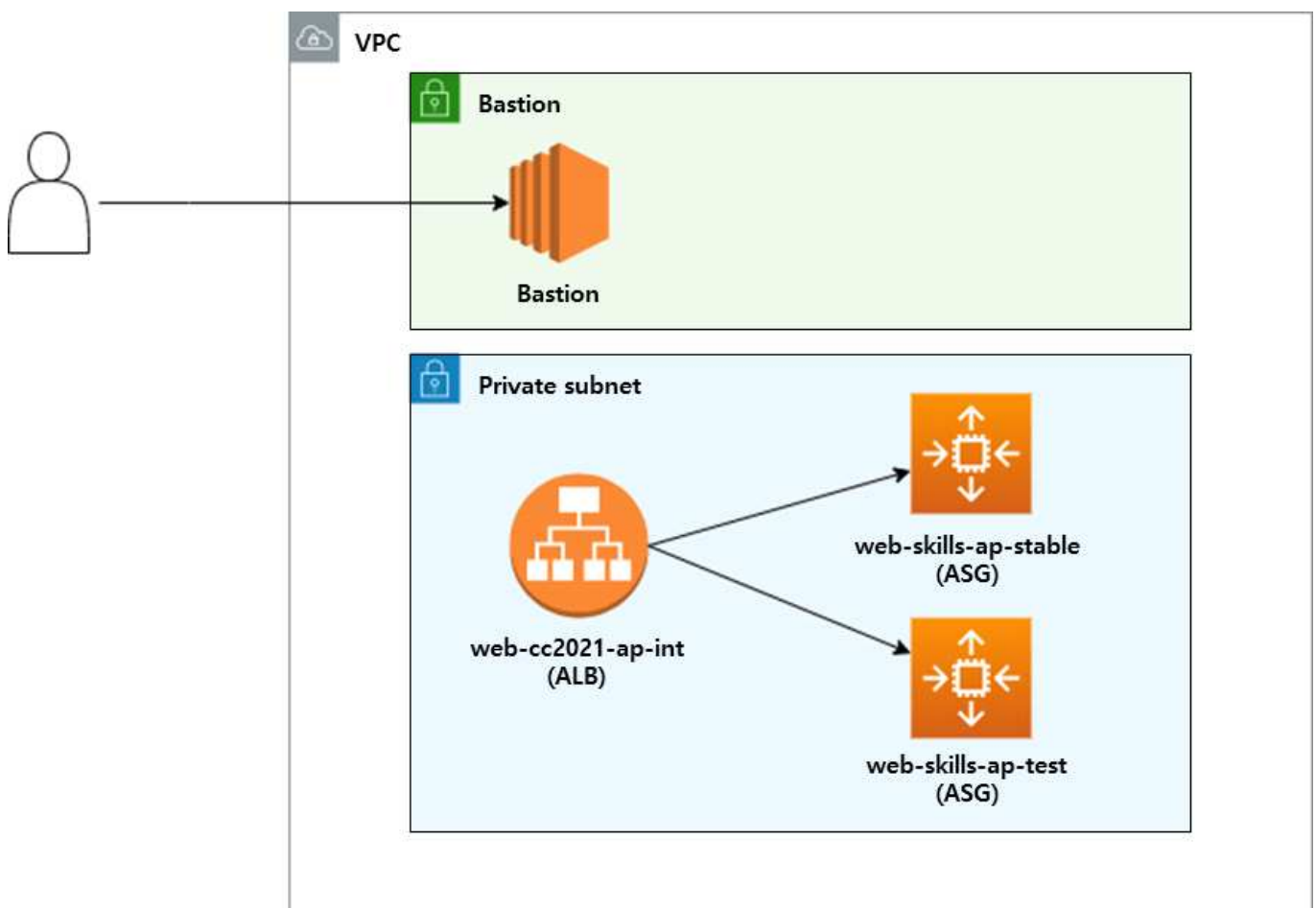


# 2021년도 지방기능경기대회 과제

직 종 명	클라우드컴퓨팅	과 제 명	IT Infrastructure	과제번호	제 1과제
경기시간	4시간	비 번 호		심사위원 확 인	(인)

## 1. 요구사항

당신은 웹서비스를 운영하는 회사에서 클라우드 인프라 엔지니어로 일하고 있습니다. 백엔드 개발자가 개발한 어플리케이션을 클라우드에 배포하여 서비스를 운영하는 것이 업무입니다. 서비스 운영을 위하여 고가용성과 확장성, 부하분산을 고려한 네트워크, 서버 설계 및 구축을 진행해야 하고, 개발된 어플리케이션 배포를 위한 자동화를 구성해야 합니다. 또한 효과적인 서비스 운영을 위해 A/B 테스트도 구현해야 합니다.



## 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 주의하시기 바랍니다.
- 5) 모든 EC2 타입은 t3.small을 사용하시기 바랍니다.
- 6) EC2의 OS는 Amazon Linux2를 사용하시기 바랍니다.
- 7) Seoul region을 사용하시기 바랍니다.
- 8) 채점 시 EC2 종료 등으로 불이익을 받지 않도록 주의하여 구성하시기 바랍니다.
- 9) 웹서버 인스턴스는 삭제 후 재생성 하여 채점 할 수 있으므로 구성이 초기화 되어 불이익을 받지 않도록 유의하시기 바랍니다.
- 10) 클라우드 리소스 특성상 인스턴스는 갑자기 삭제 될 수 있기 때문에 이미지나 스냅 샷을 생성 하는 등 백업하여 불이익을 받지 않도록 유의하시기 바랍니다.
- 11) 채점은 Bastion 서버에서 명령어를 실행해 이루어지므로 과제 종료 전 Bastion 서버가 종료 되지 않도록 구성하여야 합니다.
- 12) 과제에 제시된 이름 혹은 태그를 사용하지 않는 경우 채점 시 불이익이 있을 수 있습니다.
- 13) 문제에 제시된 <변수>부분은 그대로 사용하는 것이 아니라 선수가 변경하여 사용해야 합니다.
- 14) 패키지 설치를 위하여 모든 EC2 인스턴스의 tcp 80/443 포트의 outbound 트래픽은 0.0.0.0/0로 열어두어야 합니다.
- 15) 원활한 채점을 위해 SSH 접속방법은 패스워드 방식으로 변경해야 합니다.
- 16) 경기 종료 전 웹서버들의 ASG는 min:2, desired:2, max: 10으로 변경해야 합니다.
- 17) 채점시 AWS 명령어 수행이 가능하도록 AWSCLI를 모든 EC2에 설치합니다. 권한 설정은 서버마다 다를 수 있으며, 해당내용은 과제에 명시된 대로 구성합니다.
- 18) 채점시 curl 명령어 수행이 가능하도록 curl을 모든 EC에 설치합니다.

### 3. 네트워크 구성

클라우드 리소스 생성을 위해 AWS의 VPC 구성합니다. 생성 시 부하 분산과고가용성을 고려하여 VPC를 생성해야 합니다.고가용성을 위한 구성 시 A와 B 두개의 가용영역(AZ)만 사용해야 합니다.

#### 3.1. Virtual Private Cloud

- VPC에 할당하는 기본 CIDR은 10.0.0.0/16을 사용합니다.
- 이름은 vpc-skills-ap로 설정합니다.
- VPC 아래 생성되는 서브넷은 모두 24bit를 갖도록 생성합니다.
- 서브넷은 obit을 사용해 시작하도록 합니다.(10.0.0.0/24부터 사용)

#### 3.2. Public subnet

- 서브네팅하여 구성되는 가용한 대역 중 첫 번째/세 번째 서브넷을 public-a, public-b에 할당합니다.
- 첫 번째 서브넷은 10.0.0.0/21이며, 세 번째 서브넷은 10.0.2.0/24입니다.
- public subnet에 위치하는 VM은 본인의 IP를 통해 인터넷에 접근 가능해야 합니다.
- A존 서브넷 이름은 skills-pub-a로 설정합니다.
- B존 서브넷 이름은 skills-pub-b로 설정합니다.

#### 3.3. Private subnet

- 서브네팅하여 구성되는 가용한 대역 중 두 번째/네 번째 서브넷을 private-a, private-b에 할당합니다.
- 두 번째 서브넷은 10.0.1.0/21이며, 네 번째 서브넷은 10.0.3.0/24입니다.
- 해당 서브넷에 위치하는 VM은 NAT gateway를 통해 인터넷에 접근 가능해야 합니다.
- A존 서브넷 이름은 skills-priv-a로 설정합니다.
- B존 서브넷 이름은 skills-priv-b로 설정합니다.

### 4. Simple Storage Service

웹서버에 배포될 정적파일 저장을 위하여 AWS의 S3를 구성합니다.

- S3는 아무나 접근 하도록 구성하면 안되고, 필요한 EC2에서만 접근 가능하도록 구성합니다.
- 버킷 이름은 skills-<임의값> 으로 설정합니다. (예, skills-seoul99)
- 제공 받은 파일을 각각 s3://<bucket>/web/v1.tar, s3://<bucket>/web/v2.tar 경로에 업로드 하도록 합니다. 버킷 이름이 skills-seoul99이라면 해당 명령어로 파일 다운로드가 가능해야 합니다. `aws s3 cp s3://skills-seoul99/web/v1.tar`.

### 5. Domain Name Service

생성되는 인프라의 도메인 관리를 위해 AWS의 Route53을 사용합니다. DNS는 VPC 내에서 사용 가능한 private hosted zone을 생성하며, 도메인 이름은 ws.local로 설정합니다.

## 6. Bastion 서버

SSH를 통한 EC2 접근을 위해 Bastion 서버를 생성합니다. 해당 서버를 경유하여 private zone에 위치한 서버로 ssh 접근해야 합니다.

- AWS EC2를 사용하여 인스턴스를 생성합니다.
- bastion 서버는 VPC의 public subnet에 위치합니다.
- 보안을 위해 bastion의 SSH 포트는 2222로 변경합니다.
- "Name": "bastion-skills-ap" 라는 EC2 tag를 추가합니다.
- 외부에서 접근이 가능한 리소스임으로 보안설정에 유의합니다.

## 7. 웹서버 - Stable version

- 웹서버 운영을 위하여 오토스케일링 그룹을 이용해 EC2를 생성합니다.
- Scale-out 되었을 때 별도의 설정 없이 자동으로 웹서버가 구성되어 동작되도록 합니다.
- 해당 EC2는고가용성이 보장되어야 합니다.
- 최소 2대 이상 운영되도록 구성합니다.
- 해당 EC2에 Apache 웹서버를 설치하도록 합니다.
- Apache 웹서버의 listen port는 80으로 설정합니다.
- 제공된 v1.tar 파일의 압축을 푼 파일들을 DocumentRoot에 위치시키도록 합니다.  
아파치 설정을 정상적으로 끝냈다면 local에서 GET http://localhost:80/health 호출시  
"{\"health\": \"UP\"}"라는 응답을 받을 수 있습니다.
- ASG와 EC2에 "Name": "web-skills-ap-stable" 라는 태그를 갖도록 구성합니다.
- 평균 CPU사용률이 10% 이상 높아지면 scale-out을 하도록 오토스케일링을 구성합니다.
- AWS 명령어 이용시 access key 없이, role 베이스로 권한을 획득할 수 있도록 합니다.
- 해당 EC2는 선수가 S3 문제에서 생성한 버킷에 접근 가능해야 합니다.

## 8. 웹서버 - Test version

- 웹서버 운영을 위하여 오토스케일링 그룹을 이용해 EC2를 생성합니다.
- Scale-out 되었을 때 별도의 설정 없이 자동으로 웹서버가 구성되어 동작되도록 합니다.
- 해당 EC2는고가용성이 보장되어야 합니다.
- 최소 2대 이상 운영되도록 구성합니다.
- 해당 EC2에 Apache 웹서버를 설치하도록 합니다.
- Apache 웹서버의 listen port는 80으로 설정합니다.
- 제공된 v2.tar 파일의 압축을 푼 파일들을 DocumentRoot에 위치시키도록 합니다.  
아파치 설정을 정상적으로 끝냈다면 local에서 GET http://localhost:80/health 호출시  
"{\"health\": \"UP\"}" 라는 응답을 받을 수 있습니다.

- ASG와 EC2에 "Name": "web-skills-ap-test" 라는 태그를 갖도록 구성합니다.
- 평균 CPU사용률이 10% 이상 높아지면 scale-out을 하도록 오토스케일링을 구성합니다.
- aws 명령어 이용시 access key 없이, role 베이스로 권한을 획득할 수 있도록 합니다.
- 해당 EC2는 선수가 S3 문제에서 생성한 버킷에 접근 가능해야 합니다.

## 9. Load Balancing

웹서버의 부하분산을 위해 Application Load Balancer를 구성 합니다.

### 9.1. ALB 기본 구성

- 보안을 위하여 인스턴스는 LB에서만 트래픽을 받도록 구성합니다.
- LB는 VPC내 모든 곳에서 트래픽을 받을 수 있습니다.
- Internal ALB를 생성하여 웹서버의 트래픽을 받도록 구성합니다.
- ALB에서 제공하는 CNAME을 아용하여 web.ws.local라는 레코드를 추가합니다.
- ALB의 이름은 "web-cc2021-ap-int"로 지정합니다.
- ALB의 listener 포트는 80으로 지정합니다.
- 최종적으로 Bastion에서 `http://web.ws.local/health` 호출시 `{"health": "UP"}` 이라는 문구가 보여야 합니다.

### 9.2. 개발용 페이지 보안

swagger page는 해당 웹서버 내부에서만 호출이 되어야 합니다.

만약 외부 엔드포인트인 `http://web.ws.local/swagger-ui.html`로 페이지 접근시, EC2 서버로 접근이 불가해야 하고, 404 응답코드를 내려줘야 합니다. Body는 "Not found this WSI page" 라고 표기되어야 합니다.

### 9.3. A/B 테스트

A/B testing을 위하여 `test=true`라는 쿼리 파라미터를 포함하여 `http://web.ws.local`에 호출할 시 Test 웹서버로 호출되고, 해당 쿼리 파라미터 없이 호출된다면 Stable 웹서버로 호출되어야 합니다.

## 10. Monitoring

ALB의 메트릭을 이용하여 모니터링 알람을 구성 합니다. ALB에 연결된 서버에서 리턴하는 HTTP 4XX 값이 1분에 55개 이상으로 높아지면, CloudWatch에서 alert을 볼 수 있도록 구성 합니다. alert 레벨은 "Alarm(경보)" 단계로 설정합니다.

최종적으로 CloudWatch에서 Alert을 확인 할 수 있어야 하며, SNS 토픽 설정 등은 임의로 구성하고, 알람이름은 ALB-4XX-high로 구성합니다.