

2024년도 전국기능경기대회 과제

직 종 명	클라우드컴퓨팅	과제명	Small Challenge	과제번호	제1과제
경기시간	30분	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.

Software Stack

AWS	개발언어/프레임워크
- VPC - EC2 - CloudWatch - CloudTrail	

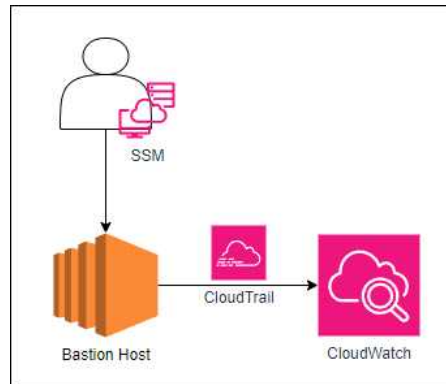
2. 선수 유의사항

※ 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 뜻하므로 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.
- 10) 과제 지에 별다른 요구사항이 없는 경우 선수가 AWS Best Practices를 참고하여 알아서 구성합니다.

8. Cloud governance

Private 형태로 생성된 Bastion Host에 사용자가 SSM을 통해 접근 시 CloudWatch Dashboard에 경보가 발생되도록 구성합니다.



8-1. VPC

VPC의 경우 아래 표를 참고하여 생성합니다.

VPC

Name Tag	CIDR
cg-vpc	10.0.0.0/16

Subnet

Name Tag	CIDR	Availability Zone	Internet Access
cg-public-sn-a	10.0.100.0/24	ap-northeast-2a	Direct Access

8-2. Bastion Host

아래 요구 사항을 참고하여 Bastion Host를 생성합니다. 해당 서버는 채점 시 사용되는 서버이므로, 채점 시 SSH로 접근이 불가능할 경우 불이익을 받을 수 있습니다.

- Name Tag : cg-bastion
- Instance Type : t3.medium
- OS : Amazon Linux 2023
- Policy : Poweruser
- Packages : awscliv2, jq, amazon-ssm-agent

8-3. AWS CloudWatch Dashboard

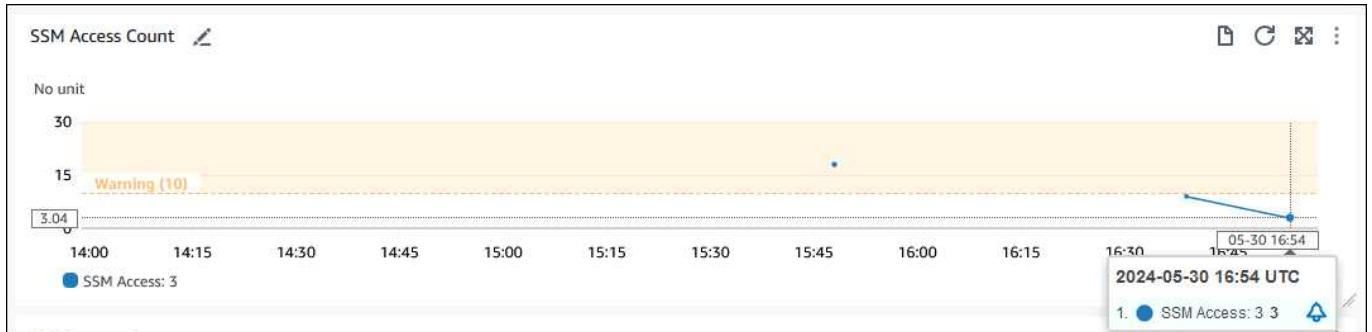
사용자가 Bastion Host에 SSM을 통해 접근 시 해당 Dashboard에 생성된 Widget에서 관련 메트릭, 정보들을 한 눈에 확인이 가능하도록 구성합니다. 단, 이때 CloudTrail만 사용하여 필요한 메트릭 정보를 5분 내에 가져와야합니다.

- Dashboard Name: cg-dashboard

- Widget

1) SSM Access Count Widget

Bastion Host에 SSM 접속한 횟수를 count하여 Line Graph형태로 표현되어야합니다.
또한 그래프의 시각화를 위해 thresholds은 10으로 설정하며, 해당 thresholds에 Warning이라는 주석을 설정합니다.



- Widget Name : SSM Access Count
- Label name : SSM Access: <최근 SSM 접속 횟수>
(e.g 15번 접근 시, SSM Access: 15)

2) SSM Access Logs

Bastion Host에 SSM Access Log를 log table widget을 통해 표현되어야합니다.
아래 요구사항을 참고하여 log table을 구성합니다.

- Widget Name : SSM Access Logs
- log fields : 아래 표를 참고하여 Log table을 구성합니다.

eventTime	eventSource	state	accountId	sessionId
<SSM 접근 시간>	ssm.amazonaws.com	Active	<aws accountid>	<SSM 세션 ID>

#	eventTime	eventSource	state	accountId	sessionId
▶ 1	2024-05-30T16:36:55Z	ssm.amazonaws.com	Active	1101-28	root-v3cvudkads5u6k4jn2iqbv6hoe
▶ 2	2024-05-30T16:36:54Z	ssm.amazonaws.com	Active	1101-28	root-v3cvudkads5u6k4jn2iqbv6hoe
▶ 3	2024-05-30T16:36:53Z	ssm.amazonaws.com	Active	1101-28	root-7kkgrgimfsbqrjvpvgfo6dxhhy
▶ 4	2024-05-30T16:36:53Z	ssm.amazonaws.com	Active	1101-28	root-7kkgrgimfsbqrjvpvgfo6dxhhy
▶ 5	2024-05-30T16:36:53Z	ssm.amazonaws.com	Active	1101-28	root-7kkgrgimfsbqrjvpvgfo6dxhhy
▶ 6	2024-05-30T16:36:52Z	ssm.amazonaws.com	Active	1101-28	root-v3cvudkads5u6k4jn2iqbv6hoe
▶ 7	2024-05-30T16:36:52Z	ssm.amazonaws.com	Active	1101-28	root-t7hruf71xmovpcubo6qqabx65m