

2024 경상북도 제59회 전국기능경기대회 채점기준

1. 채점상의 유의사항	직 종 명	클라우드컴퓨팅
<p>※ 다음 사항을 유의하여 채점하십시오.</p> <ol style="list-style-type: none"> 1) AWS의 지역은 ap-northeast-2을 사용합니다. 2) 웹페이지 접근은 크롬이나 파이어폭스를 이용합니다. 3) 웹페이지에서 언어에 따라 문구가 다르게 보일 수 있습니다. 4) shell에서의 명령어의 출력은 버전에 따라 조금 다를 수 있습니다. 5) 문제지와 채점지에 있는 <> 는 변수입니다. 해당 부분을 변경해 입력합니다. 6) 채점은 문항 순서대로 진행해야 합니다. 7) 삭제된 채점자료는 되돌릴 수 없음으로 유의하여 진행하며, 이의신청까지 완료 이후 선수가 생성한 클라우드 리소스를 삭제합니다. 8) 부분 점수가 있는 문항은 채점 항목에 부분 점수가 적혀져 있습니다. 9) 부분 점수가 따로 없는 문항은 모두 맞아야 점수로 인정됩니다. 10) 리소스의 정보를 읽어오는 채점항목은 기본적으로 스크립트 결과를 통해 채점을 진행하며, 만약 선수가 이의가 있다면 명령어를 직접 입력하여 확인해볼 수 있습니다. 11) [] 기호는 채점에 영향을 주지 않습니다. 12) 명령어 입력 Box 안의 명령줄은 한 줄 명령어입니다. 별도의 지시가 없으면 수정 없이 박스 안의 전체 내용을 복사하고 쉘에 붙여넣어 명령을 실행합니다. 13) (예상 출력)은 바로 이전 (명령어 입력)의 예상 출력을 의미합니다. 		

2. 채점기준표

1) 주요항목별 배점				직 종 명		클라우드컴퓨팅		
과제 번호	일련 번호	주요항목	배점	채점방법		채점시기		비고
				독립	합의	경기 진행중	경기 종료후	
제1과제	1	네트워크 구성	0.75		○		○	
	2	Bastion 서버	0.5		○		○	
	3	웹 어플리케이션	0.5		○		○	
	4	OpenSearch	2		○		○	
합 계			3.75					

2) 채점방법 및 기준

과제 번호	일련 번호	주요항목	일련 번호	세부항목(채점방법)	배점
1과제	1	네트워크 구성	1	VPC 확인	0.25
			2	Subnets 확인	0.25
			3	RouteTables 확인	0.25
	2	Bastion 서버	1	인스턴스 타입 확인	0.25
			2	Bastion EC2 Public IP 확인	0.25
	3	웹 어플리케이션	1	API 요청 확인	0.5
	4	OpenSearch	1	도메인 확인	0.2
			2	세부설정 확인	0.8
			3	로그 확인	1
	총점				3.75

3) 채점내용

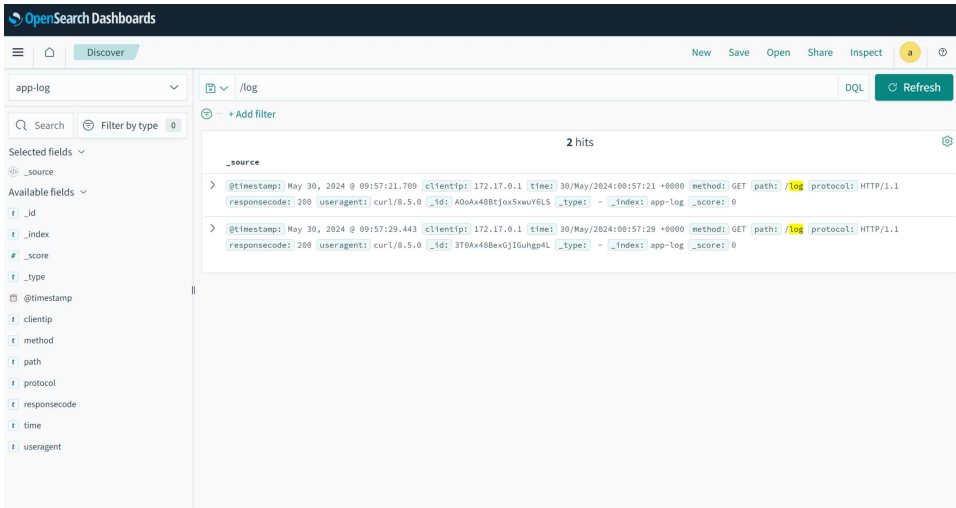
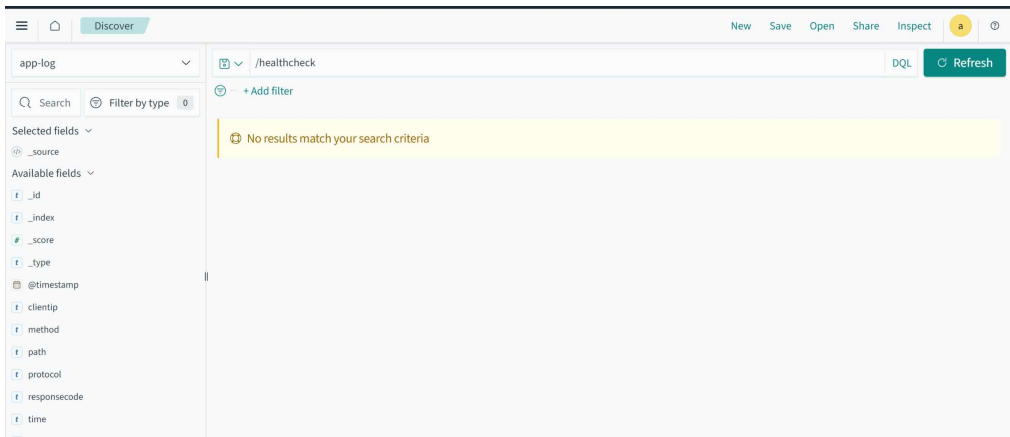
순번	사전준비
0	<p>1) Bastion 서버에 SSH를 통해 접근합니다. (별도 명시가 없는 경우 모든 채점은 Bastion 서버에서 진행합니다.)</p> <p>2) Bastion 명령어 및 권한을 확인합니다. (awscli permission, jq, curl, awscli region)</p> <p>3) 채점 스크립트들을 /root/marking에 다운로드 합니다.</p> <p>4) /root/marking 경로에서 스크립트를 실행합니다. 실행 결과를 기반으로 채점을 진행하되 선수가 이의를 제기할 경우 수동으로 채점을 진행할 수 있도록 합니다.</p> <p>5) 채점을 진행하는 Bastion 서버의 셸을 초기 실행할 때 다음 명령어를 실행하여 환경 변수를 초기화합니다. (채점 스크립트로 진행 시 생략)</p> <p>6) 4-3번은 수동으로 채점합니다.</p>
	<pre># set default region of aws cli aws configure set default.region ap-northeast-2</pre>

순번	채점 항목	
1-1	1-1-A (명령어 입력)	aws ec2 describe-vpcs --filter Name=tag:Name,Values=ws-i-vpc \ --query "Vpcs[].CidrBlock"
	1-1-A (예상 출력)	10.0.0.0/16
1-2	1-2-A (명령어 입력)	aws ec2 describe-subnets --filter Name=tag:Name,Values=ws-i-public-a \ --query "Subnets[].[AvailabilityZone, CidrBlock][]" ₩ ; aws ec2 describe-subnets --filter Name=tag:Name,Values=ws-i-public-b \ --query "Subnets[].[AvailabilityZone, CidrBlock][]" ₩ ; aws ec2 describe-subnets --filter Name=tag:Name,Values=ws-i-private-a \ --query "Subnets[].[AvailabilityZone, CidrBlock][]" ₩ ; aws ec2 describe-subnets --filter Name=tag:Name,Values=ws-i-private-b \ --query "Subnets[].[AvailabilityZone, CidrBlock][]"
	1-2-A (예상 출력) <u>정확히 일치</u> <u>순서 중요</u>	["ap-northeast-2a", "10.0.1.0/24"] ["ap-northeast-2b", "10.0.2.0/24"] ["ap-northeast-2a", "10.0.3.0/24"] ["ap-northeast-2b", "10.0.4.0/24"]

순번	채점 항목	
1-3	1-3-A (명령어 입력)	aws ec2 describe-route-tables --filter Name=tag:Name,Values=ws1-public-rtb \ --query "RouteTables[].Routes[].GatewayId" \ ; aws ec2 describe-internet-gateways --filter Name=tag:Name,Values=ws1-igw \ --query "InternetGateways[].InternetGatewayId"
	1-3-A (예상 출력)	["local", "igw-"로 시작하는 문자열] ["igw-"로 시작하는 문자열] "igw-"로 시작하는 문자열 두 개가 동일한지 확인
	1-3-B (명령어 입력)	aws ec2 describe-route-tables --filter Name=tag:Name,Values=ws1-private-a-rtb \ --query "RouteTables[].Routes[].NatGatewayId" \ ; aws ec2 describe-nat-gateways --filter Name=tag:Name,Values=ws1-nat-a \ --query "NatGateways[].NatGatewayId"
	1-3-B (예상 출력)	["nat-" 로 시작하는 문자열] ["nat-" 로 시작하는 문자열] "nat-" 로 시작하는 문자열 두 개가 동일한지 확인
	1-3-C (명령어 입력)	aws ec2 describe-route-tables --filter Name=tag:Name,Values=ws1-private-b-rtb \ --query "RouteTables[].Routes[].NatGatewayId" \ ; aws ec2 describe-nat-gateways --filter Name=tag:Name,Values=ws1-nat-b \ --query "NatGateways[].NatGatewayId"
	1-3-C (예상 출력)	["nat-" 로 시작하는 문자열] ["nat-" 로 시작하는 문자열] "nat-" 로 시작하는 문자열 두 개가 동일한지 확인

순번	채점 항목	
2-1	2-1-A (명령어 입력)	aws ec2 describe-instances --filter Name=tag:Name,Values=ws-i-bastion \ --query "Reservations[].Instances[].InstanceType"
	2-1-A (예상 출력)	["t3.small"]
2-2	2-2-A (명령어 입력)	aws ec2 describe-instances --filter Name=tag:Name,Values=ws-i-bastion --query "Reservations[].Instances[].PublicIpAddress" aws ec2 describe-addresses --query "Addresses[].PublicIp"
	2-2-A (예상 출력)	["15.164.148.30"] ["15.164.148.30"] 첫 번째로 출력된 아이피가 두 번째 출력에 존재하는지 확인
3-1	3-1-A (명령어 입력)	APP_PRIVATE_IP=\$(aws ec2 describe-instances --filters "Name=tag:Name,Values=ws-i-app" --query "Reservations[*].Instances[*].PrivateIpAddress" --output text) aws ec2 describe-instances --filters "Name=tag:Name,Values=ws-i-app" --query "Reservations[*].Instances[*].PrivateIpAddress" curl \$APP_PRIVATE_IP:5000/log
	3-1-A (예상 출력)	Log entry created
4-1	4-1-A (명령어 입력)	aws opensearch list-domain-names grep ws-i-opensearch
	4-1-A (예상 출력)	"DomainName": "ws-i-opensearch" 클라우드컴퓨팅 제2과제 채점기준 9 - 7

순번	채점 항목	
4-2	4-2-A (명령어 입력)	aws opensearch describe-domain --domain-name wsi-opensearch --query "DomainStatus.ClusterConfig.[InstanceCount, DedicatedMasterCount]"
	4-2-A (예상 출력)	[2, 3]
	4-1-B (명령어 입력)	aws opensearch describe-domain --domain-name wsi-opensearch --query "DomainStatus.EngineVersion"
	4-1-B (명령어 입력)	"OpenSearch_2.13"
	4-2-C (명령어 입력)	OPENSEARCH_ENDPOINT=\$(aws opensearch describe-domain --domain-name wsi-opensearch jq -r '.DomainStatus.Endpoint') curl -s -u admin:Password01! "https://\$OPENSEARCH_ENDPOINT/_cat/indices?index=app-log"
	4-2-C (예상 출력)	green open app-log dWxHtcnyQcGsMwhGB0FMYw 5 1 2 0 34kb 17kb 위와 같이 app-log가 포함된 출력이 있는지 확인
	4-2-D (명령어 입력)	OPENSEARCH_ENDPOINT=\$(aws opensearch describe-domain --domain-name wsi-opensearch jq -r '.DomainStatus.Endpoint') curl -s -u admin:Password01! https://\$OPENSEARCH_ENDPOINT/app-log jq '.["app-log"].mappings.properties keys[]'
	4-2-D (예상 출력)	"clientip" "method" "path" "protocol" "responsecode" "time" "useragent" 위와 같이 clientip, method, path, protocol, responsecode, time, useragent가 출력되는지 확인

순번	채점 항목	
4-3	4-3-A (명령어 입력)	aws opensearch describe-domain --domain-name wsi-opensearch --output json jq -r '.DomainStatus.Endpoint + "/_dashboards"'
	4-3-A (예상 출력)	대시보드 URL이 출력됩니다.
	4-3-B (대시보드 접속)	출력된 URL에 브라우저로 접속합니다. 아이디는 admin 패스워드는 Password01!로 로그인합니다. 대시보드의 discover탭에 접속합니다. index는 app-log로 지정합니다.
	4-3-B (대시보드 확인)	search에 /log를 입력합니다.
	4-3-B (예상 출력)	 <p>로그가 출력되는지 확인합니다.</p>
	4-3-C (대시보드 확인)	search에 /healthcheck를 입력합니다.
	4-3-C (예상 출력)	 <p>출력되는 로그가 없는지 확인합니다.</p>