2024년도 전국기능경기대회 채점기준

1. 채점상의 유의사항	직 종 명	클라우드컴퓨팅

※ 다음 사항을 유의하여 채점하시오.

1) AWS 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, 이의 신청까지 완료 이후 선수가 생성한 클라우드 리소스를 삭제합니다.
8) 부분 점수가 있는 문항은 채점 항목에 부분 점수가 적혀저 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	
제2과제	1	EC2	0.6		○		○	
	2	Config	0.65		○		○	
	3	CloudWatch	0.4		○		○	
	4	Movement	2.1		○		○	
합 계			3.75					

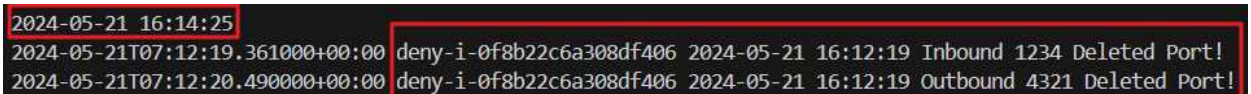
2) 채점방법 및 기준

과제 번호	일련 번호	주요항목	일련 번호	세부항목(채점방법)	배점
제2과제	1	EC2	1	EC2 생성 확인	0.2
			2	Security Group Port 확인	0.4
	2	Config	1	Config Rule 생성 확인	0.2
			2	Config Rule 상태 확인	0.45
	3	CloudWatch	1	Log Group 생성 확인	0.2
			2	Log Stream 생성 확인	0.2
	4	Movement	1	Security Group Revoke 확인	0.7
			2	Loggig 확인	0.7
			3	Config Rule 결과값 확인	0.7
	총점				3.75

3) 채점 내용

순번	채점 항목
0	1) SSH를 통해 EC2에 접근합니다. (awscli, permission, jq, curl, awscli region) 2) 아래 파일들을 EC2의 /root/marking 디렉터리로 복사합니다. - mark.sh 3) /root/marking 경로에서 스크립트를 실행합니다. 실행 결과를 기반으로 채점을 진행하되 선수가 이의를 제거할 경우 수동으로 채점을 진행할 수 있도록 합니다. 4) 채점을 진행하기 전에 다음 명령어를 수행하여 채점 진행을 위한 사전 작업을 진행합니다. (채점 스크립트로 진행 시 생략)
	# set default region of aws cli aws configure set default.region ap-northeast-2 # set default output of aws cli aws configure set default.output json

순번	채점 항목
1-1	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어 입력 후 “i-”가 출력되는지 확인합니다. aws ec2 describe-instances --filter Name=tag:Name,Values=wsi-app-ec2 -query 'Reservations[].Instances[].InstanceId'
1-2	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어를 입력합니다. EC2_SG_ID=$(aws ec2 describe-instances --filter Name=tag:Name,Values=wsi-app-ec2 W --query "Reservations[].Instances[].SecurityGroups[].GroupId[]" --output text) 3) 아래 명령어를 입력 후 22, 80이 출력되는지 확인합니다. 출력 될 시 0.2점 aws ec2 describe-security-groups --group-id $EC2_SG_ID W --query "SecurityGroups[].IpPermissions[].FromPort “ 3) 아래 명령어를 입력합니다. EC2_SG_ID=$(aws ec2 describe-instances --filter Name=tag:Name,Values=wsi-app-ec2 W --query "Reservations[].Instances[].SecurityGroups[].GroupId[]" --output text) 4) 아래 명령어 입력 후 22, 80, 4430이 출력되는지 확인합니다. 출력 될 시 0.2점 aws ec2 describe-security-groups --group-id $EC2_SG_ID W --query "SecurityGroups[].IpPermissionsEgress[].FromPort"
2-1	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어 입력 후 “wsi-config-port”가 출력되는지 확인합니다. aws configservice describe-config-rules --config-rule-names wsi-config-port W --query "ConfigRules[].ConfigRuleName “
2-2	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어 입력 후 “COMPLIANT”가 출력되는지 확인합니다. aws configservice get-compliance-details-by-config-rule -config-rule-name wsi-config-port W --query "EvaluationResults[].ComplianceType"
3-1	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어를 입력 후 “/ec2/deny/port”가 출력되는지 확인합니다. aws configservice get-compliance-details-by-config-rule -config-rule-name wsi-config-port W --query "EvaluationResults[].ComplianceType “

순번	채점 항목
3-2	1) SSH를 통해 EC2에 접근합니다. 2)아래 명령어 입력합니다. CW_LOG_STREAM_NAME=$(aws logs describe-log-streams --log-group-name /ec2/deny/port W --query "logStreams[].logStreamName" --output text) EC2_ID=$(aws ec2 describe-instances --filter "Name=tag:Name,Values=wsi-app-ec2" W --query "Reservations[].Instances[].InstanceId" --output text) MATCHING_LOG_STREAM_NAME="deny-$EC2_ID" 3) 아래 명령어를 입력 후 “deny-{instance_Id}”가 출력되는지 확인합니다. **{instance_id}는 해당 EC2 ID를 의미하며, 선수마다 값이 다를 수 있습니다.** ["$CW_LOG_STREAM_NAME" == "$MATCHING_LOG_STREAM_NAME"] && aws logs describe-log-streams W --log-group-name /ec2/deny/port -query "logStreams[].logStreamName “
4-1	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어를 입력합니다. EC2_SG_ID=$(aws ec2 describe-instances --filter Name=tag:Name,Values=wsi-app-ec2 W --query "Reservations[].Instances[].SecurityGroups[].GroupId[]" --output text) aws ec2 authorize-seecurity-group-ingress --group-id $EC2_SG_ID --protocol tcp W --port 1234 --cidr 0.0.0.0/0 > /dev/null 2>&1 aws ec2 authorize-security-group-egress --group-id $EC2_SG_ID --protocol tcp W --port 4321 --cidr 0.0.0.0/0 > /dev/null 2>&1 sleep 180 **최대 3분까지 기다린 후 입력할 수 있습니다.** 3) 아래 명령어를 입력 후 22, 80이 출력되는지 확인합니다. aws ec2 describe-security-groups --group-id $EC2_SG_ID W --query "SecurityGroups[].IpPermissions[].FromPort “ 4) 아래 명령어 입력 후 22, 80, 4430이 출력되는지 확인합니다. aws ec2 describe-security-groups --group-id $EC2_SG_ID W --query "SecurityGroups[].IpPermissionsEgress[].FromPort"
4-2	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어를 입력합니다. date -d "+9 hours" "+%Y-%m-%d %H:%M:%S" aws logs tail /ec2/deny/port | tail -n 2  3)로깅 시간이 위에 출력된 시간과 유사하며, “<년-월-일 시:분:초> <Security Group Rule> <Port> Deleted Port!” 라는 문구가 있는지 확인합니다. 오차는 3분 이내까지 허용합니다.

순번	채점 항목
4-3	1) SSH를 통해 EC2에 접근합니다. 2) 아래 명령어를 입력 후 “COMPLIANT”가 출력되는지 확인합니다. aws configservice get-compliance-details-by-config-rule --config-rule-name wsi-config-port W --query "EvaluationResults[].ComplianceType"