2023 충청남도 제58회 전국기능경기대회 채점기준

1. 채점상의 유의사항	직 종 명	클라우드컴퓨팅

※ 다음 사항을 유의하여 채점하시오.

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.

1) Bastion 서버에 SSH를 통해 접근합니다. (별도 명시가 없는 경우 모든 채점은 Bastion 서버에서 진행합니다.)

2) Bastion 명령어 및 권한을 확인합니다. (awscli permission, jq, curl, awscli region)

3) mark 스크립트들을 /root/mark에 다운로드 합니다.

4) /root/mark 경로에서 스크립트를 실행합니다. 실행 결과를 기반으로 채점을 진행하되 선수가 이의를 제기할 경우 수동으로 채점을 진행할 수 있도록 합니다.

5) 채점을 진행하는 Bastion 서버의 쉘을 초기 실행할 때 다음 명령어을 실행하여 환경 변수를 초기화합니다. (**채점 스크립트로 진행 시 생략**)

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	IAM	0.9		○		○	
	2	Monitering service Name	0.65		○		○	
	3	Lambda	0.2		○		○	
	4	Employee - movement	1.0		○		○	
	5	Admin - movement	1.0		○		○	
합 계			3.75					

2) 채점방법 및 기준

과제 번호	일련 번호	주요항목	일련 번호	세부항목(채점방법)	배점
2과제	1	IAM	1	User Name	0.2
			2	User policy	0.25
			3	instance role Name	0.2
			4	instance role policy	0.25
	2	Monitering service Name	1	CloudTrail Name	0.2
			2	CloudWatch Alarm Name	0.25
			3	CloudWtach Log Group Name	0.2
	3	Lambda	1	Lambda name	0.2
	4	Employee - movement	1	Employee - Alarm	0.5
			2	Employee - instance role policy test	0.5
	5	Admin - movement	1	Admin - Alarm	0.5
			2	Admin - instance role policy test	0.5
	총점				3.75

3) 채점내용

순번	채점 항목	
1-1	1-1-A (명령어 입력)	aws iam list-users --query "Users[?UserName=='Admin'].UserName" aws iam list-users --query "Users[?UserName=='Employee'].UserName"
	1-2-A (예상 출력) **정확히 일치**	["Admin"], [" Employee"]

순번	채점 항목	
1-2	1-2-A (명령어 입력)	aws iam list-attached-user-policies --user-name Admin aws iam list-attached-user-policies --user-name Employee

	1-2-A
	(예상 출력)
	정확히 일치
		{
		"AttachedPolicies": [
		{
		"PolicyName": "AdministratorAccess",
		"PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
		}
		]
		},
		{
		"AttachedPolicies": [
		{
		"PolicyName": "IAMFullAccess",
		"PolicyArn": "arn:aws:iam::aws:policy/IAMFullAccess"
		}
		]
		}

1-3	1-3-A (명령어 입력)	aws iam get-role --role-name wsc2024-instance-role --query 'Role.RoleName'
	1-3-A (예상 출력) **정확히 일치**	"wsc2024-instance-role"

순번	채점 항목	
1-4	1-4-A (명령어 입력)	aws iam list-attached-role-policies --role-name wsc2024-instance-role --query "AttachedPolicies[].PolicyArn"
	1-4-A (예상 출력) **정확히 일치**	["arn:aws:iam:aws:policy/AmazonSSMManagedInstanceCore"]
2-1	2-1-A (명령어 입력)	aws cloudtrail describe-trails --trail-name-list wsc2024-CT --query "trailList[].Name
	2-1-A (예상 출력) **정확히 일치**	["wsc2024-CT"]
2-2	2-2-A (명령어 입력)	aws cloudwatch describe-alarms --alarm-name-prefix wsc2024-gvn-alarm --query 'MetricAlarms[*].AlarmName
	2-2-A (예상 출력) **정확히 일치**	["wsc2024-gvn-alarm"]
2-3	2-3-A (명령어 입력)	aws logs describe-log-groups --log-group-name-prefix wsc2024-gvn-LG --query 'logGroups[].logGroupName' --output text
	2-3-A (예상 출력) **정확히 일치**	wsc2024-gvn-LG

순번	채점 항목	
3-1	3-1-A (명령어 입력)	aws lambda list-functions --query 'Functions[].FunctionName'
	3-1-A (예상 출력) **정확히 일치**	["wsc2024-gvn-Lambda"]
4-1	4-1-A (명령어 입력)	USERNAME="Employee" CREATED_KEYS=$(aws iam create-access-key --user-name "$USERNAME") ACCESS_KEY_ID=$(echo "$CREATED_KEYS" | jq -r '.AccessKey.AccessKeyId') SECRET_ACCESS_KEY=$(echo "$CREATED_KEYS" | jq -r '.AccessKey.SecretAccessKey') aws configure set aws_access_key_id "$ACCESS_KEY_ID" aws configure set aws_secret_access_key "$SECRET_ACCESS_KEY" sleep 10 aws iam attach-role-policy --role-name wsc2024-instance-role --policy-arn arn:aws:iam::aws:policy/AdministratorAccess rm -rf ~/.aws/* timeout 180 bash -c 'while ["$(aws cloudwatch describe-alarms --alarm-names "wsc2024-gvn-alarm" --query "MetricAlarms[0].StateValue" --output text)" != "ALARM"]; do echo "Waiting for alarm to enter ALARM state..."; sleep 30; done; echo "Alarm is now in ALARM state."
	4-1-A (예상 출력) **밑줄 부분 일치**	Wating for alarm to enter ALARM state... Wating for alarm to enter ALARM state... Wating for alarm to enter ALARM state... Wating for alarm to enter ALARM state... **Alarm is now in ALARM state.**

순번	채점 항목	
4-2	4-2-A (명령어 입력)	aws iam list-attached-role-policies --role-name wsc2024-instance-role

	4-2-A
	(예상 출력)
	정확히 일치
		{
		"AttachedPolicies": [
		{
		"PolicyName": "AmazonSSMManagedInstanceCore",
		"PolicyArn":
		"arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
		}
		]
		}

5-1	5-1-A (명령어 입력)	USERNAME="Admin" CREATED_KEYS=$(aws iam create-access-key --user-name "$USERNAME") ACCESS_KEY_ID=$(echo "$CREATED_KEYS" | jq -r '.AccessKey.AccessKeyId') SECRET_ACCESS_KEY=$(echo "$CREATED_KEYS" | jq -r '.AccessKey.SecretAccessKey') aws configure set aws_access_key_id "$ACCESS_KEY_ID" aws configure set aws_secret_access_key "$SECRET_ACCESS_KEY" sleep 10 aws iam attach-role-policy --role-name wsc2024-instance-role --policy-arn arn:aws:iam::aws:policy/AdministratorAccess sleep 180 && aws cloudwatch describe-alarms --alarm-names "wsc2024-gvn-alarm" --query "MetricAlarms[0].StateValue" --output text
	5-1-A (예상 출력) **ALARM 상태가 아닌지만 확인**	INSUFFICIENT_DATA OK

순번	채점 항목	
5-2	5-2-A (명령어 입력)	aws iam list-attached-role-policies --role-name wsc2024-instance-role

	5-2-A
	정확히 일치
		{
		"AttachedPolicies": [
		{
		"PolicyName": "AmazonSSMManagedInstanceCore",
		"PolicyArn":
		"arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
		}
		]
		},
		{
		"AttachedPolicies": [
		{
		"PolicyName": "AdministratorAccess",
		"PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
		}
		]
		}