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) 채점 내용의 $ 기호는 명령어에 포함되는 것이 아니라 쉘을 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	
제3과제	1	컨테이너 이미지 빌드	5		○		○	
	2	S3 Data Protect	5		○		○	
	3	IAM Permission	5		○		○	
	4	IaC	5		○		○	
합 계			20					

2) 채점방법 및 기준

과제 번호	일련 번호	주요항목	일련 번호	세부항목(채점방법)	배점
3과제	1	컨테이너 이미지 빌드	1	foo repository 확인	0.5
			2	푸쉬 스크립트 확인	1.5
			3	컨테이너 이미지 빌드/동작 확인	1.5
			4	컨테이너 이미지 취약점 확인	1.5
	2	S3 Data Protect	1	S3 버킷 확인	0.5
			2	기존 데이터 확인	1.5
			3	Macie Job 확인	1.5
			4	변경 데이터 확인	1.5
	3	IAM Permission	1	red-user 로그인 확인	1
			2	red-user 일반 권한 확인	1
			3	red-user RunInstance 권한 확인 (실패)	1.5
			4	red-user RunInstance 권한 확인 (성공)	1.5
	4	IaC	1	Cloudformation stack 생성 확인	0.5
			2	S3 버킷 확인	1.5
			3	S3 버킷 구성 확인	1.5
			4	KMS Key 확인	1.5
	총점				20

3) 채점내용

순번	사전준비
0	1) bastion 명령어 및 권한 확인(awscli permission, jq, curl, awscli region) 2) marking 스크립트들을 /root/marking에 다운로드 합니다.

순번	채점 항목
1-1	- AWS 콘솔에서 ECR에 접근하여 foo 이름을 가진 repository가 존재하는 지 확인합니다. - AWS 콘솔에서 ECR에 접근하여 foo 이름을 가진 repository에 scan-on-push 기능이 켜져 있는 지 확인합니다.
1-2	- Bastion 서버에 ssh를 통하여 ec2-user 계정으로 접근 후 root 계정으로 전환합니다. - /home/ec2-user/container 경로로 이동합니다. $ cd /home/ec2-user/container - ./build.sh 명령어를 입력하여 스크립트를 실행합니다. $ ./build.sh - AWS 콘솔에서 ECR에 접근하여 foo 이름을 가진 repository에 현재 시간대의 태그를 가진 이미지가 업로드 되는 것을 확인합니다. 최대 5분까지 대기할 수 있습니다.
1-3	- Bastion 서버에 ssh를 통하여 ec2-user 계정으로 접근 후 root 계정으로 전환합니다. - 아래 명령어를 수행하여 컨테이너를 실행합니다. (<time>부분은 1-2의 이미지 태그로 대체) $ docker run -d -p 8080:8080 foo:<time> curl -X GET -w "₩n%{http_code}₩n" http://localhost:8080/v1/foo - 다음과 같은 출력을 확인합니다. {"application":"foo"} 200
1-4	- AWS 콘솔에서 ECR에 접근하여 foo 이름을 가진 repository에 현재 시간대의 태그를 가진 이미지가 취약점이 0개임을 확인합니다.
2-1	- AWS 콘솔에서 S3에 접근하여 2개의 S3 버킷이 생성된 것을 확인합니다. wsi-day3-private-<임의의 영문 4자리> wsi-day3-public-<임의의 영문 4자리>
2-2	- wsi-day3-private-<임의의 영문 4자리> 버킷에서 employee024.csv 파일을 다운로드 받습니다. - birthday, name, licensenumber, gender, epid 컬럼이 존재하는 것을 확인합니다.
2-3	- AWS 콘솔에서 Macie에 접근하여 하나 이상의 Job이 실행된 것을 확인합니다.
2-4	- wsi-day3-public-<임의의 영문 4자리> 버킷에서 employee024.csv 파일을 다운로드 받습니다. - birthday, name, gender 컬럼만 존재하는 것을 확인합니다.
3-1	- AWS 콘솔에서 red-user 사용자로 정상적으로 로그인합니다. - 정상적으로 로그인되는지 확인합니다.
3-2	- AWS 콘솔에서 ec2에 접근하여 wsi-bastion 인스턴스가 리스트에 보이는지 확인합니다. - AWS 콘솔에서 ec2에 접근하여 wsi-bastion 인스턴스의 인스턴스 타입이 보이는지 확인합니다.

순번	채점 항목
3-3	- AWS 콘솔에서 임의의 ec2 인스턴스 생성을 시도합니다. (태그 정보는 key=project, value=blue 로 설정합니다.) -> 인스턴스가 생성되지 않고 에러가 발생하는 것을 확인합니다.
3-4	- AWS 콘솔에서 임의의 ec2 인스턴스 생성을 시도합니다. (태그 정보는 key=project, value=red 로 설정합니다.) -> 인스턴스가 정상적으로 생성되어야 합니다.
4-1	- AWS 콘솔에서 Cloudformation에 접근하여 day3-wsi-s3-bucket-stack 스택의 상태가 CREATE_COMPLETE 또는 UPDATED_COMPLETE 상태임을 확인합니다.
4-2	- AWS 콘솔에서 S3에 접근하여 S3 버킷을 확인합니다. day3-wsi-temp-bucket-<임의의 영문 4자리>
4-3	- AWS 콘솔에서 S3에 접근하여 S3 속성을 확인합니다. - Default encryption 항목의 Encryption Type이 SSE-KMS로 설정된 것을 확인합니다.
4-4	- AWS 콘솔에서 KMS에 접근하여 Customer managed key를 확인합니다. - day3-wsi-temp-bucket-<임의의 영문 4자리> Alias를 가진 CMK가 있음을 확인합니다.