

2024년도 전국기능경기대회 채점기준

1. 채점상의 유의사항	직 종 명	클라우드컴퓨팅
<p>※ 다음 사항을 유의하여 채점하십시오.</p> <ol style="list-style-type: none"> 1) AWS의 리전은 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) 삭제 채점은 되돌릴 수 없으므로 유의하여 진행합니다. 8) 이의신청까지 완료 이후 선수가 생성한 클라우드 리소스를 삭제합니다. 9) 부분 점수가 있는 문항은 채점 항목에 부분 점수가 적혀져 있습니다. 10) 부분 점수가 따로 없는 문항은 전체 다 맞아야 점수로 인정됩니다. 11) 채점 진행 전 환경 셋업을 위해 다음 사항을 확인해야 합니다. <ul style="list-style-type: none"> - Bastion에 SSH로 접근할 수 있는지 확인합니다. - Bastion 접근 할 때 포트 2220으로 접속했는지 확인합니다. - Bastion에서 AWS CLI v2, curl, jq가 설치되어 있는지 확인합니다. - Bastion에서 IAM Role이 매핑되어 AWS CLI로 AWS의 모든 리소스에 접근 가능한지 확인합니다. - <code>aws sts get-caller-identity</code> 명령을 통해 선수의 계정이 아닌 다른 계정에 접근하고 있는지 확인합니다. 만약, 다른 계정이라면 부정행위를 의심할 수 있습니다. 12) 채점 전 채점환경 구성을 위해 ~/.aws/config 에 아래 내용이 추가되도록 합니다. <pre>[default] region = ap-northeast-2 output = json</pre> 13) 채점 시에는 별도로 제공한 채점 스크립트(mark.sh)를 실행하여 채점할 수 있습니다. 다만, 선수가 직접 입력을 원할 경우 채점기준표에 명시된 명령어 그대로 입력하여 채점할 수 있습니다. 		

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	0.5		○		○	
	2	IAM	0.5		○		○	
	3	CloudTrail	0.5		○		○	
	4	CloudWatch	1.75		○		○	
	5	Lambda	0.5		○		○	
합 계			3.75					


2) 채점방법 및 기준

과제 번호	일련 번호	주요항목	일련 번호	세부항목(채점방법)	배점
2과제	1	EC2	1	EC2 Server Configuration	0.5
	2	IAM	1	IAM User	0.5
	3	CloudTrail	1	Trailing	0.5
	4	CloudWatch	1	User Login	0.5
			2	Login Log	1.25
	5	Lambda	1	Lambda Configuration	0.5
총점					3.75

3) 채점내용

채점 항목		
1-1	1-1A (명령어 입력)	<pre>aws ec2 describe-instances --filters "Name=tag:Name,Values=wsj-bastion-ec2" --query "Reservations[*].Instances[*].[InstanceId, InstanceType, IamInstanceProfile.Arn]" --output text awk '{print \$1,\$2,\$3}' xargs -l {} bash -c 'INSTANCE_PROFILE_NAME=\$(echo {} awk -F"/" '{print W\$NF}'); ROLE_NAME=\$(aws iam get-instance-profile --instance-profile-name \$INSTANCE_PROFILE_NAME --query "InstanceProfile.Roles[*].RoleName" --output text); echo "Instance ID: \$(echo {} awk "{print W\$1}"); echo "Instance Type: \$(echo {} awk "{print W\$2}"); aws iam list-attached-role-policies --role-name \$ROLE_NAME --query "AttachedPolicies[*].[PolicyName, PolicyArn]" --output text'</pre>
	1-1-A (예상 출력) <u>정확히</u> <u>일치</u> <u>순서 중요</u>	<pre>Instance ID: i-xxxxxxxxxxxxxxxxxxxxxxxxx Instance Type: t3.small AdministratorAccess arn:aws:iam::aws:policy/AdministratorAccess</pre>
2-1	2-1A (명령어 입력)	<pre>aws iam get-user --user-name wsi-project-user --query "User.UserName" --output text W ; aws iam list-attached-user-policies --user-name wsi-project-user --query 'AttachedPolicies[*].PolicyName' --output text && aws iam list-user-policies --user-name wsi-project-user --query 'PolicyNames' --output text</pre>
	2-1-A (예상 출력) <u>정확히</u> <u>일치</u> <u>순서 중요</u>	<pre>wsi-project-user AdministratorAccess</pre>

3-1	3-1A (명령어 입력)	aws cloudtrail describe-trails --query 'trailList[?Name=='wsi-project-trail'].Name' --output json
	3-1-A (예상 출력) <u>정확히</u> <u>일치</u> <u>순서 중요</u>	["wsi-project-trail"]

4-1	4-1A	계정에 로그아웃 후 생성했던 IAM 사용자로 로그인합니다.
	4-1-A	 <p>The screenshot shows the AWS IAM console login page. At the top is the AWS logo. Below it is the heading 'IAM 사용자로 로그인'. There are three input fields: '계정 ID(12자리) 또는 계정 별칭' with the value '12341234', '사용자 이름:' with the value 'wsi-project-user', and '암호:' with masked characters. Below the password field is a checkbox labeled '이 계정 기억하기'. At the bottom is a blue '로그인' button. Below the button are two links: '루트 사용자 이메일을 사용하여 로그인' and '암호 찾기'.</p>

4-2	4-2A (명령어 입력)	로그인 후 4분 소요 aws logs describe-log-groups --log-group-name-prefix wsi-project-login --query 'logGroups[?logGroupName==`wsi-project-login`].logGroupName' --output json ₩ ; LATEST_LOG_STREAM=\$(aws logs describe-log-streams --log-group-name \$LOG_GROUP_NAME --order-by LastEventTime --descending --limit 1 --query 'logStreams[0].logStreamName' --output text) && aws logs get-log-events --log-group-name \$LOG_GROUP_NAME --log-stream-name \$LATEST_LOG_STREAM --limit 100 --query 'events[*].message' --output json
	4-2-A (예상 출력) <u>timestamp</u> <u>확인하여</u> <u>4분내에</u> <u>포함되어있</u> <u>는지 확인</u>	["wsi-project-login"] ["{₩"USER₩": ₩"wsi-project-user has logged in!₩"}", "{₩"USER₩": ₩"wsi-project-user has logged in!₩"}"]
5-1	5-1A (명령어 입력)	aws lambda get-function --function-name wsi-project-log-function --query 'Configuration.FunctionName' --output json
	5-1-A (예상 출력) <u>정확히</u> <u>일치</u> <u>순서 중요</u>	"wsi-project-log-function"