2025년도 전국기능경기대회

직 종 명	클라우드컴퓨팅	과제명	Trouble-shooting	과제번호	제 3과제
경기시간	2시간	비 번 호		심사위원 확인	(인)

1. 요구사항

본 과제는 AWS EKS 클러스터 환경에서 발생할 수 있는 트러블슈팅 문제를 다루며, 다음 세 가지 항목으로 구성됩니다.

1-1. VPC CNI Setting Problems

1-2. Pod IAM Problems

1-3. Node Shutdown Problems

S/W Stack

trouble-shooting으로 미제공

2. 선수 유의사항

1) 기계 및 공구 등의 사용 시 안전에 유의하시고, 필요 시 안전장비 및 복장 등을 착용하여 사고를 예방하여 주시기 바랍니다.

2) 작업 중 화상, 감전, 찰과상 등 안전사고 예방에 유의하시고, 공구나 작업도구 사용 시 안전보호구 착용 등 안전수칙을 준수하시기 바랍니다.

3) 작업 중 공구의 사용에 주의하고, 안전수칙을 준수하여 사고를 예방하여 주시기 바랍니다.

4) 경기 시작 전 가벼운 스트레칭 등으로 긴장을 풀어주시고, 작업도구의 사용 시 안전에 주의하십시오.

5) 선수의 계정에는 비용의 제한이 존재하며, 이보다 더 높게 요금이 부과될 시 계정 사용이 불가능할 수 있습니다.

6) 만약 문제에서 <>가 나온다면, 이는 변수를 뜻함으로 선수가 적절히 변경하여 사용해야 합니다.

7) 과제의 Bastion 서버가 항상 실행 중이어야 하며, 별도 언급이 없는 경우 채점은 Bastion 서버에 SSH로 접속하거나, AWS CLI명령어를 통해 진행되므로 적절한 IAM Role을 EC2 인스턴스에 할당해야 합니다.

8) Bastion 서버 외에도 EKS 클러스터 및 노드 그룹 상태가 정상이어야 하며, 노드가 NotReady이거나 삭제된 경우 채점이 불가능합니다.

9) 문제에서 요구하는 경우에만 새로운 Spot 전용 노드 그룹을 추가로 생성해야 합니다. 기존 노드 그룹 수정 또는 삭제 시 감점 처리 됩니다.

10) 별도 언급이 없는 경우, ap-northeast-2 리전에 리소스를 생성하도록 합니다.

11) 모든 리소스의 이름, 태그, 변수는 대소문자를 구분합니다.

3. Bastion 서버

EC2를 활용해 Bastion 서버를 구성합니다. 네트워크 위치는 무관하며 외부에서 접근할 수 있도록 구성합니다. Bastion 서버 자체는 채점하지 않으나, 이후 과제 풀이를 위해 아래 조건을 참고하여 반드시 생성해야 합니다. 별도 언급이 없는 한, 채점은 Bastion에 root 계정으로 SSH 접속한 뒤 awscli 등의 명령어를 실행하는 방식으로 이루어집니다. 또한, wsi-cluster 클러스터에 대해 kubectl get all --all-namespaces 명령이 정상적으로 실행되어야 합니다.

- Name Tag : wsi-bastion
- Instance type : t3.medium
- AMI : Amazon Linux 2023
- Key pair name : wsi-bastion-key
- 설치 패키지 : jq, yq, awscli, kubectl, helm, eksctl
- EC2 IAM Role : wsi-bastion-role (모든 리소스에 대해 full access를 가지는 role을 생성하여 붙입니다.)

4. VPC CNI Setting Problems

1) 지급 파일

제공된 wsi_day3_troubleshooting.zip을 Bastion 서버의 /home/ec2-user 경로에 압축 해제 한 후, wsi_day3_troubleshooting 내의 wsi_day3_vpc_cni zip을 압축 해제합니다. 압축 파일 내에는 다음 리소스가 포함되어 있습니다.

- deployment.yaml : 199개의 일반 Pod를 생성하는 Deployment 파일
- backup-pod.yaml : backup-pod 라벨이 부여된 1개의 Pod를 생성하는 Deployment 파일
- pod-sg-policy.yaml : 특정 Pod에만 Security Group을 적용하기 위한 Policy 파일

- wsi-env-resource-cf.yaml : 문제 풀이 환경을 구성하는 CloudFormation 템플릿 파일

2) 문제

금융 클라우드 보안 전문기업 A사는 고객사의 데이터를 안전하게 처리하기 위해 AWS 기반 EKS 클러스터를 운영하고 있습니다.

최근 신규 애플리케이션을 배포하는 과정에서 200개 이상의 Pod를 동시에 생성할 때 일부 Pod가 Pending 상태로 머무르는 현상이 발생하고 있습니다. IP 주소 부족 문제를 해결하여deployment.yaml과 backup-pod.yaml을 둘 다 배포했을 때 200개의 Pod가 전부 Running 상태가 되도록 만드는 것이 필요합니다.

또한 신규 애플리케이션은 사용자 데이터를 주기적으로 백업하는 기능을 제공합니다. 이 기능은 backup-pod 라벨이 부여된 특정 Pod에서만 수행되며, 해당 Pod는 wsi-main-vpc에 배포된 클러스터에서 wsi-backup-vpc 내 배포된 file-server EC2로 접근해야 합니다.

사전 지급된 wsi-env-resource-cf.yaml을 이용하여 CloudFormation 스택을 배포하세요. Cloudformation Stack 이름은 **wsi-env-resource**로 설정합니다. 부록 1에 명시된 Cloudformation 리소스 정보를 참고하여 위의 트러블슈팅 문제를 해결해야 합니다.

3) 구성

Cloudformation을 통해 배포된 wsi-main-vpc 내에 EKS 클러스터를 생성합니다. 관리형 노드그룹으로 노드를 생성해야 하며, 아래 명시되어 있는 구성을 참고하여 노드그룹을 만들어야 합니다.

지급된 deployment.yaml 파일을 적용하여 199개의 일반 Pod를 생성하고, backup-pod.yaml 파일을 적용하여 backup-pod 라벨이 부여된 1개의 Pod를 추가로 생성합니다. IP부족 문제로 Pod 생성 후 일부 Pod가 Pending 상태로 남아 있을 수 있습니다. VPC CNI Add-on 설정 중 Prefix Delegation 활성화 여부를 점검하여 모든 Pod가 Running 상태가 되도록 합니다.

마지막으로 지급파일 내 pod-sg-policy.yaml 을 수정하여 wsi-backup-pod에만 별도의 Security Group을 부여하고 해당 Pod만 wsi-backup-vpc내 파일 서버에 접근 가능하도록 설정합니다. wsi-backup-pod에 사용되는 Security Group의 이름은 **wsi-backup-pod-sg** 로 설정합니다. file-server EC2 인스턴스는 HTTP (80번 포트)로 서비스 중입니다. File-server EC2 Security Group의 Inbound rule Type은 반드시 특정 포트로만 지정해야 합니다. 채점 시 모든 Pod가 Running 상태임을 확인하고, wsi-backup-pod만 cross-VPC 통신이 가능한지 Pod 내에서 'curl http://<backup-file-server Private IP>' 명령어를 통해 테스트합니다.

- 클러스터 구성

- Cluster Name : wsi-cluster
- Cluster VPC : wsi-main-vpc
- Cluster IAM Role Name : wsi-cluster-role
- 클러스터는 사용자 지정 구성 옵션으로 생성해야 하며, EKS auto mode는 비활성화 합니다.

- 노드그룹 구성

- Nodegroup Name : wsi-main-nodegroup
- Node IAM Role : wsi-node-role
- Tag : Name=wsi-eks-main-node
- Nodegroup Capacity Type : On-Demand
- Node EC2 Instance Type : c5.xlarge
- AMI Type : Amazon Linux 2023 Standard
- min : 3 / max : 3 / desired : 3
- Nodegroup Subnet : wsi-main-vpc의 Private Subnet (10.0.11.0/24, 10.0.12.0/24)

* 유의사항

- 노드 수는 기존 구성에서 변경하지 않도록 합니다.

- file-server EC2의 보안그룹 설정 시, Pod의 IP를 직접 허용하는 방식은 금지되며, 반드시 Security Group ID를 Source로 명시하여 접근을 허용해야 합니다.

5. Pod IAM Problems

1) 지급파일 소개

제공된 wsi_day3_troubleshooting.zip 내의 wsi_day3_pod_iam.zip을 압축 해제합니다. 압축 파일 내에는 다음 리소스가 포함되어 있습니다.

- storageclass.yaml : StorageClass 정의

- pvc.yaml : 4Gi volume을 요청하는 PVC

- pod.yaml : PVC를 사용하는 애플리케이션 Pod

2) 문제

A 사는 wsi-cluster에 EBS CSI Driver를 배포하여 EBS 동적 프로비저닝을 구성하려고 했지만, 에러로 인해 볼륨이 생성되지 않는 문제를 발견하였습니다.

또한, 애플리케이션 Pod를 배포한 이후, PVC가 정상적으로 바인딩되지 않고 Pending 상태에 머무르는 문제가 추가로 발생하고 있습니다. StorageClass는 존재하지만, 동적 프로비저닝이 정상적으로 동작하지 않는 상황입니다.

사내 보안 정책에 따라 다음 조건을 반드시 준수해야 합니다.

- IRSA (ServiceAccount 기반 IAM Role 연결) 사용 금지

- IMDS (Instance Metadata Service) 기반 노드 IAM Role사용 금지

주어진 지급 파일을 이용하여 EBS CSI Driver가 정상 동작하는지 확인하고, Pod가 EBS 볼륨을 성공적으로 마운트하는지 확인해야 합니다.

3) 구성

Pod Identity용 IAM Role을 생성합니다. IAM Role 이름은 AmazonEKS-PodIdentity-EBS-CSI-DriverRole로 설정하고, 생성한 IAM Role에 AmazonEBSCSIDriverPolicy 라는 이름의 AWS managed 정책을 Attach 합니다. 지급된 storageclass.yaml, pvc.yaml, pod.yaml 파일을 적용하여 애플리케이션을 배포합니다. PVC가 Pending 상태로 머무르는 경우 kubectl describe pvc 명령어를 통해 에러 메시지를 분석하고 문제를 해결하여 PVC가 정상적으로 Bound 상태가 되도록 수정합니다.

* 유의사항

- 노드 수는 기존 구성에서 변경하지 않도록 합니다.

- PVC가 Bound 상태가 된 후, Pod가 정상적으로 Running 상태로 배포되어야 합니다.

- IMDS 또는 IRSA를 통한 IAM Role 연결은 금지되며, 반드시 Pod Identity를 통해 IAM 권한을 위임해야 합니다.

6. Non-Graceful Node Shutdown

1) 지급파일 소개

제공된 wsi_day3_troubleshooting.zip 에는 다음 리소스가 포함되어 있습니다.

- busy-app.yaml : EBS PVC 및 Pod 정의가 포함된 yaml 파일

2) 문제

A사는 안정적인 클라우드 운영을 위해 EC2 Spot Instance 기반의 전용 EKS 노드 그룹을 추가하여 비용 최적화를 시도하고 있습니다. 그러나 Spot Instance가 중단되거나 노드가 비정상적으로 종료될 경우, 기존 Pod에 Attach 된 EBS 볼륨이 이전 노드에 남아 있어 새로운 노드에서 Pod 재스케줄링 시 FailedAttachVolume에러가 발생하고 있습니다.

이 문제를 수동으로 detach 하지 않고 Node Termination Handler(NTH)를 통한 Graceful Node Termination 처리를 통해 자동으로 해결되도록 구성해야 합니다. 즉, Node가 강제로 termination 되었을 때 Graceful Shutdown이 되어 FailedAttachVolume 상태에서 SuccessfulAttachVolume 상태로 가는 데 2분 이하가 걸리도록 해야 합니다.

문제 상황 구성을 위해, 선수는 직접 Fault Injection Simulator (FIS)를 사용하여 Spot Instance Interruption 이벤트를 발생시켜야 합니다.

3) 구성

기존 node group은 그대로 두고, Spot Instance로만 구성된 새로운 node group을 추가로 생성합니다. 해당 node group은 반드시 self managed nodegroup으로 구성해야만 합니다.

- 노드그룹 구성

- Nodegroup Name : wsi-spot-nodegroup

- Nodegroup Capacity Type : Spot

- Node EC2 Instance Type : c5.xlarge

- min : 2 / max : 2 / desired : 2

- subnet : wsi-main-vpc의 Public Subnet (10.0.1.0/24, 10.0.2.0/24)

- Labels : nodegroup: wsi-self-managed-ng

busy-app.yaml을 적용하여 장기 실행하는 EBS 볼륨 기반 Pod를 배포합니다. 이 때 AWS **Node Termination Handler**를 클러스터에 설치하여 사용해야 하며, IMDS Processor mode를 활성화 하여 이벤트를 감지해야 합니다.

- FIS Experiment template 구성

- Fault Injection Simulator(FIS) Template Name : wsi-spot-interruption-test

- Target Name : wsi-spot-target

- Action Name : wsi-send-spot-interruptions-action

- Tag : Name=wsi-fis-experiment

- FIS Action Type : aws:ec2:send-spot-instance-interruptions

- FIS Duration Before Interruption : 2 Minutes

해당 실험을 실행하면 Spot Instance에 중단 알림이 전달되어야 하며, 알림이 수신된 후 Node Termination Handler가 2분 이내에 해당 노드를 cordon 및 drain 처리하고 busy-app Pod를 다른 노드로 정상 재스케줄링 해야 합니다. Spot Instance 중단 알림을 받은 노드에 배포된 aws-node-termination-handler Pod의 로그를 확인했을 때 인스턴스가 cordon 및 drain 되었다는 로그가 보여야 해결한 것으로 간주됩니다.

* 유의사항

- wsi-spot-nodegroup 은 wsi-main-vpc 내 public subnet에 배포해야 합니다.

- EC2 인스턴스를 직접 종료하거나, 수동으로 볼륨을 detach하는 행위는 금지되며, 채점 대상에서 제외됩니다.

- wsi-spot-nodegroup을 managed nodegroup으로 생성했다면 채점 대상에서 제외됩니다.

- Karpenter Add-on은 사용하지 않도록 합니다.

부록 1

VPC 정보

Name Tag	CIDR
wsi-main-vpc	10.0.0.0/16
wsi-backup-vpc	10.20.0.0/16

Subnets 정보

Name Tag	CIDR	Availability Zone
wsi-main-public-subnet-1	10.0.1.0/24	ap-northeast-2a
wsi-main-public-subnet-2	10.0.2.0/24	ap-northeast-2b
wsi-main-private-subnet-1	10.0.11.0/24	ap-northeast-2a
wsi-main-private-subnet-2	10.0.12.0/24	ap-northeast-2b
wsi-backup-public-subnet	10.20.1.0/24	ap-northeast-2a
wsi-backup-private-subnet	10.20.2.0/24	ap-northeast-2b

Route Tables 정보

Name Tag	Subnet	Gateway
wsi-main-public-rt	wsi-main-public-subnet-1 wsi-main-public-subnet-2	Internet Gateway (Name Tag : wsi-main-igw)
wsi-main-private-rt	wsi-main-private-subnet-1 wsi-main-private-subnet-2	NAT Gateway (Name Tag : wsi-main-natgw)
wsi-backup-public-rt	wsi-backup-public-subnet	Internet Gateway (Name Tag : wsi-backup-igw)
wsi-backup-prviate-rt	wsi-backup-private-subnet	NAT Gateway (Name Tag : wsi-backup-natgw)

VPC Peering Connection정보

VPC Peering
Main-to-backup-peering (wsi-main-vpc <-> wsi-backup-vpc)

File Server EC2 인스턴스 정보

Name Tag	VPC	Subnet
backup-file-server	wsi-backup-vpc	wsi-backup-private-subnet