

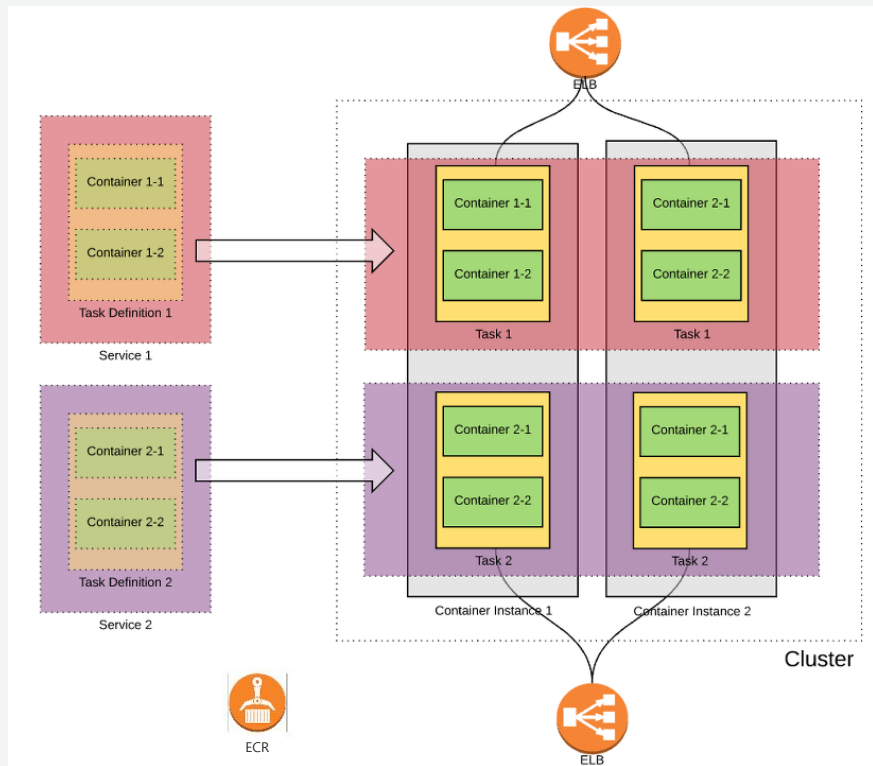
AWS ECS Case Study

2019.04.13 – 하수용



Amazon ECS

Amazon ECS 용어 정리



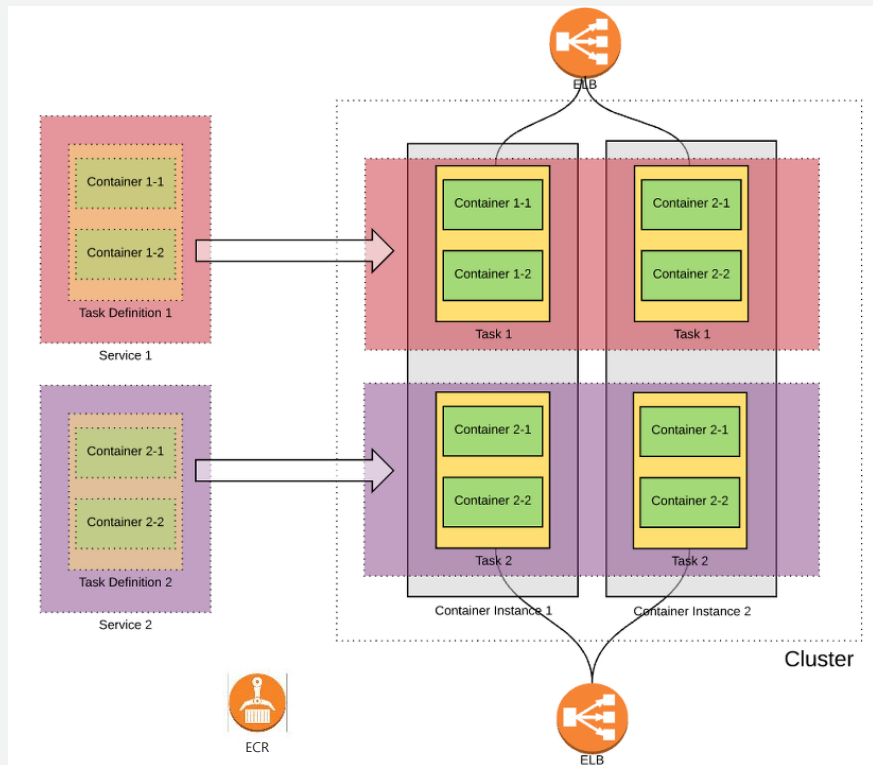
ECS Cluster

- **Container Instance의 집합**
- 서비스나 태스크가 실행되는 공간
- ECS의 가장 기본적인 단위이며, 논리적인 개념
- 클러스터가 없으면 ECS에서 컨테이너를 실행할 수 없음

Container Instance

- **ECS Cluster에 속한 EC2 인스턴스**
- 컨테이너 인스턴스는 클러스터에서 서비스나 태스크를 실행하기 위해 사용하는 컴퓨팅 자원
- EC2 인스턴스에 ecs-agent를 설치하고 클러스터명을 설정해서 특정 클러스터의 컨테이너 인스턴스로 등록할 수 있음
- 클러스터(스케줄러)는 컨테이너 인스턴스를 조작할 수 있는 권한을 가지고 있으며, 클러스터에서 서비스나 태스크를 실행하면 조건을 만족하는 컨테이너 인스턴스를 찾아 컨테이너로 실행
- 단, fargate를 사용하는 경우 컨테이너 인스턴스가 없음

Amazon ECS 용어 정리



Task (ECS Cluster에서의 Task를 의미)

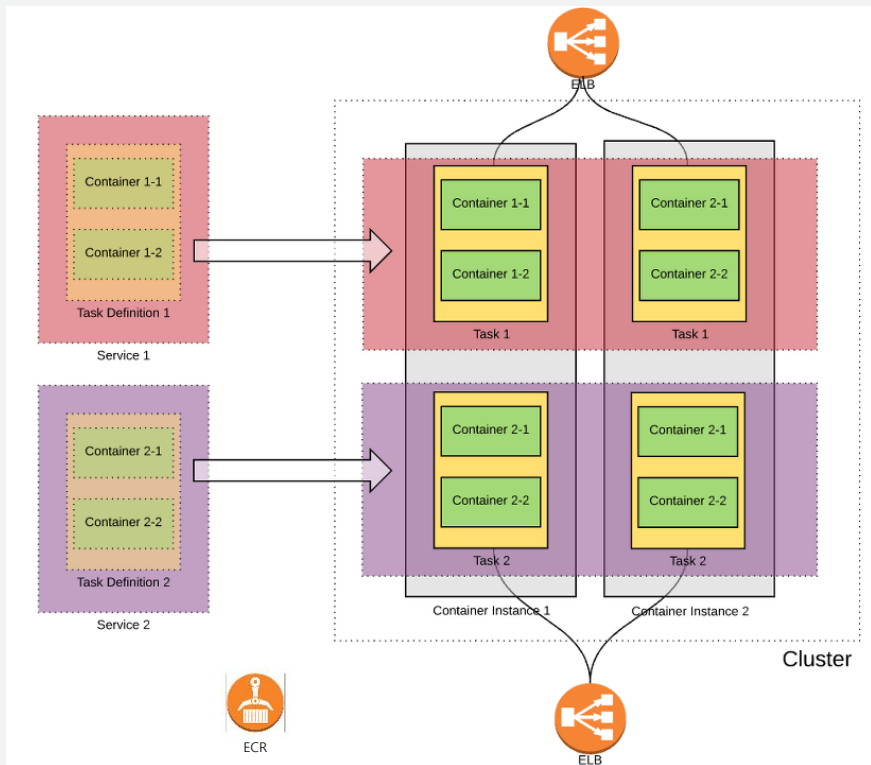
- 애플리케이션 컨테이너들의 집합
- 태스크는 ECS의 최소 실행 단위로 하나 이상의 컨테이너의 묶음
- 태스크는 독립 실행되거나 서비스에 의해서 실행될 수 있음
- 클러스터는 적절한 컨테이너 인스턴스를 찾아 태스크 디피니션을 기반으로 태스크를 실행
- 만약 독립적으로 태스크를 실행하였을 경우 생성한 이후로 관리되지 않음

Service

- Task를 지속적으로 관리하는 역할
- 서비스는 태스크를 지속적으로 관리하는 단위
- 서비스는 클러스터 내에서 태스크가 지정된 수만큼 지속적으로 실행될 수 있도록 관리
- 로드 밸런서와 연동해서 실행중인 태스크를 찾아 자동적으로 로드 밸런서에 등록 및 제거하는 역할도 담당

Amazon ECS

Amazon ECS 용어 정리



Task Definition

- 컨테이너 집합의 사전 명세서
- 태스크 디피니션은 ECS의 최소 실행 단위인 태스크를 실행하기 위한 설정을 저장하고 있는 리소스.
- 태스크 디피니션은 하나 이상의 컨테이너에 대한 정보 (컨테이너 디피니션)를 포함할 수 있으며 최대 10개 컨테이너까지 가능
- 컨테이너 별로 실행하고자 하는 이미지를 지정 해야하며, CPU와 RAM과 같은 리소스 제한 정보와 컨테이너 실행에 필요한 옵션들을 지정
- 태스크 디피니션은 클러스터에 종속되어있지 않으며 여러 클러스터에서 사용할 수 있음

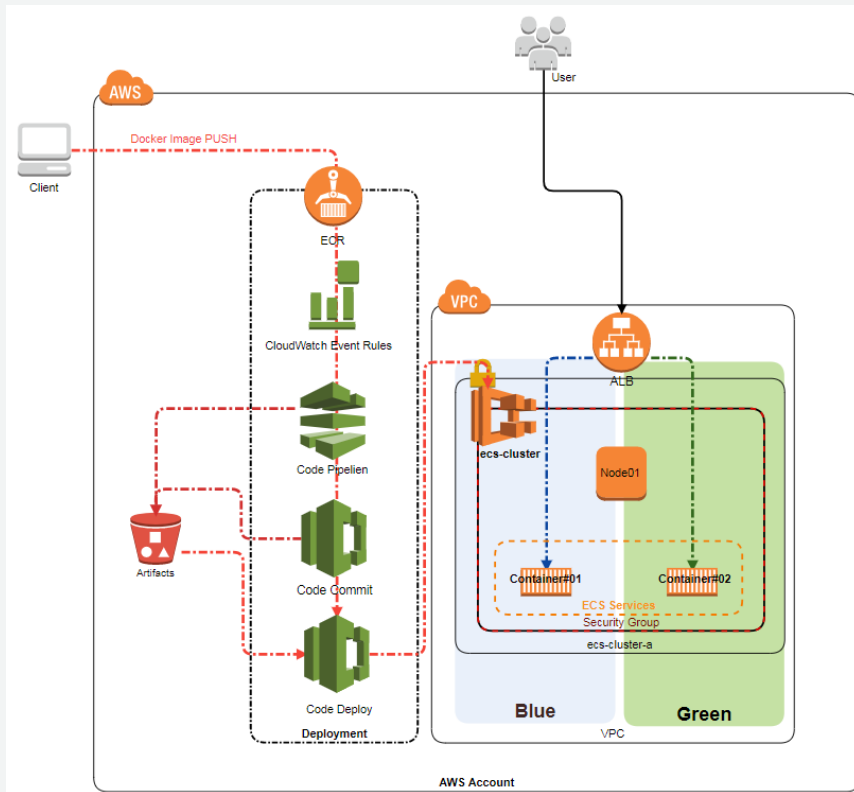
Amazon ECR

- Docker image 저장소
- ECS는 컨테이너 오케스트레이션 도구로, 컨테이너를 관리하는 역할
- 컨테이너는 이미지로부터 실행되며, 이미지는 특정 애플리케이션을 실행 가능한 환경을 재현하기 위한 파일 집합
- 이 이미지는 ECS와는 별개로 생성 및 관리되며, ECS 사용자는 먼저 자신이 실행하고자 하는 애플리케이션을 이미지로 가지고 있어야 함
- ECS를 사용할 때 이미지는 도커Docker 이미지와 같다고 이해하면 됨

ECS CI/CD Pipeline

1. ECS 환경에서 CD(Continuous Delivery) 환경 구성

- Code Pipeline, Code Commit, Code Deploy를 이용한 CD(Continuous Delivery) 환경 구성

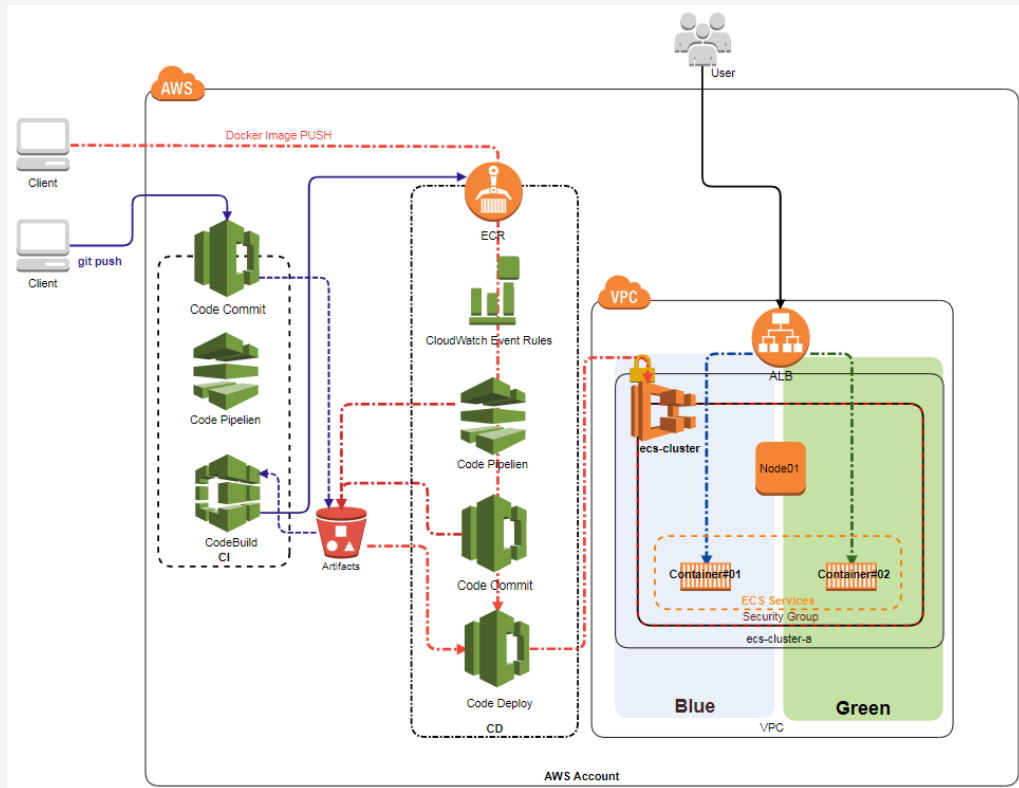


- Rolling update 환경도 아키텍처는 동일
- ECS 환경에서의 Canary 배포는 Code Deploy에서 아직 지원하지 않음
- Rolling update와 Blue/Green deploy는 Code Deploy에서 결정

ECS CI/CD Pipeline

1. ECS 환경에서 CI/CD(Continuous Integration/Continuous Delivery) 환경 구성

- Code Pipeline, Code Commit, Code Deploy를 이용한 CD(Continuous Delivery) 환경 구성



- CI(Continuous Integration) 부분과 CD(Continuous Delivery) 부분을 분리하여야 함
- CodeBuild에서 Docker engine을 제외한 이미지는 모두 Docker in Docker 형태로 build 시켜야 함

ECS 장애 상황

1. Container Instance가 Launch 되었음에도 ECS Cluster에 속하지 않을 때

- Container Instance에 Roles(역할)이 부여되지 않아 권한 부족으로 Cluster에 속하지 못할 때

```
# cat /var/log/ecs/ecs-agent.log.2019-04-13-03
```

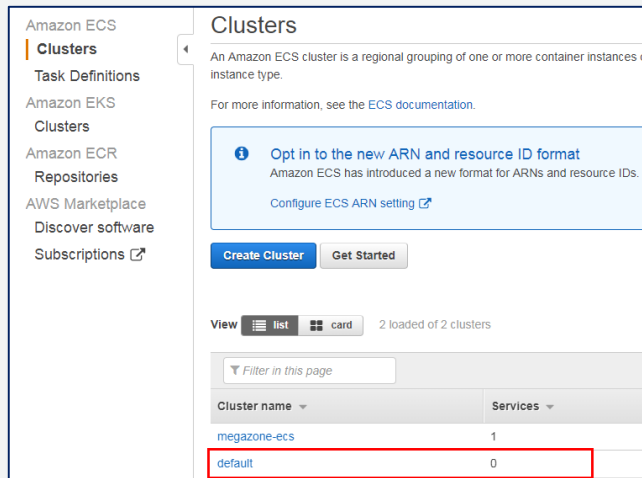
```
2019-04-13T03:31:48Z [ERROR] Unable to register as a container instance with ECS: NoCredentialProviders: no valid providers in chain.  
Deprecated.
```

✓ 조치 방법

- AutoScale Launch Configurations에서 역할(role) 부여
- 예) ecsInstanceRole

1. Container Instance가 Launch 되었음에도 ECS Cluster에 속하지 않을 때

- /etc/ecs/ecs.config 파일에 ECS cluster name이 명시되지 않았거나, 잘못 기입되었을 경우
 - ECS default cluster가 생기는 경우



```
# cat /var/log/ecs/ecs-agent.log.2019-04-13-03
```

2019-04-13T03:38:11Z [INFO] Registration completed successfully. I am running as 'arn:aws:ecs:ap-northeast-2:578611160639:container-instance/8ab73fa2-8f96-4c02-b26f-a9167a58dc42' in cluster 'default'

✓ 조치 방법

- 기존 ECS Cluster(megazone-ecs)에서 인스턴스 scale in - default cluster 삭제하여도 인스턴스 안 지워짐
- AutoScale Launch Configurations에서 Userdata 재 확인

2. ECS Service에서 Container 컨테이너가 시작되지 않거나 배포되지 않을 때

- ECS Cluster의 인터넷 연결이 안되어 있을 때
 - 'ECS Cluster -> Service -> Events'에서 메시지를 확인할 수 있음
 - Container Instance는 IGW 혹은 NAT G/W로 ECS agent가 인터넷과 무조건 연결되어 있어야 함

Clusters > megazone-ecs > Service: megazone-service

Service : megazone-service

Update Delete

Cluster [megazone-ecs](#) Desired count 1



Status **ACTIVE** Pending count 0

Task definition [megazone-taskdef.1](#) Running count 0

Service type REPLICA

Launch type EC2

Details Tasks **Events** Auto Scaling Deployments Metrics Tags

Last updated on April 13, 2019 12:15:43 PM (0m ago)  

Filter in this page < 1-1 >

Event Id	Event Time	Message
18a0e497-04a7-407d-98ab-4d8131a8e311	2019-04-13 12:15:31 +0900	service megazone-service was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster. For more information, see the Troubleshooting section .

✓ 조치 방법 :

- Container Instance가 속한 VPC Subnet의 Route table을 수정

3. ECS Service에서 Container 컨테이너가 시작되지 않거나 중지되지 않을 때

- ECS Agent container가 죽었을 때
 - ECS Agent가 죽게 되면 ECS Cluster와 통신하지 못하게 되어 비 정상적으로 동작한다.
 - Container 배포가 제대로 되지 않을 수 있다.
 - Service를 중지를 시켜도 실제 Container Instance에 떠있는 컨테이너가 중지되지 않는다. (콘솔에선 중지된 것으로 보임)

Clusters > megazone-ecs > Service: megazone-service

Service : megazone-service Update Delete

Cluster megazone-ecs Desired count 1

Status ACTIVE Pending count 0

Task definition megazone-taskdef:1 Running count 0

Service type REPLICA

Launch type EC2

Details Tasks **Events** Auto Scaling Deployments Metrics Tags

Last updated on April 13, 2019 1:02:41 PM (0m ago) Refresh Help

Filter in this page < 1-8 >

Event Id	Event Time	Message
78ac39ac-47c1-4762-ab82-64dfcfef9a86	2019-04-13 13:01:52 +0900	service megazone-service was unable to place a task because no container instance met all of its requirements. The closest matching container-instance b6e08f1d-1bcb-49d7-b3e1-96348c12dc91 doesn't have the agent connected. For more information, see the Troubleshooting section .

✓ 조치 방법 :

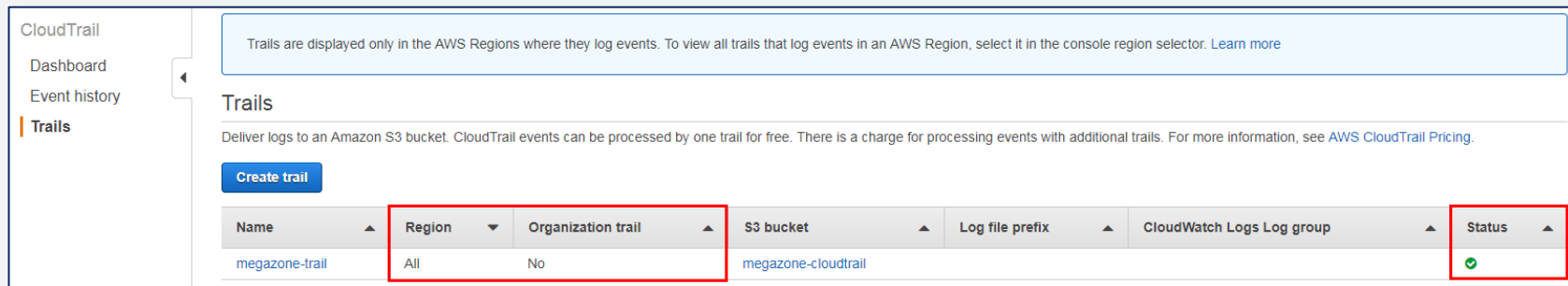
- Container Instance의 agent container를 기동 (# sudo start ecs)
- 재발 방지를 위해 스크립트를 Launch configuration Userdata에 적용 (Git : <https://github.com/blueice123/ecs-case-study.git>)

4. ECR에 PUSH를 하였지만, Code Pipeline에 trigger되지 않을 때

- CloudTrails enabled 되어 있지 않은 경우
 - ECR에 image를 push하게 되면 실제로 CloudTrail에서 API를 감지하여 CloudWatch rules에 전달함.

✓ 조치 방법 :

- CloudTrails enable 설정



CloudTrail

Trails are displayed only in the AWS Regions where they log events. To view all trails that log events in an AWS Region, select it in the console region selector. [Learn more](#)

Trails

Deliver logs to an Amazon S3 bucket. CloudTrail events can be processed by one trail for free. There is a charge for processing events with additional trails. For more information, see [AWS CloudTrail Pricing](#).

[Create trail](#)

Name	Region	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs Log group	Status
megazone-trail	All	No	megazone-cloudtrail			On

- workaround로 CloudWatch rules를 비활성화 하고 ECR image push 후에 AWS CLI로 code pipeline 시작
 - \$ aws codepipeline start-pipeline-execution --name *pipelines_name*

4. ECR에 PUSH를 하였지만, Code Pipeline에 trigger되지 않을 때

- Code pipelin에서 source 부분의 ECR에 Image tag가 잘못 정의되어 있을 경우
 - ECR에 image를 push하게 되면 실제론 CloudTrail에서 API를 감지하여 CloudWatch rules에 전달함.

✓ 조치 방법 :

- Code Pipeline에서 Source 설정 재 확인

Source

Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.

Amazon ECR ▼

Repository name
Choose an Amazon ECR repository as the source location.

megazone-repo ▼ [Create repository ↗](#)

Image tag - optional
Choose the image tag that triggers your pipeline when a change occurs in the image repository.

🔍 latest ✕

If an image tag is not selected, defaults to latest

