**AWS CNI란?**

AWS EKS는 Kubernetes Network Addon인 CNI(Container Networking Interface)로 VPC(Virtual Private Cloud)의 IP 주소를 Pod에 할당하는 AWS VPC CNI를 사용하고 있다. 즉, 생성되는 Pod가 할당 받는 IP주소는 AWS VPC에서 할당해주는 IP주소가 된다.

AWS CNI를 사용하면 AWS에서 지원하는 VPC Flow Log, VPC Routing Policy, 네트워크 트래픽 격리를 위한 보안 그룹을 사용할 수 있다.

Worker Node 역할을 하는 EC2 인스턴스가 생성된 때 인스턴스에 연결된 네트워크 인터페이스를 기본 네트워크 인터페이스라고 하며, 인스턴스가 연결된 추가 네트워크 인터페이스를 보조 네트워크 인터페이스라고 한다.

각 네트워크 인터페이스에는 여러 개의 Private IP 주소가 할당될 수 있다. Private IP 주소 중 하나는 기본 IP 주소지만 네트워크 인터페이스에 할당된 다른 모든 주소는 보조 IP 주소이다.

[m5.large 인스턴스 유형인 Worker Node의 경우]

각 네트워크 인터페이스에 대해 3개의 네트워크 인터페이스와 10개의 Private IP 주소를 지원한다.

즉, pod를 생성할 경우 eth0(기본 인터페이스)에서 eth1(보조 인터페이스)가 생성이된다. m5.large의 사양마냥 최대 3개의 네트워크 인터페이스와 각 인터페이스 별로 10개의 Private IP 주소를 지원한다고 가정해보자. 이럴 경우에는 Pod를 12개 생성하면 인터페이스당 할당 가능 IPv4 주소인 10개를 초과하므로 eth2(보조 인터페이스)를 추가로 생성한다.

만약 Pod가 없다면 eth0(기본 인터페이스)만 존재하게 된다.

[AWS CNI는 Network Policy]

AWS CNI는 Network Policy를 지원하지 않는다. 그래서 추가적으로 Calico, weave net과 같은 CNI를 연동해서 방화벽 정책을 적용해야 한다.

**AWS CNI 장점**

1. Overlay Network처럼 캡슐화 및 캡슐화 해제의 오버 헤드가 발생하지 않는다.
2. VPC Flow Logs를 사용할 수 있음. Pod에서 송수신되는 IP 트래픽에 대한 정보를 캡처할 수 있다.
3. ENI(Elastic Network Interface)를 공유하는 Pod가 적기 때문에 네트워크 대역폭에 대한 경합이 줄어든다.
4. VPC 트래픽을 Pod로 직접 라우팅 할 수 있다.

**AWS CNI 단점**

1. VPC CNI 사용자 지정 네트워킹을 통해 Pod에 할당할 수 있는 IP 주소가 제한되어 Worker Node에 Pod를 배포할 수 있는 수가 제한됨.
2. 만약 Worker Node 중 특정 Node만 인스턴스 유형과 사양이 높다면 해당 Node에 과부하가 걸릴 수 있음

**Node instance Secondary IP제한하기**

실제 실무에서는 Node instance가 갖는 ip의 개수가 많아지면 많아질수록 네트워크 대역을 차지하게 되기 때문에 이를 제한 해야하는 상황이 발생하기도 한다. 이럴 때는 아래와 같이 aws-node daemonset을 설정하여 IP 개수에 대한 제어가 가능하다.

aws-node daemonset이 L-IPAM데몬을 실행하여 ENI에 secondary IP 할당과 Pod IP 할당을 하기 때문이다.

|  |
| --- |
| $ kubectl set env ds aws-node -n kube-system WARM\_IP\_TARGET=1  $ kubectl set env ds aws-node -n kube-system MINIMUM\_IP\_TARGET=30 |

* WARM\_IP\_TARGET: 특정 IP 개수만 Warm Pool을 설정. 1로 설정되면 pod가 생성될 때마다 secondary IP가 1개 씩 추가로 할당된다.  
  (Pod의 생성이 빈번할 때 인스턴스에 IP를 할당하고 해제하는 API call 횟수가 늘어나게 되서 Throttling이 발생할 수 있으므로 MINIMUM\_IP\_TARGET 설정을 같이 설정한다.)
* MINIMUM\_IP\_TARGET: Node instance에 일반적으로 유지되는 Pod 수를 설정한다. 해당 수만큼 미리 ENI에 Secondary IP가 할당된다.