

## 4-1. EKS Cluster 구성

클라우드 네이티브 운영체제

Exported on 09/15/2022

## Table of Contents

<b>1 사전 준비 .....</b>	<b>3</b>
1.1 네트워크 구성 .....	3
1.2 EKS 클러스터 IAM Role 생성 .....	4
1.3 kubectl 수행용 Bastion 인스턴스 생성 .....	6
1.4 Bastion 서버 접속 및 Credentials 설정 .....	8
<b>2 EKS 클러스터 생성 .....</b>	<b>9</b>
2.1 클러스터 생성 .....	9
2.2 Bastion 서버 kubectl 설정 .....	11
<b>3 Fargate 생성 .....</b>	<b>13</b>
3.1 Fargate IAM 역할 생성 .....	13
3.2 Fargate 프로필 생성 .....	16
3.3 CoreDNS pod 수정 .....	17

# 1 사전 준비

---

## 1.1 네트워크 구성

※ 별도로 준비된 네트워크(VPC)가 있다면 생략한다.

### 1. VPC 생성

- Name : vpc-sts
- IPv4 Addr Block : 10.0.0.0/16

### 2. Subnet 생성

- Public Subnet 1
  - Name : subnet-sts-public-a
  - AZ : az-a
  - IPv4 addr block : 10.0.1.0/24
- Public Subnet 2
  - Name : subnet-sts-public-c
  - AZ : az-c
  - IPv4 addr block : 10.0.2.0/24
- Private Subnet 1
  - Name : subnet-sts-private-a
  - AZ : az-a
  - IPv4 addr block : 10.0.3.0/24
- Private Subnet 2
  - Name : subnet-sts-private-c
  - AZ : az-c
  - IPv4 addr block : 10.0.4.0/24

### 3. IGW 생성

- Name : igw-sts
- 1번에서 생성한 vpc에 연결

### 4. NAT Gateway 생성

- Name : nat-sts
- Subnet : subnet-sts-public-a

### 5. Route Table 생성

- Public Route Table
  - Name : rtb-public

- 이 라우팅 테이블에 Public Subnet 두 개를 연결한다.

대상 ▾	대상 ▾
0.0.0.0/0	igw-0873f8fb246733393
10.0.0.0/16	local

- Private Route Table
  - Name : rtb-private
  - 이 라우팅 테이블에 Private Subnet 두 개를 연결한다.

대상 ▾	대상 ▾
0.0.0.0/0	nat-0294a5a1949b33b17
10.0.0.0/16	local

## 1.2 EKS 클러스터 IAM Role 생성

To create your Amazon EKS cluster role in the IAM console

- Open the IAM console at <https://console.aws.amazon.com/iam/>.
- Choose **Roles**, then **Create role**.
- Under **Trusted entity type**, select **AWS service**.
- From the **Use cases for other AWS services** dropdown list, choose **EKS**.
- Choose **EKS - Cluster** for your use case, and then choose **Next**.
- On the **Add permissions** tab, choose **Next**.
- For **Role name**, enter a unique name for your role, such as `eksClusterRole`.
- For **Description**, enter descriptive text such as `Amazon EKS - Cluster role`.
- Choose **Create role**.

## 신뢰할 수 있는 엔터티 유형

☒ **AWS 서비스**  
 EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

☐ **AWS 계정**  
 사용자 또는 서드 파티에 속한 다른 AWS 계정의 엔터티가 이 계정에서 작업을 수행하도록 허용합니다.

☐ **웹 자격 증명**  
 지정된 외부 웹 자격 증명 공급자와 연동된 사용자가 이 역할을 맡아 이 계정에서 작업을 수행하도록 허용합니다.

☐ **SAML 2.0 연동**  
 기업 디렉터리에서 SAML 2.0과 연동된 사용자가 이 계정에서 작업을 수행할 수 있도록 허용합니다.

☐ **사용자 지정 신뢰 정책**  
 다른 사용자가 이 계정에서 작업을 수행할 수 있도록 사용자 지정 신뢰 정책을 생성합니다.

## 사용 사례

EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

### 일반 사용 사례

- ☐ **EC2**  
Allows EC2 instances to call AWS services on your behalf.
- ☐ **Lambda**  
Allows Lambda functions to call AWS services on your behalf.

다른 AWS 서비스의 사용 사례:

EKS

☐ **EKS**  
 Allows EKS to manage clusters on your behalf.

☒ **EKS - Cluster**  
 Allows access to other AWS service resources that are required to operate clusters managed by EKS.

IAM → 역할 → 역할 생성

신뢰할 수 있는 엔터티 유형 : AWS 서비스

사용 사례 : EKS - Cluster

## 역할 세부 정보

### 역할 이름

이 역할을 식별하는 의미 있는 이름을 입력합니다.

EKSClusterRole

최대 64자입니다. 영숫자 및 '+', '@', '-' 문자를 사용하세요.

### 설명

이 역할에 대하여 간단한 설명을 추가합니다.

Allows access to other AWS service resources that are required to operate clusters managed by EKS.

최대 1,000자입니다. 영숫자 및 '+', '@', '-' 문자를 사용하세요.

역할 이름 : EKSClusterRole

### 1.3 kubectl 수행용 Bastion 인스턴스 생성

## 이름 및 태그 정보

이름

ec2-sts-bastion

[추가 태그 추가](#)

### ▼ 애플리케이션 및 OS 이미지(Amazon Machine Image) 정보

AMI는 인스턴스를 시작하는 데 필요한 소프트웨어 구성(운영 체제, 애플리케이션 서버 및 애플리케이션)이 포함된 템플릿입니다. 아래에서 찾고 있는 항목이 보이지 않으면 AMI를 검색하거나 찾아보십시오.

수천 개의 애플리케이션 및 OS 이미지를 포함하는 전체 카탈로그 검색

최근 사용

#### 4 AMI

## Quick Start

Amazon  
Linux



macOS



Ubuntu

ubuntu®

## Windows



Red Hat



더 많은 AMI 찾아보  
기

AWS, Marketplace 및 커뮤니티의 AMI 포함

## Amazon Machine Image(AMI)

▼ 네트워크 설정 정보

VPC - 필수 정보

vpc-09d94a795f7f7fc03

10.0.0.0/16

↻

서브넷 정보

subnet-0c4891dbf8e07791f

VPC: vpc-09d94a795f7f7fc03    소유자: 694833324522

가용 영역: ap-northeast-2c    IP 주소 사용 가능: 251    CIDR: 10.0.11.0/24

↻    새 서브넷 생성

퍼블릭 IP 자동 할당 정보

활성화

방화벽(보안 그룹) 정보

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 특정 트래픽이 인스턴스에 도달하도록 허용하는 규칙을 추가합니다.

☒ 보안 그룹 생성

☐ 기존 보안 그룹 선택

보안 그룹 이름 - 필수

scg-ec2-eks-bastion

이 보안 그룹은 모든 네트워크 인터페이스에 추가됩니다. 보안 그룹을 만든 후에는 이름을 편집할 수 없습니다. 최대 길이는 255자입니다. 유효한 문자는 a~z, A~Z, 0~9, 공백 및 .\_-:/()#,@[]+=&{}!\$\*입니다.

설명 - 필수 정보

scg-ec2-eks-bastion

유형 정보

ssh

프로토콜 정보

TCP

포트 범위 정보

22

소스 유형 정보

내 IP

원본 정보

Q CIDR, 접두사 목록 또는 보안

27.122.140.10/32 X

설명 - optional 정보

예: 관리자 데스크톱용 SSH

EC2 → 인스턴스 → 인스턴스 시작

이름 : ec2-sts-bastion

인스턴스 유형 : t3.nano

키 페어 : '새 키 페어 생성' 또는 '기존 키 페어' 선택

VPC : vpc-sts

Subnet : subnet-sts-public-a

퍼블릭 IP 자동 할당 : 활성화

보안 그룹 : 신규 생성 (내 IP로 ssh 접근 가능하도록 설정)

사전 준비 - 7

## 1.4 Bastion 서버 접속 및 Credentials 설정

```
[ec2-user@ip-10-0-2-156 ~]$ aws configure
AWS Access Key ID [*****04RH]:
AWS Secret Access Key [*****KX0j]:
Default region name [ap-northeast-2]:
Default output format [json]:
```

ssh 접속 후 자신 계정의 credentials 설정

```
aws configure
```



## 2 EKS 클러스터 생성

### 2.1 클러스터 생성

#### 클러스터 구성

##### 클러스터 구성 정보

###### 이름

이 클러스터의 고유 이름을 입력합니다. 클러스터가 생성된 후에는 이 속성을 변경할 수 없습니다.

eks-sts-cluster

클러스터 이름은 문자 또는 숫자로 시작해야 하며 유니코드 문자 세트, 숫자, 하이픈 및 밑줄을 사용할 수 있습니다. 최대 길이는 100자입니다.

###### Kubernetes 버전 정보

이 클러스터의 Kubernetes 버전을 선택합니다.

1.22

###### 클러스터 서비스 역할 정보

Kubernetes 컨트롤 플레인 사용자 대신하여 AWS 리소스를 관리하도록 허용하는 IAM 역할을 선택합니다. 클러스터가 생성된 후에는 이 속성을 변경할 수 없습니다. 새 역할을 생성하려면 [Amazon EKS 사용 설명서](#)의 지침을 따르세요.

EKSClusterRole



EKS → 클러스터 → EKS 클러스터 생성

이름 : eks-sts-cluster

Kubernetes 버전 : 1.22

클러스터 서비스 역할 : EKSClusterRole

## 네트워킹 지정

### 네트워킹 정보

클러스터를 생성한 후에는 이러한 속성을 변경할 수 없습니다.

#### VPC 정보

EKS 클러스터 리소스에 사용할 VPC를 선택합니다. 새 VPC를 생성하려면 [VPC 콘솔](#)(으)로 이동합니다.

vpc-037b0055718d635b0



#### 서브넷 정보

클러스터와의 원활한 통신을 위해 제어 플레인 이 탄력적 네트워크 인터페이스(ENI)를 배치할 수 있는 서브넷을 VPC 내에서 선택합니다. 새 서브넷을 생성하려면 [VPC 콘솔](#)의 해당 페이지로 이동합니다.

서브넷 선택



subnet-02ed25f2d4b017a3a

subnet-05879d8c45d04add8

#### 보안 그룹 정보

작업자 노드 서브넷에서 생성된 EKS 관리형 탄력적 네트워크 인터페이스에 적용할 보안 그룹을 선택합니다. 새 보안 그룹을 생성하려면 [VPC 콘솔](#)의 해당 페이지로 이동합니다.

보안 그룹 선택



#### 클러스터 IP 주소 패밀리 선택 정보

클러스터의 Pod 및 서비스에 대한 IP 주소 유형을 지정합니다.

☒ IPv4

☐ IPv6

☐ Kubernetes 서비스 IP 주소 범위 구성 정보

클러스터 서비스가 IP 주소를 수신할 범위를 지정합니다.

### 클러스터 엔드포인트 액세스 정보

Kubernetes API 서버 엔드포인트에 대한 액세스 권한을 구성합니다.

☐ 퍼블릭

VPC 외부에서 클러스터 엔드포인트에 액세스할 수 있습니다. 작업자 노드 트래픽은 엔드포인트에 연결하기 위해 VPC를 벗어납니다.

☐ 퍼블릭 및 프라이빗

VPC 외부에서 클러스터 엔드포인트에 액세스할 수 있습니다. 엔드포인트에 대한 작업자 노드 트래픽은 VPC 내에 유지됩니다.

☒ 프라이빗

클러스터 엔드포인트는 VPC를 통해서만 액세스할 수 있습니다. 엔드포인트에 대한 작업자 노드 트래픽은 VPC 내에 유지됩니다.

VPC : vpc-sts

Subnet : subnet-sts-private-a, subnet-sts-private-c

클러스터 엔드포인트 액세스 : 프라이빗

## 2.2 Bastion 서버 kubectl 설정

**인스턴스: i-0cd825e971565bb5f(ec2-sts-bastion)**

세부 정보

**보안**

네트워킹

스토리지

상태 검사

모니터링

태그

▼ 보안 세부 정보

IAM 역할

role-ec2-eks-kugar

소유자 ID

694833324522

보안 그룹

sg-0461f80268bdf733e (launch-wizard-10)

Bastion 서버에서 kubectl을 사용하여 EKS 클러스터로 API를 요청할 수 있도록 443포트를 허용해주도록 한다.  
Bastion 서버의 보안 그룹을 확인한다.

개요

리소스

컴퓨팅

**네트워킹**

추가 기능

인증

로깅

업데이트 기록

태그

네트워킹

네트워킹 관리

VPC 정보

vpc-08c5c6870e1f5364e

클러스터 IP 주소 패밀리 정보

IPv4

서비스 IPv4 범위 정보

172.20.0.0/16

서브넷

subnet-0ada68c306ec98501

subnet-035c27d5461bac818

클러스터 보안 그룹 정보

sg-0050fbdf9e254d09c

추가 보안 그룹

없음

API 서버 엔드포인트 액세스 정보

퍼블릭

퍼블릭 액세스 소스 허용 목록

0.0.0.0/0

(모든 트래픽에 개방됨)

EKS 클러스터의 보안 그룹으로 이동한다.

인바운드 규칙 정보

보안 그룹 규칙 ID

sgr-04eb2f93602a5fedb

유형 정보

모든 트래픽

프로토콜 정보

전체

포트 범위 정보

전체

소스 정보

사용자 ...

sg-0050fbdf9e254d09c

HTTPS

TCP

443

사용자 ...

sg-0461f80268bdf733e

인바운드 규칙 편집 → HTTPS에 Bastion SG 추가

bastion 서버 접속하여 아래 명령어를 수행한다.

```
aws eks update-kubeconfig --region [region-code] --name [cluster-name]
```

kubectl 설치

```
curl -o kubectl https://s3.us-west-2.amazonaws.com/amazon-eks/1.22.6/2022-03-09/bin/
linux/amd64/kubectl
chmod +x ./kubectl
mkdir -p $HOME/bin && cp ./kubectl $HOME/bin/kubectl && export PATH=$PATH:$HOME/bin
echo 'export PATH=$PATH:$HOME/bin' >> ~/.bashrc

kubectl version --short --client

kubectl get ns
```

## 3 Fargate 생성

### 3.1 Fargate IAM 역할 생성

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 **역할(Roles)**을 선택합니다.
3. **역할(Roles)** 페이지에서 **역할 생성(Create role)**을 선택합니다.
4. 신뢰할 수 있는 엔티티 선택(**Select trusted entity**) 페이지에서 다음을 수행합니다.
  - a. 신뢰할 수 있는 엔티티 유형(**Trusted entity type**) 섹션에서 **AWS 서비스( service)**를 선택합니다.
  - b. 기타 AWS 서비스에 대한 사용 사례(**Use cases for other**) 드롭다운에서 **EKS**를 선택합니다.
  - c. **EKS - Fargate pod**를 선택합니다.
  - d. **다음(Next)**을 선택합니다.
5. 권한 추가(**Add permissions**) 페이지에서 **다음(Next)**을 선택합니다.
6. 이름, 검토 및 생성(**Name, review, and create**) 페이지에서 다음을 수행합니다.
  - a. 역할 이름(**Role name**)에 역할의 고유한 이름(예: **AmazonEKSFargatePodExecutionRole**)을 입력합니다.
  - b. 태그 추가(**Add tags**)(선택 사항)에서 태그를 키 값 페어로 연결하여 메타데이터를 역할에 추가합니다. IAM에서 태그 사용에 대한 자세한 내용은 **IAM 사용 설명서**의 **IAM 엔티티 태깅**을 참조하세요.
  - c. **역할 생성(Create role)**을 선택합니다.
7. **역할(Roles)** 페이지에서 **AmazonEKSFargatePodExecutionRole**에 대한 역할 목록을 검색합니다. 역할을 선택합니다.
8. **AmazonEKSFargatePodExecutionRole** 페이지에서 다음을 수행합니다.
  - a. **신뢰 관계(Trust relationships)**를 선택합니다.
  - b. **신뢰 정책 편집(Edit trust policy)**을 선택합니다.
9. **신뢰 정책 편집(Edit trust policy)** 페이지에서 다음 작업을 수행합니다.
  - a. 다음 내용을 복사하여 **신뢰 정책 편집(Edit trust policy)** 양식에 붙여 넣습니다. **region-code**을 해당 클러스터가 있는 AWS 리전으로 바꿉니다. 계정의 모든 AWS 리전에서 동일한 역할을 사용하려는 경우 **region-code**을 \*로 바꾸세요. **111122223333**를 계정 ID로, **my-cluster**를 클러스터의 이름으로 바꿉니다. 계정의 모든 클러스터에 대해 동일한 역할을 사용하려는 경우 **my-cluster**를 \*로 바꾸세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:eks:region-code:111122223333:fargateprofile/my-cluster/*"
        }
      },
      "Principal": {
        "Service": "eks-fargate-pods.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- b. **정책 업데이트(Update policy)**를 선택합니다.

## 신뢰할 수 있는 엔터티 유형

### ☒ AWS 서비스

EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

### ☐ AWS 계정

사용자 또는 서드 파티에 속한 다른 AWS 계정의 엔터티가 이 계정에서 작업을 수행하도록 허용합니다.

### ☐ 웹 자격 증명

지정된 외부 웹 자격 증명 공급자와 연동된 사용자가 이 역할을 맡아 이 계정에서 작업을 수행하도록 허용합니다.

### ☐ SAML 2.0 연동

기업 디렉터리에서 SAML 2.0과 연동된 사용자가 이 계정에서 작업을 수행할 수 있도록 허용합니다.

### ☐ 사용자 지정 신뢰 정책

다른 사용자가 이 계정에 작업을 수행할 수 있도록 사용자 지정 신뢰 정책을 생성합니다.

## 사용 사례

EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

### 일반 사용 사례

#### ☐ EC2

Allows EC2 instances to call AWS services on your behalf.

#### ☐ Lambda

Allows Lambda functions to call AWS services on your behalf.

### 다른 AWS 서비스의 사용 사례:

EKS

#### ☐ EKS

Allows EKS to manage clusters on your behalf.

#### ☐ EKS - Cluster

Allows access to other AWS service resources that are required to operate clusters managed by EKS.

#### ☐ EKS - Nodegroup

Allow EKS to manage nodegroups on your behalf.

### ☒ EKS - Fargate pod

Allows access to other AWS service resources that are required to run Amazon EKS pods on AWS Fargate.

## IAM → 역할 → 역할 생성

신뢰할 수 있는 엔터티 유형 : AWS 서비스

사용 사례 : EKS - Fargate pod

## 역할 세부 정보

### 역할 이름

이 역할을 식별하는 의미 있는 이름을 입력합니다.

EKSFargatePodExecutionRole

최대 64자입니다. 영숫자 및 '+', '@', '-' 문자를 사용하세요.

### 설명

이 역할에 대하여 간단한 설명을 추가합니다.

Allows access to other AWS service resources that are required to run Amazon EKS pods on AWS Fargate.

최대 1,000자입니다. 영숫자 및 '+', '@', '-' 문자를 사용하세요.

역할 이름 : EKSFargatePodExecutionRole

## EKSFargatePodExecutionRole

삭제

Allows access to other AWS service resources that are required to run Amazon EKS pods on AWS Fargate.

## 요약

편집

생성 날짜

September 14, 2022, 20:33 (UTC+09:00)

ARN

arn:aws:iam::694833324522:role/EKSFargatePodExecutionRole

마지막 활동

없음

최대 세션 지속 시간

1시간

권한

신뢰 관계

태그

액세스 관리자

세션 취소

## 신뢰할 수 있는 엔터티

신뢰 정책 편집

지정된 조건에서 이 역할을 수임할 수 있는 엔터티입니다.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": "eks-fargate-pods.amazonaws.com"
8       },
9       "Action": "sts:AssumeRole"
10    }
11  ]
12 }
```

역할(EKSFargatePodExecutionRole) → 신뢰 관계 → 신뢰 정책 편집

ArnLike에 EKS 클러스터 Arn을 추가한다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:eks:[region-code]:[account-id]:fargateprofile/[cluster-name]/*"
        }
      },
      "Principal": {
        "Service": "eks-fargate-pods.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```

    }
  ]
}

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Condition": {
7         "ArnLike": {
8           "aws:SourceArn": "arn:aws:eks:ap-northeast-2:694833324522:fargateprofile/eks-sts-cluster/*"
9         }
10      },
11     "Principal": {
12       "Service": "eks-fargate-pods.amazonaws.com"
13     },
14     "Action": "sts:AssumeRole"
15   }
16 ]
17 }

```

## 3.2 Fargate 프로파일 생성

**ⓘ** AWS Fargate는 현재 Amazon EKS 포드 개수 기반 할당량에서 vCPU 기반 할당량으로 서비스 할당량을 마이그레이션하고 있습니다. 새로운 vCPU 환경에 익숙해지려면 [자세히 알아보기](#) [🔗](#)을(를) 참조하세요.

**Fargate 프로파일 (0) 정보** 편집 삭제 Fargate 프로파일 추가

프로파일 이름	네임스페이스	상태
<p><b>Fargate 프로파일 없음</b></p> <p>이 클러스터에는 Fargate 프로파일이 없습니다.</p> <p><span>Fargate 프로파일 추가</span></p>		

EKS Cluster → 컴퓨팅 탭 > Fargate 프로파일 추가



### 프로파일 구성

프로파일을 생성한 후에는 이러한 속성을 변경할 수 없습니다.

#### 이름

이 프로파일에 대한 고유한 이름을 할당합니다.

kube-system

Fargate 프로파일 이름은 문자 또는 숫자로 시작해야 하며 유니코드 문자 세트, 숫자, 하이픈 및 밑줄을 사용할 수 있습니다. 최대 길이는 63자입니다.

#### 포드 실행 역할 정보

Fargate에서 클러스터에 연결하고 컨테이너 이미지를 가져오는 데 사용할 IAM 역할을 선택합니다. 새 포드 실행 역할을 생성하려면 [Amazon EKS 사용 설명서](#)의 지침을 따르세요.

EKSFargatePodExecutionRole

#### 서브넷 정보

포드가 실행될 VPC의 서브넷을 지정합니다. 새 서브넷을 생성하려면 [VPC 콘솔](#)의 해당 페이지로 이동합니다.

서브넷 선택

subnet-0ada68c306ec98501

subnet-035c27d5461bac818

이름 : kube-system

파드 실행 역할 : EKSFargatePodExecutionRole

서브넷 : subnet-sts-private-a, subnet-sts-private-c

### 포드 선택기 정보

프로파일을 생성한 후에는 이러한 속성을 변경할 수 없습니다.

#### 네임스페이스

포드를 선택할 네임스페이스를 추가합니다.

kube-system

지우기

▶ 레이블 일치 (0)

네임스페이스 추가

네임스페이스 : kube-system

## 3.3 CoreDNS pod 수정

default 로 EC2 위에서 수행되도록 설정되어 있기 때문에 Fargate 위에서 수행되도록 수정해준다.  
[eks.amazonaws.com/compute-type](https://eks.amazonaws.com/compute-type)<sup>1</sup>: ec2 주식 제거

```
kubectl patch deployment coredns \
  -n kube-system \
  --type json \
  -p='[{"op": "remove", "path": "/spec/template/metadata/annotations/eks.amazonaws.com~1compute-type"}]'
```

재기동

```
kubectl rollout restart -n kube-system deployment coredns
```

배포 확인

```
kubectl get pods -A |grep coredns
```

---

<sup>1</sup> [http://eks.amazonaws.com/compute-type](https://eks.amazonaws.com/compute-type)