AppArmor로 안전하게 지켜지는 쿠버네티스 컨테이너 환경

조 훈 (Hoon Jo)

CCIE DC, CK{ A | AD | S }, VCIX-NV6

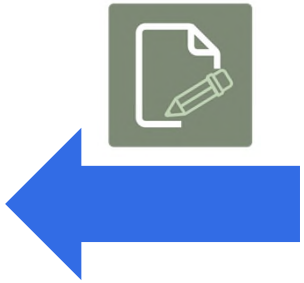
https://github.com/SysNet4Admin https://www.linkedin.com/in/hoonjo/

AppArmor

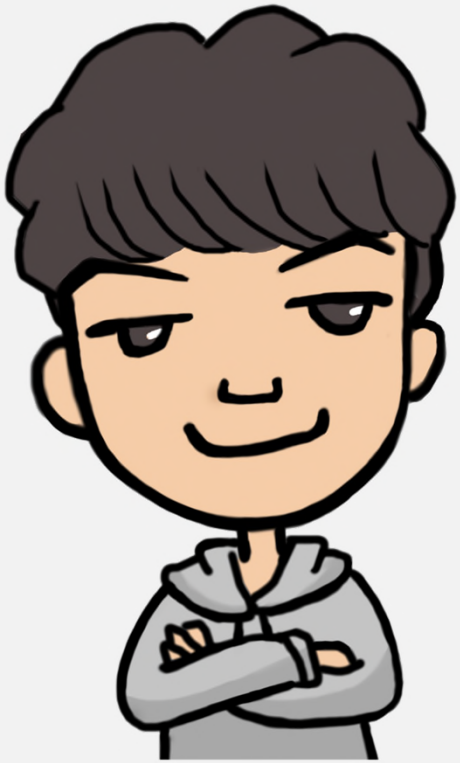
- Profile 기반으로 애플리케이션 제한
- SElinux보다 사용하기 쉬움
- 우분투 배포판에 기본으로 포함됨

Kubernetes


pod



[클라우드☁솔루션_아키텍트]@Magazone



시스템/네트워크 IT 벤더의 경험 이후 Megazone GCP 클라우드 팀으로 자리를 옮겨서 클라우드 기술 스택을 쌓고 있다. 근 시일 내에 쿠버네티스가 모든 인프라의 기반 기술이 될 것이라고 믿고 있으며 이에 발 맞추어 『 **컨테이너 인프라 환경 구축을 위한 쿠버네티스/도커** (길벗) 』책을 집필했다.

인프런/유데미에서 인프라 자동화를 위한 앤서블에 대한 강의를 진행하고 있으며, 또한 쿠버네티스 지식을 더 나누고 싶어 인프런에 '공인 쿠버네티스 자격증 잘 준비하는 법 (CKA, CKAD, CKS)', '쉽게 시작하는 쿠버네티스', '그림으로 배우는 쿠버네티스 ' 그리고 실습으로 배우는 프로메테우스 강의를 기재하였다. 또한 페이스북에 있는 'IT 인프라 엔지니어 그룹' 의 운영진을 맡고 있다.

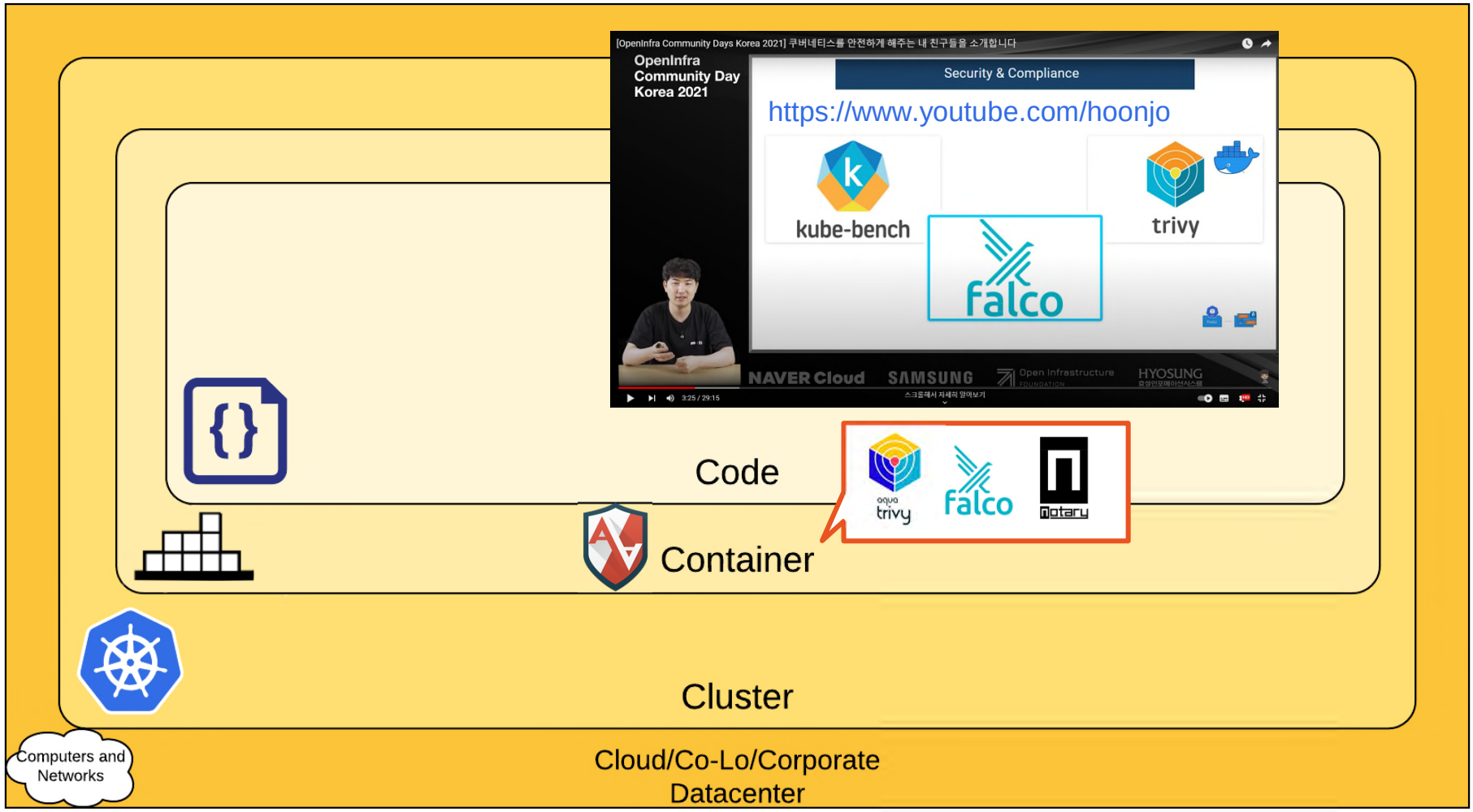
이외에 집필한 책으로는『시스템/네트워크 관리자를 위한 파이썬 실무 프로그래밍』(위키북스)』과『우아하게 앤서블』(비제이퍼블릭) 이 있고 IT잡지에 기고문을 쓰는 것을 즐긴다.

진행 순서

1. AppArmor가 보호하는 부분
2. AppArmor가 쿠버네티스 환경에서 적용되는 구조
3. AppArmor live DEMO
4. TL;DR & Tip

진행 순서

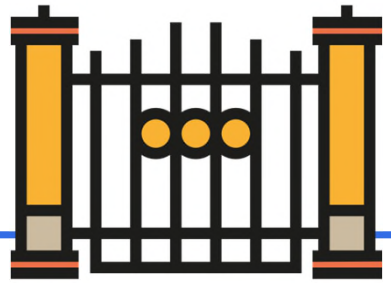
1. **AppArmor가 보호하는 부분**
2. AppArmor가 쿠버네티스 환경에서 적용되는 구조
3. AppArmor live DEMO
4. TL;DR & Tip



The 4C's of Cloud Native security (https://kubernetes.io/docs/concepts/security/overview/)

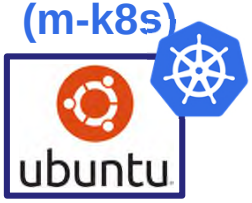
진행 순서

1. AppArmor가 보호하는 부분
2. **AppArmor가 쿠버네티스 환경에서 적용되는 구조**
3. AppArmor live DEMO
4. TL;DR & Tip



쿠버네티스 클러스터

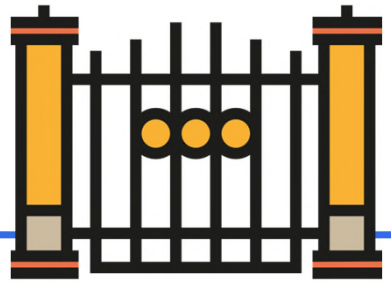
마스터 노드
(m-k8s)



워커 노드#1
(w1-k8s)

워커 노드#2
(w2-k8s)

워커 노드#3
(w3-k8s)



쿠버네티스 클러스터

1. apparmor-loader를 데몬셋으로 배포해서 적용
2. 앤서블(Ansible)로 프로파일을 배포 후 적용
3. Shell Script로 프로파일을 전달 및 적용

마스터 노드
(m-k8s)

워커 노드#1
(w1-k8s)

워커 노드#2
(w2-k8s)

워커 노드#3
(w3-k8s)

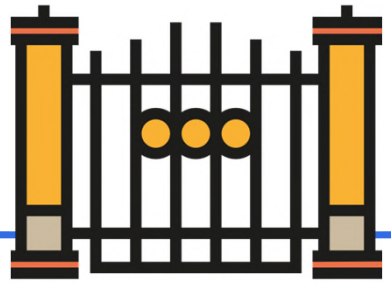
```yaml
apiVersion: v1
kind: Pod
metadata:
  labels:
    run: aa-sleepy
  name: aa-sleepy
  annotations:
    # Tell Kubernetes to apply the AppArmor profile "deny-write".
    # Note that this is ignored if the Kubernetes node is not running version 1.4 or greater.
    container.apparmor.security.beta.kubernetes.io/aa-sleepy: localhost/deny-write
spec:
  containers:
  - image: sysnet4admin/sleepy
    name: aa-sleepy
```

진행 순서

1. AppArmor가 보호하는 부분
2. AppArmor가 쿠버네티스 환경에서 적용되는 구조
3. **AppArmor live DEMO**
4. TL;DR & Tip

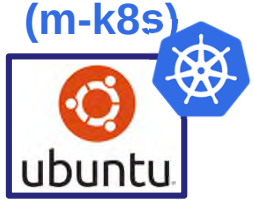
진행 순서

1. AppArmor가 보호하는 부분
2. AppArmor가 쿠버네티스 환경에서 적용되는 구조
3. AppArmor live DEMO
4. **TL;DR & Tip**



쿠버네티스 클러스터

마스터 노드
(m-k8s)



워커 노드#1
(w1-k8s)

워커 노드#2
(w2-k8s)

워커 노드#3
(w3-k8s)

```
#fileName: deny-write

#include <tunables/global>

profile deny-write flags=(attach_disconnected) {
  #include <abstractions/base>

  file,
  # Deny all path write
  deny /** w,
}
```


```yaml
apiVersion: crd.security.sysdig.com/v1alpha1
kind: AppArmorProfile
metadata:
  name: deny-write
spec:
  # Add fields here
  enforced: true
  rules: |
    # read only file paths
    file,
    deny /** w,
```

kube-apparmor-manager (https://github.com/sysdiglabs/kube-apparmor-manager)

```yaml
apiVersion: crd.security.sysdig.com/v1alpha1
kind: AppArmorProfile
metadata:
  name: apparmorprofile-sample
spec:
  rules: |
    # This is the default deny mode of AppArmor profile.
    # List the allow rules here separated by new line character.

    # allow few read/write activities
    allow /etc/* r,
    allow /tmp/* rw,

    # allow few commands execution
    allow /bin/echo mrix,
    allow /bin/sleep mrix,
    allow /bin/cat mrix,
  enforced: true # set profile to enforcement mode if true (complain mode if false)
```

kube-apparmor-manager (https://github.com/sysdiglabs/kube-apparmor-manager)


```
$ kubectl krew install apparmor-manager

$ kubectl apparmor-manager status
+-------------------------------+---------------+-----------------+--------+-------------------+
|           NODE NAME           |  INTERNAL IP  |   EXTERNAL IP   |  ROLE  | APPARMOR ENABLED  |
+-------------------------------+---------------+-----------------+--------+-------------------+
| ip-172-20-45-132.ec2.internal | 172.20.45.132 | 54.91.xxx.xx    | master | false             |
| ip-172-20-54-2.ec2.internal   | 172.20.54.2   | 54.82.xx.xx     | node   | true              |
| ip-172-20-58-7.ec2.internal   | 172.20.58.7   | 18.212.xxx.xxx  | node   | true              |
+-------------------------------+---------------+-----------------+--------+-------------------+

$ kubectl apparmor-manager enforced
+-------------------------------+--------+-----------------------------------------------------------+
|           NODE NAME           |  ROLE  |                     ENFORCED PROFILES                     |
+-------------------------------+--------+-----------------------------------------------------------+
| ip-172-20-48-62.ec2.internal  | node   | /usr/sbin/ntpd,docker-default,k8s-apparmor-example-deny-write |
| ip-172-20-77-231.ec2.internal | node   | /usr/sbin/ntpd,docker-default,k8s-apparmor-example-deny-write |
| ip-172-20-80-19.ec2.internal  | master |                                                           |
| ip-172-20-97-60.ec2.internal  | node   | /usr/sbin/ntpd,docker-default,k8s-apparmor-example-deny-write |
+-------------------------------+--------+-----------------------------------------------------------+
```

kube-apparmor-manager (https://github.com/sysdiglabs/kube-apparmor-manager)

Thank you!

Any Questions?

https://github.com/SysNet4Admin

https://www.linkedin.com/in/hoonjo/