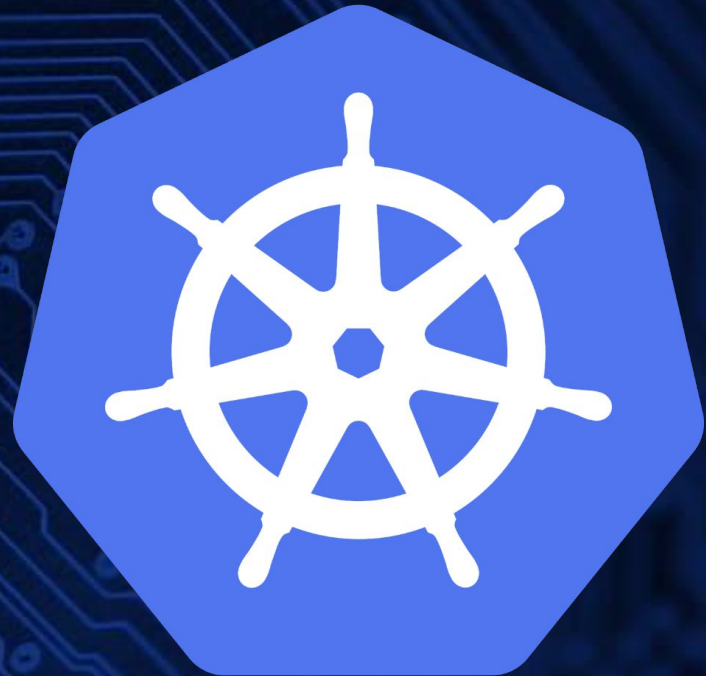


---

# CKS : Complete Certification Guide

Exploring AppArmor



### AppArmor

- AppArmor is Linux Security Kernel Module.
- This module provides granular Access Control for programs running on Linux System. Use AppArmor to control and limit what a program can do within the Host OS.
- An AppArmor Profile is a Set of rules that define what a program can do and cannot do.

### AppArmor

- Below AppArmor Profile will prevent the program from writing any data to the Disk.

```
profile k8s-deny-write flags=(attach_disconnected) {  
  
    file,  
  
    deny /** w,  
  
}
```

### AppArmor

- AppArmor profile can be loaded into AppArmor at the server level and activated in one of the two modes.
- **Complain Mode** : AppArmor generate a report on what the program is doing. This is useful to discover, what the program does normally.
- **Enforce Mode** : Load a profile in enforce mode, and AppArmor will actively prevent program from doing anything that the profile does not allow.

### AppArmor

- AppArmor profile needs to be enabled on the Server the Pod is running on, or the Pod won't start.

# Thank You...

Don't be the Same! Be Better!!!

---