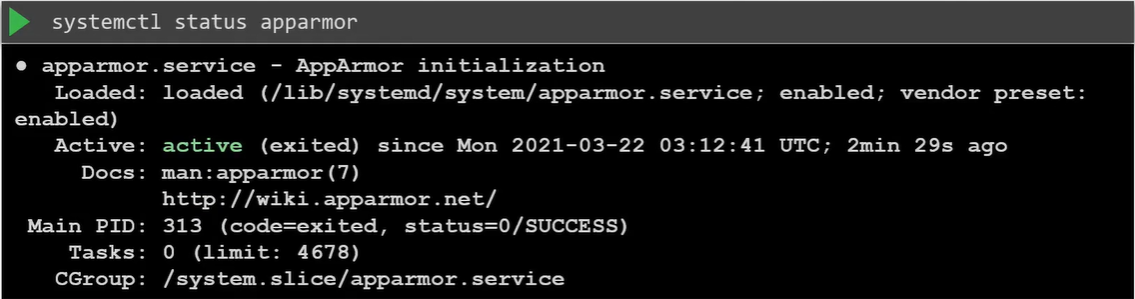
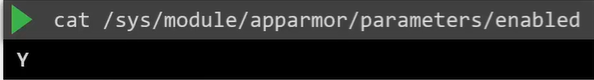
**K8S APP ARMOR**

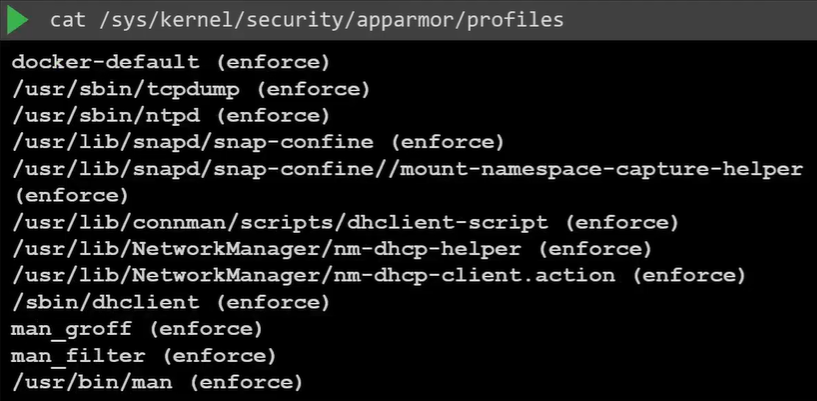
SECCOMP can restrict the system calls for a pod but cannot restrict a program’s access to specific objects, such as files or a directory.

AppArmor is a linux security module to confine a program to a limited set of resources.





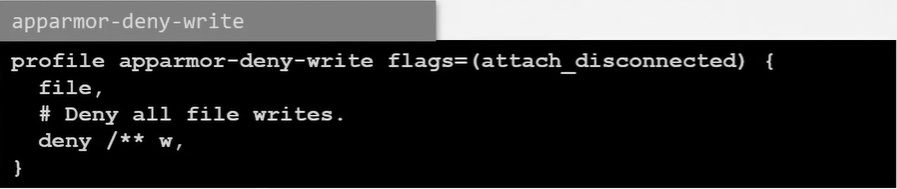
AppArmor profiles defines what resources can be used by an application

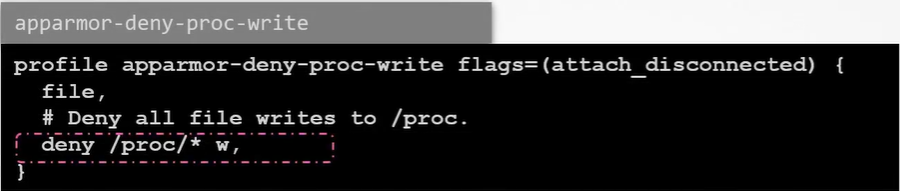


Apparmor-deny-write profile contains 2 rules:

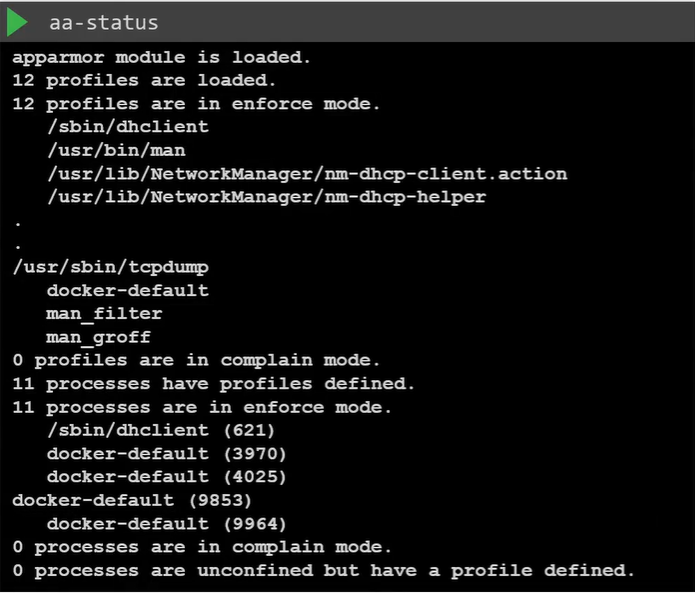
file: allows complete access to the entire file system

deny: prevent write access to all files under the root file system





Check Apparmor loaded profiles and its status



Enforce mode: apparmor will monitor and enforce the rules on any application that fits the profile.

Complain mode: apparmor will allow application to perform tasks without any restriction, only log them as events.

Unconfined mode: apparmor will allow application to perform tasks without any restriction and not log them as events

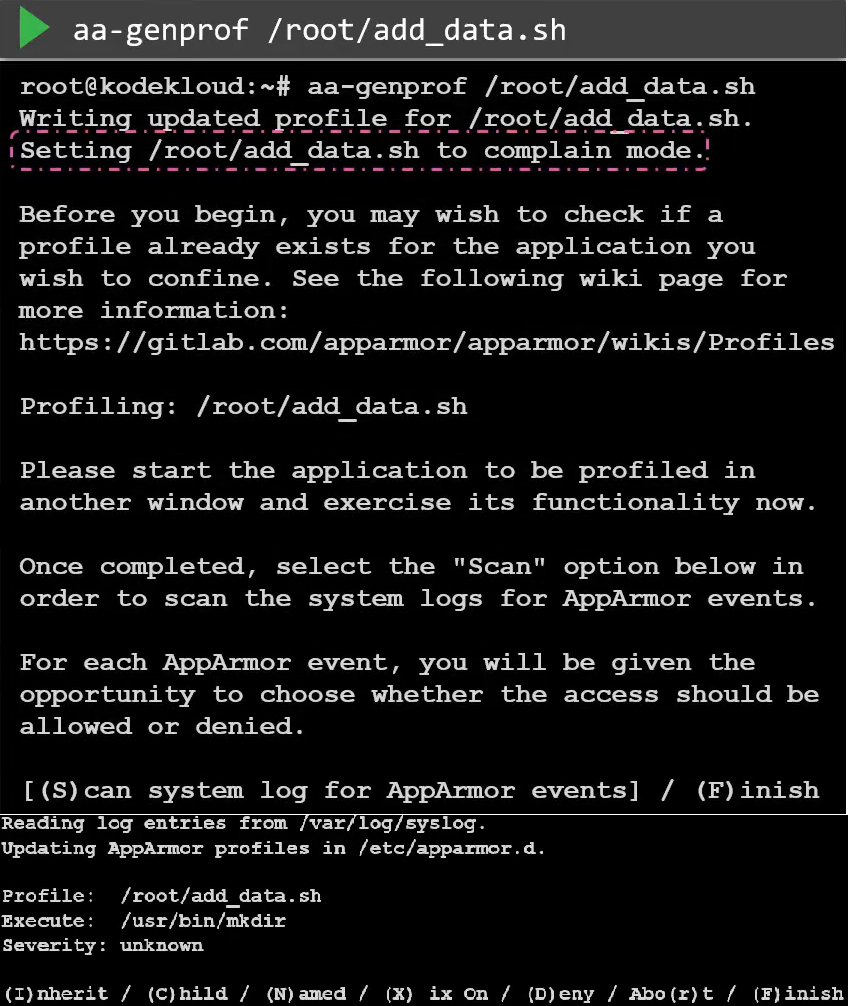
1. Create custom application-specific profiles

Use apparmor-utils

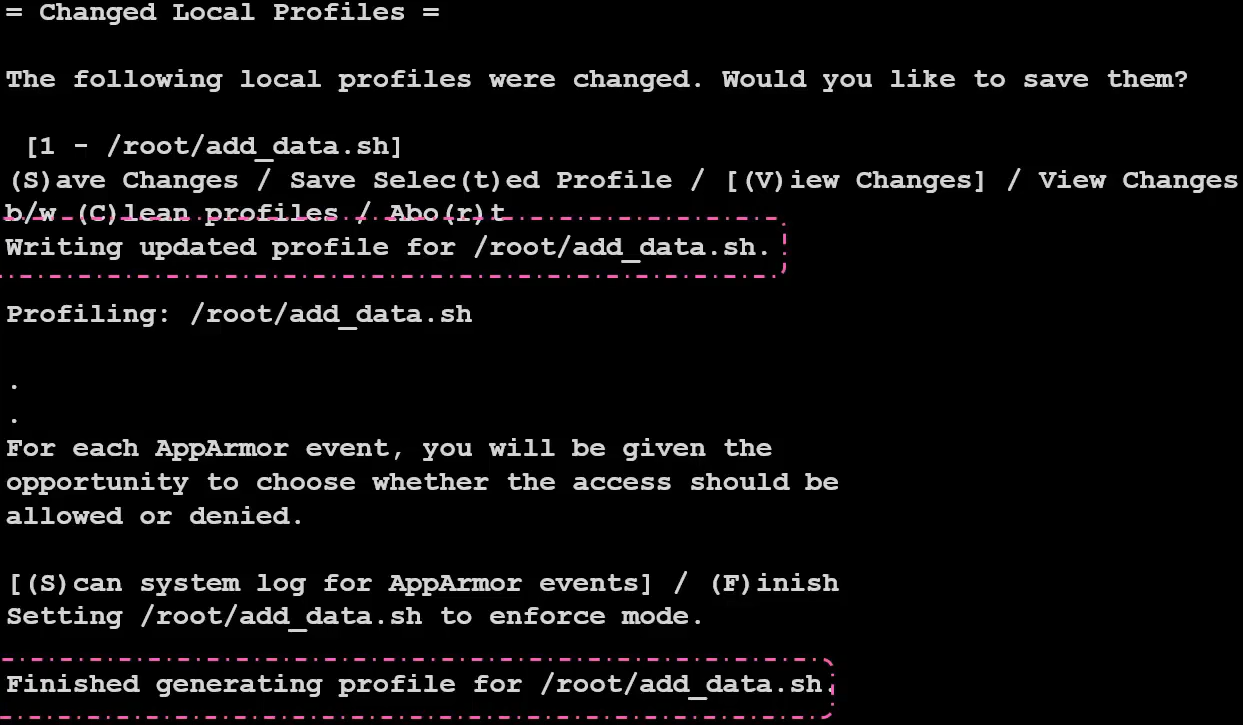
* 1. Create a script as an APP



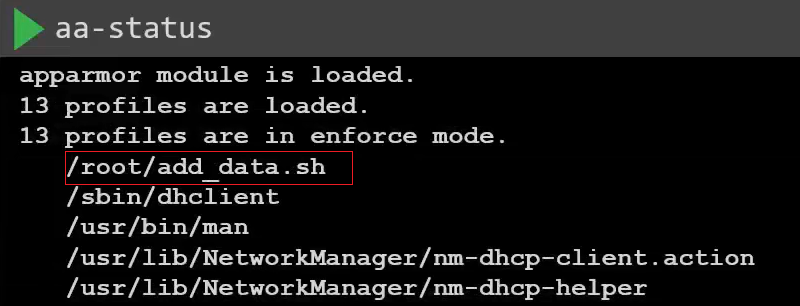
* 1. Create a profile for add\_data.sh

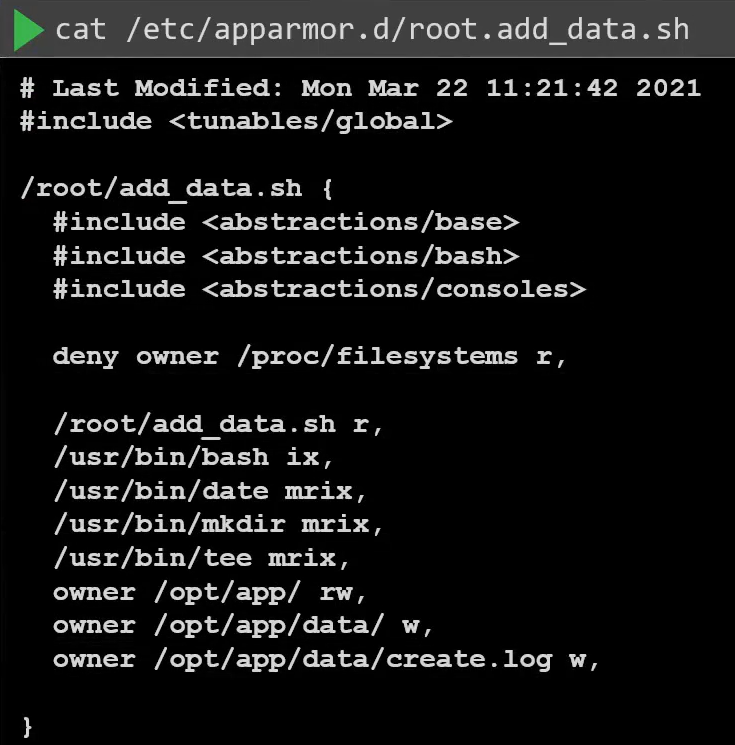


To grant access for mkdir command, need select “Inherit”, enter “I”. do the same for the next event until create the profile

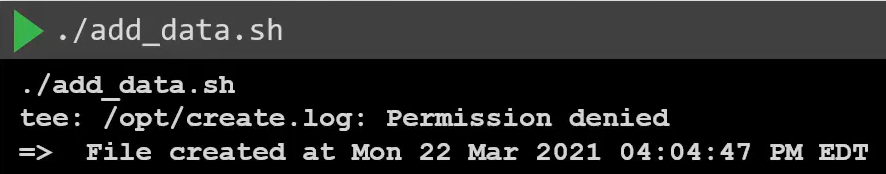


Check newly create profile





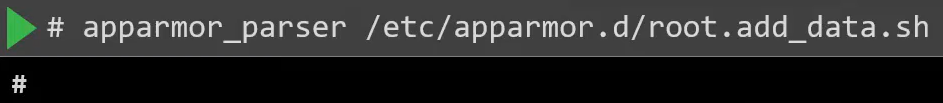
When change the “data\_directory” from “/opt/app” to “/opt” of add\_data.sh, the script will be permission denied.



* 1. Check if the profile is loaded successfully

Success:

Add Profile



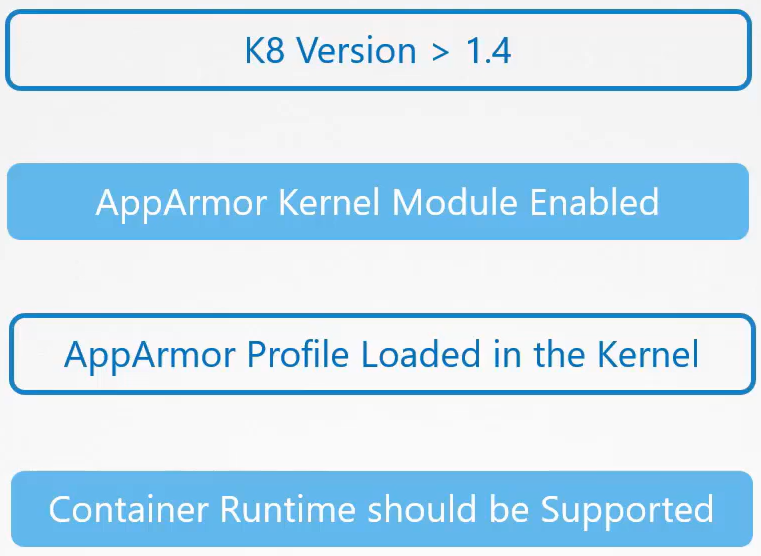
* 1. Disable the profile



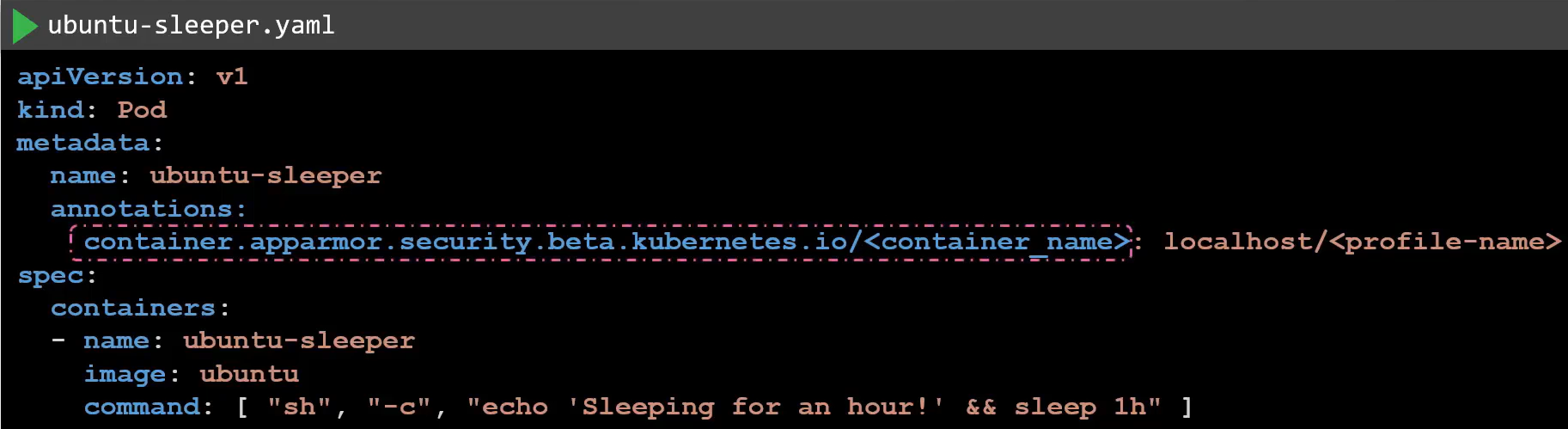


1. AppArmor in K8S

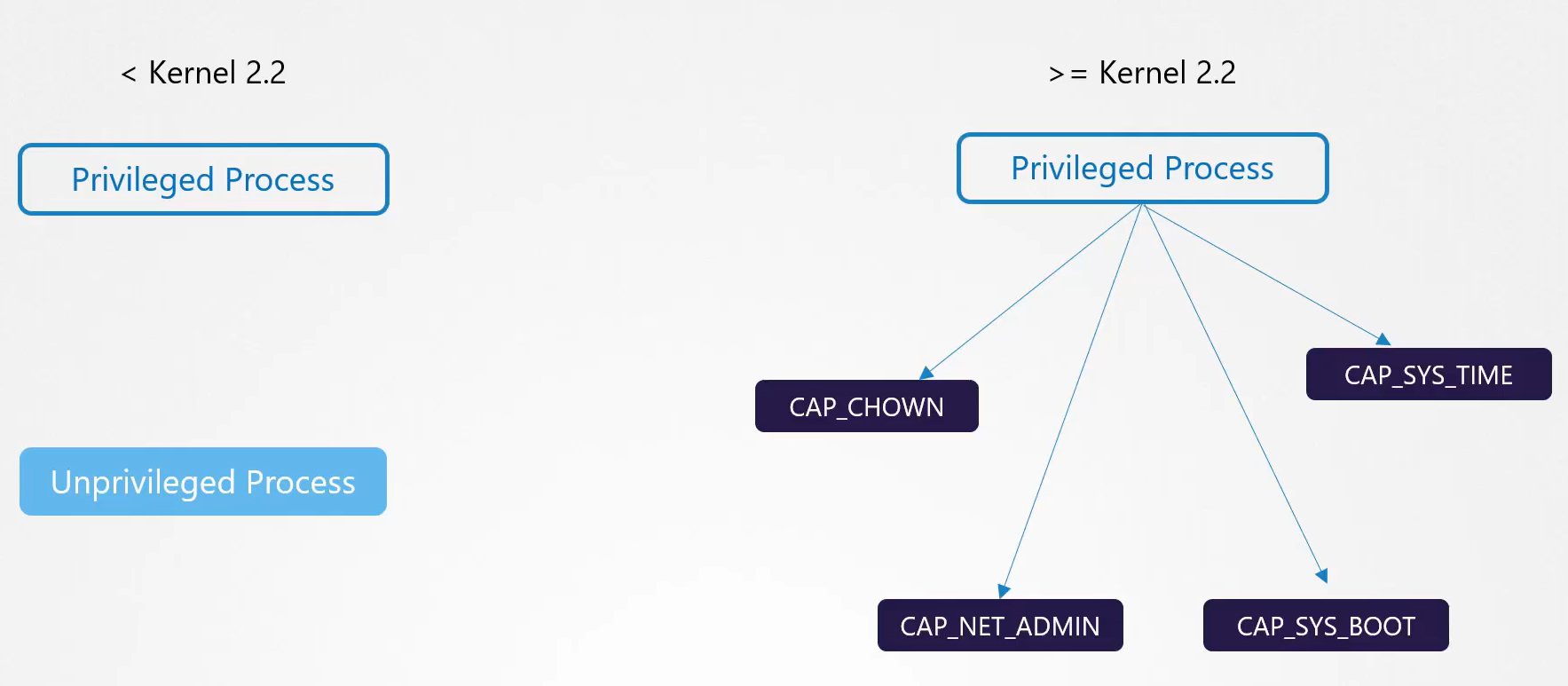
2.0. Prerequest



2.1.

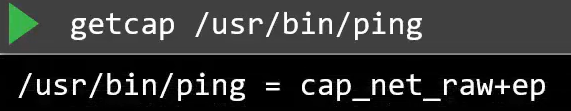


1. Add/Drop Linux Capabilities on K8S pods

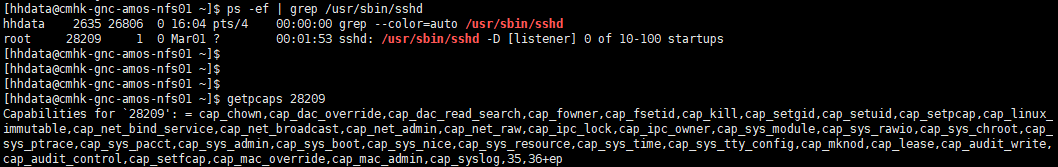




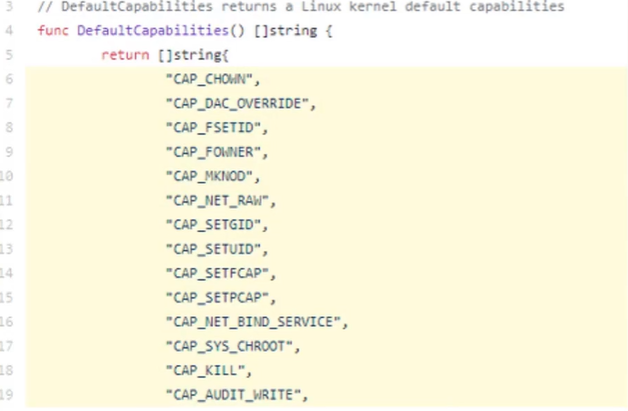
Check which capabilities the command needs:



By PID



When start docker container, it only grant some of capabilities.

  
3.1. Change capabilities when start the container

