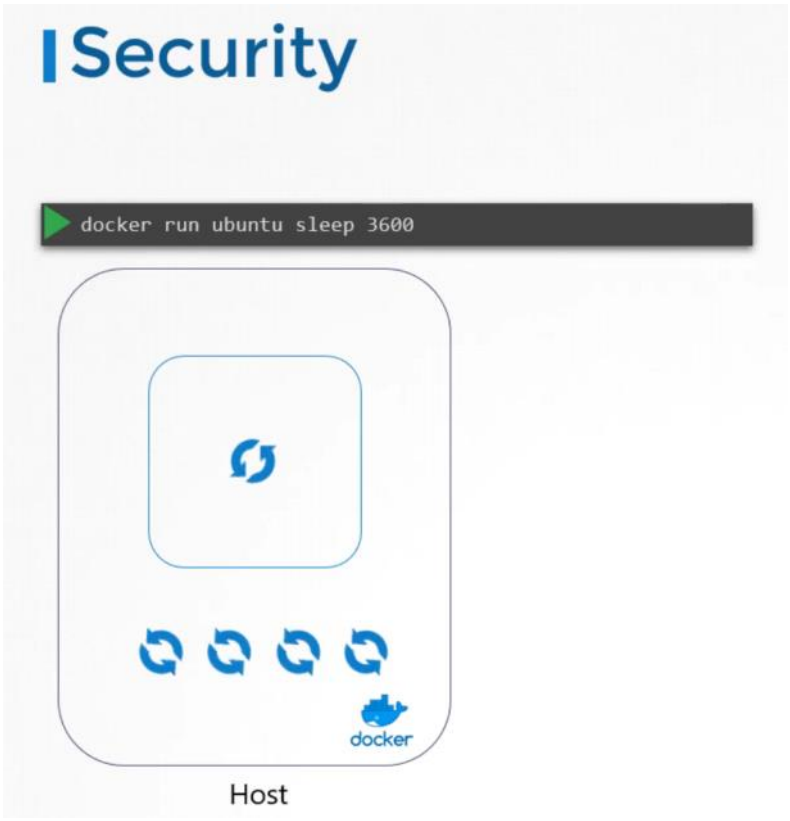
Monday, 24 October 2022 14.10

Docker Security



Security

```
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0   4528   828 ?        Ss   03:06   0:00 sleep 3600
```

Container

Security - Users

```
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
project     3720  0.1  0.1  95500  4916 ?        R    06:06   0:00 sshd: project@pts/0
project     3725  0.0  0.1  95196  4132 ?        S    06:06   0:00 sshd: project@notty
project     3727  0.2  0.1  21352  5340 pts/0    Ss   06:06   0:00 -bash
root        3802  0.0  0.0   8924  3616 ?        Sl   06:06   0:00 docker-containerd-
shim -namespace m
root        3816  1.0  0.0   4528   828 ?        Ss   06:06   0:00 sleep 3600
```

Host

```
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0   4528   828 ?        Ss   03:06   0:00 sleep 3600
```

```
docker run --user=1000 ubuntu sleep 3600
```

```
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
1000           1  0.0  0.0   4528   828 ?        Ss   03:06   0:00 sleep 3600
```

Dockerfile

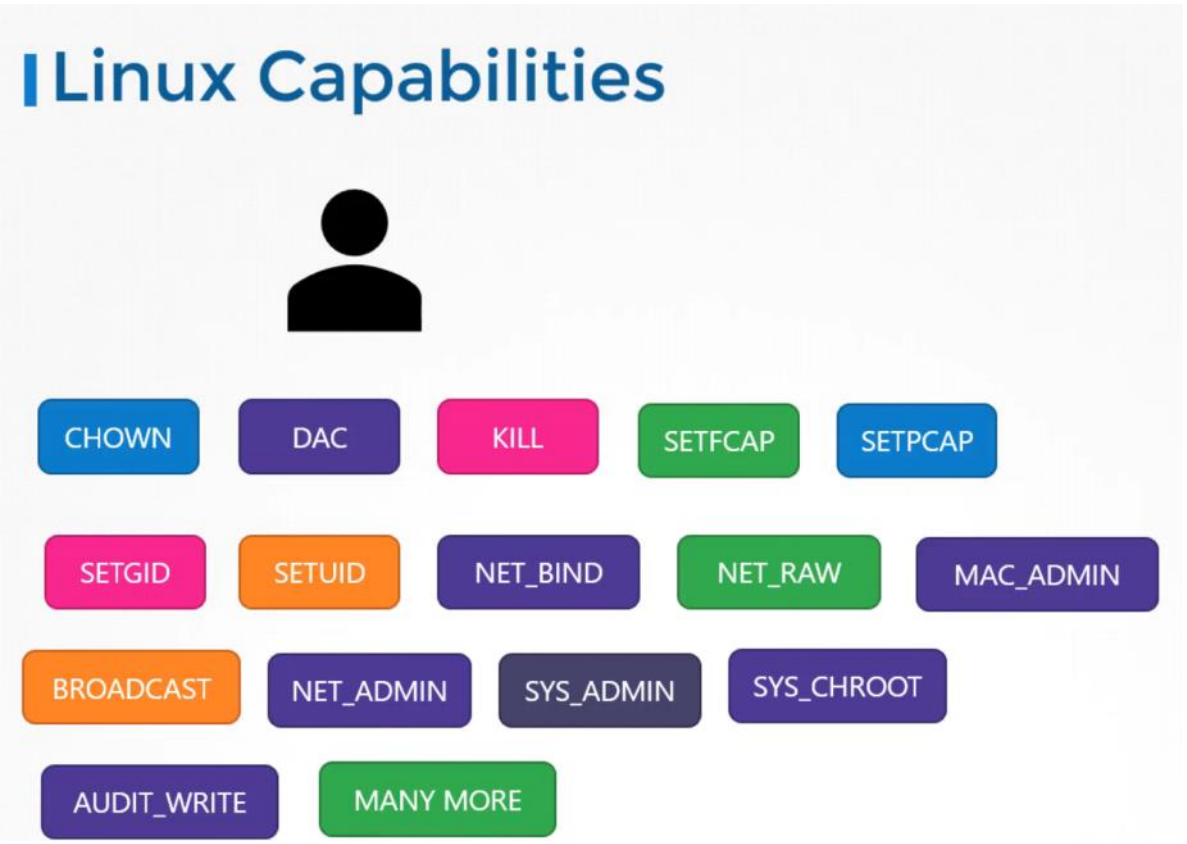
```
FROM ubuntu

USER 1000
```

```
docker build -t my-ubuntu-image .
```

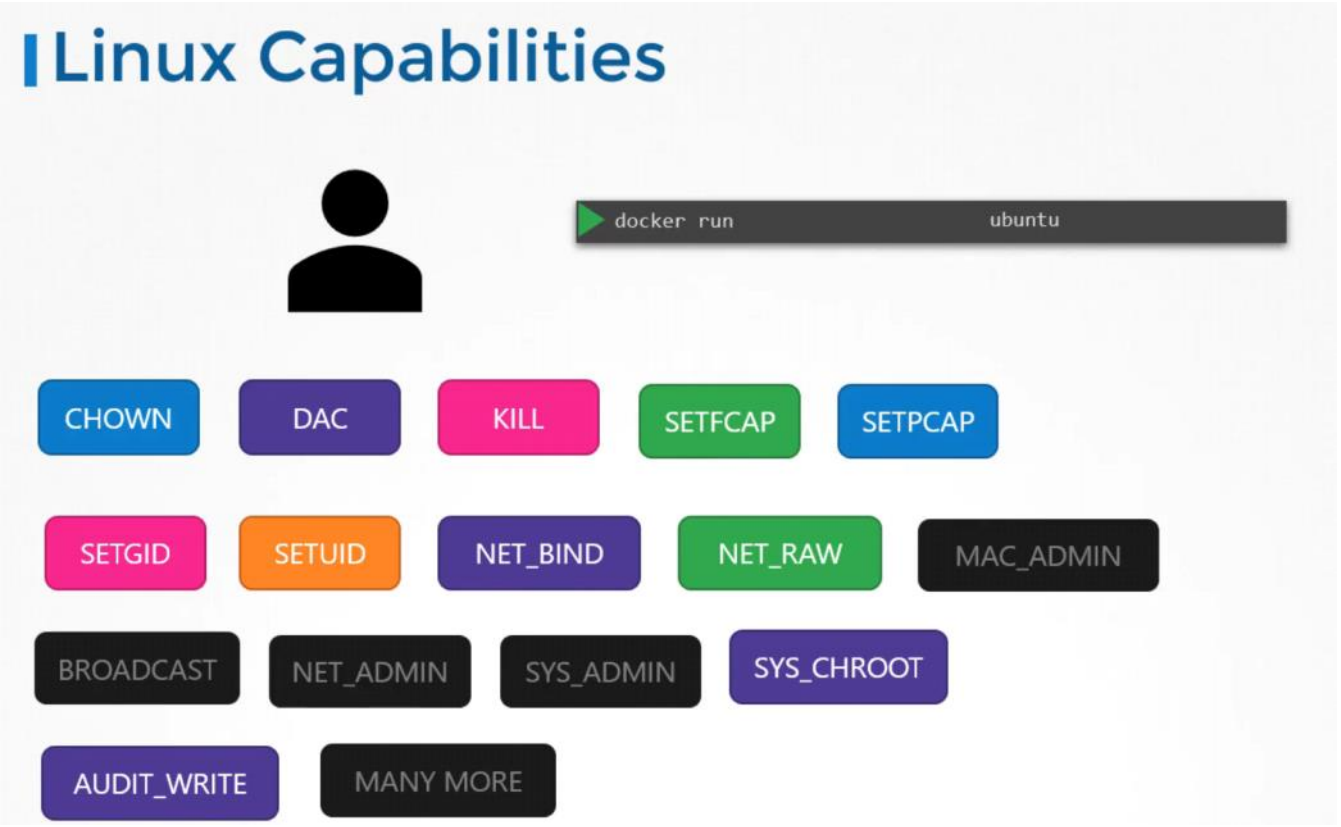
```
docker run my-ubuntu-image sleep 3600
```

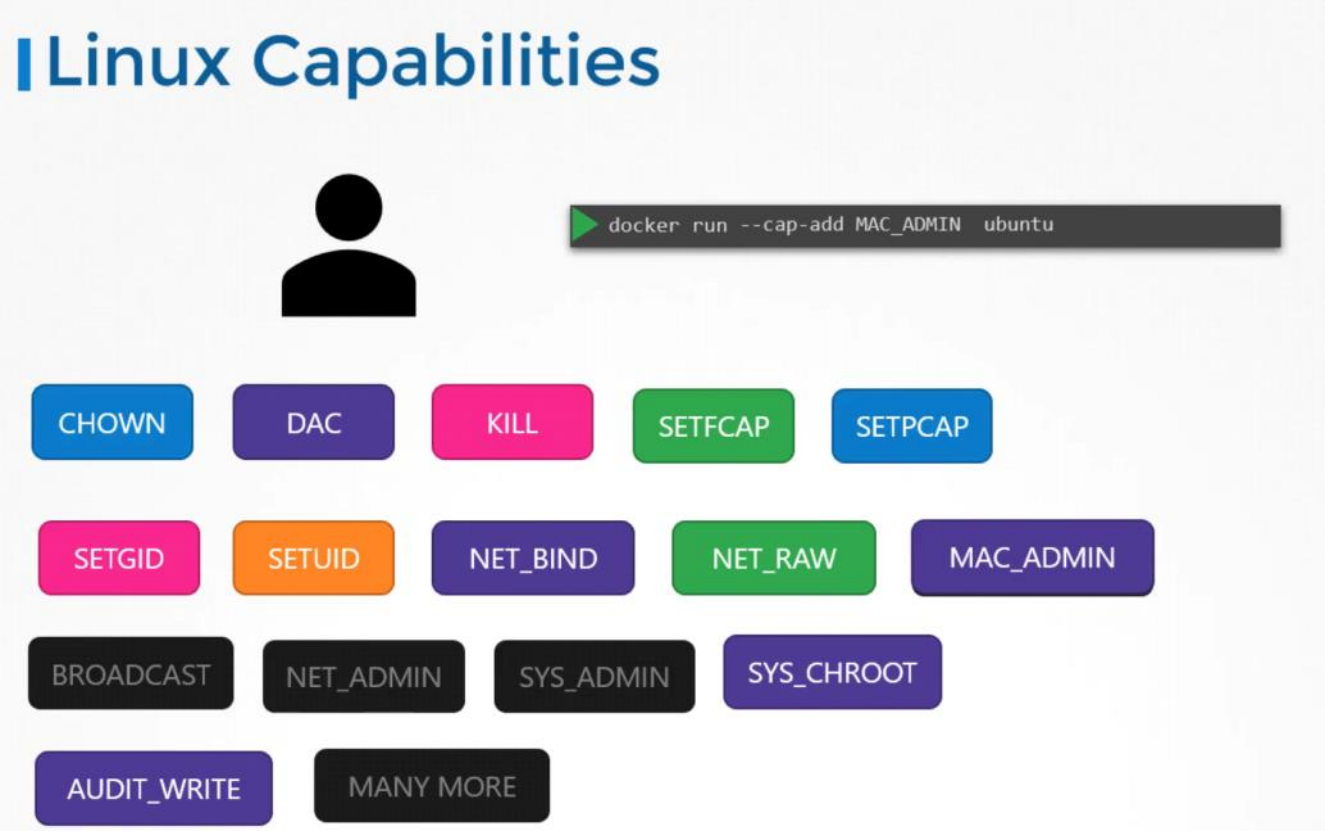
```
ps aux
```

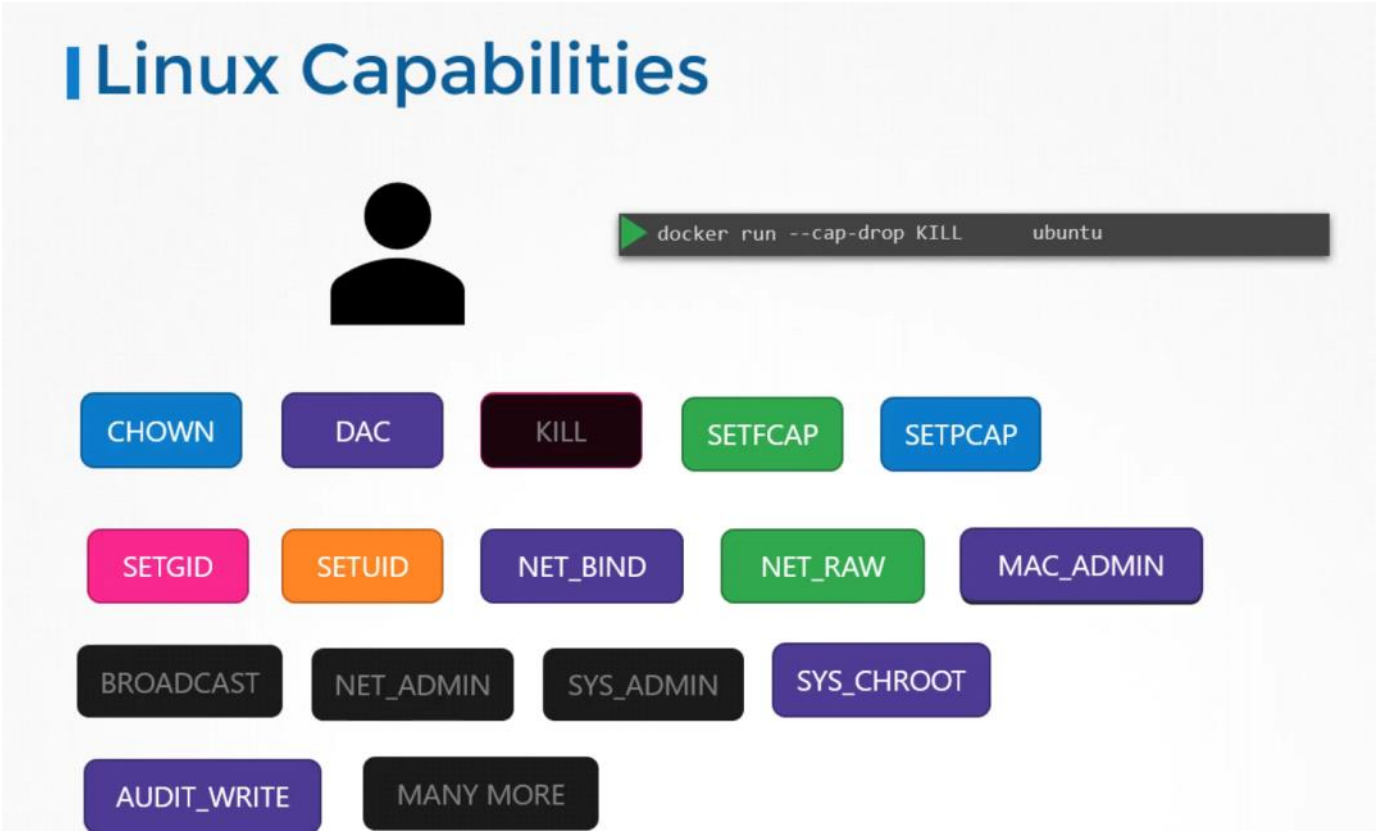
```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
1000           1  0.0  0.0   4528   828 ?        Ss   03:06   0:00 sleep 3600
```

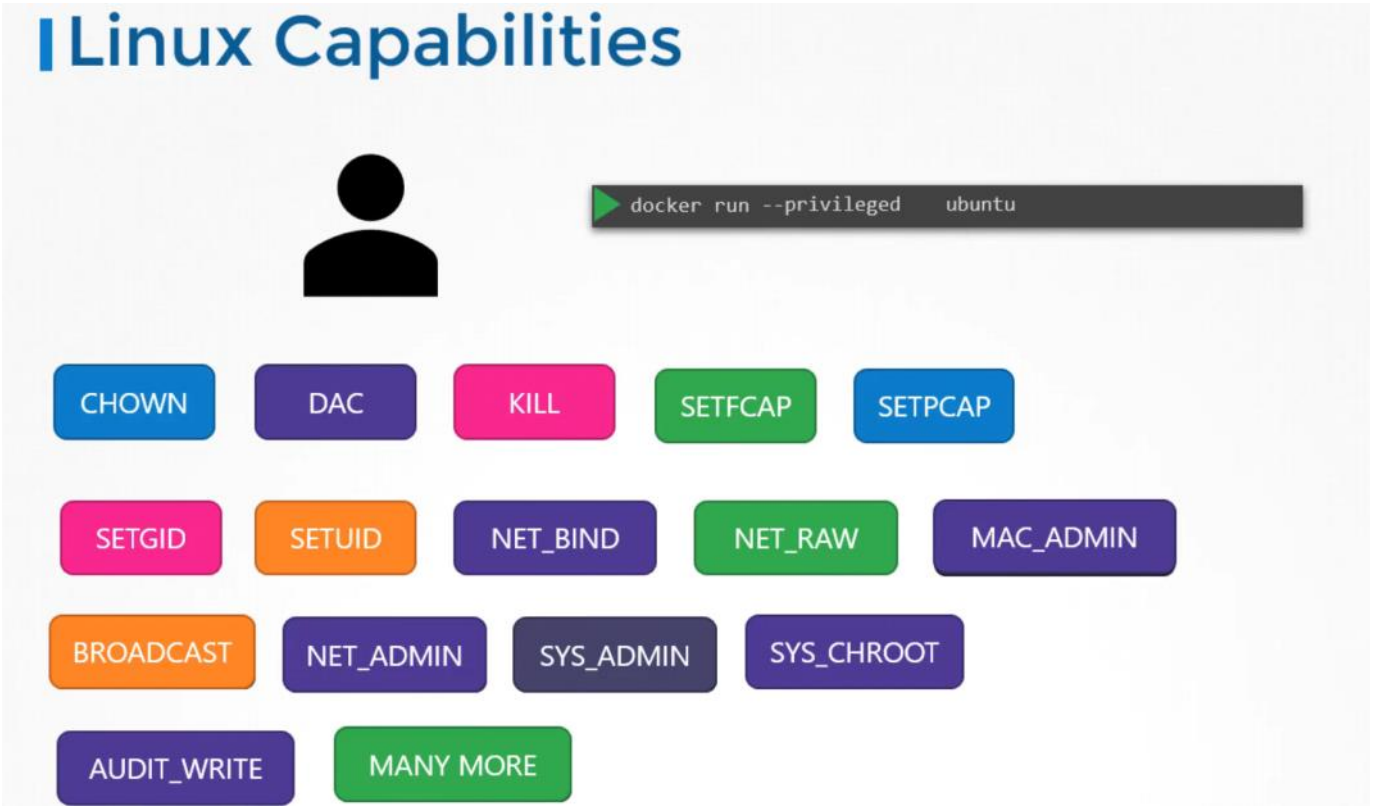


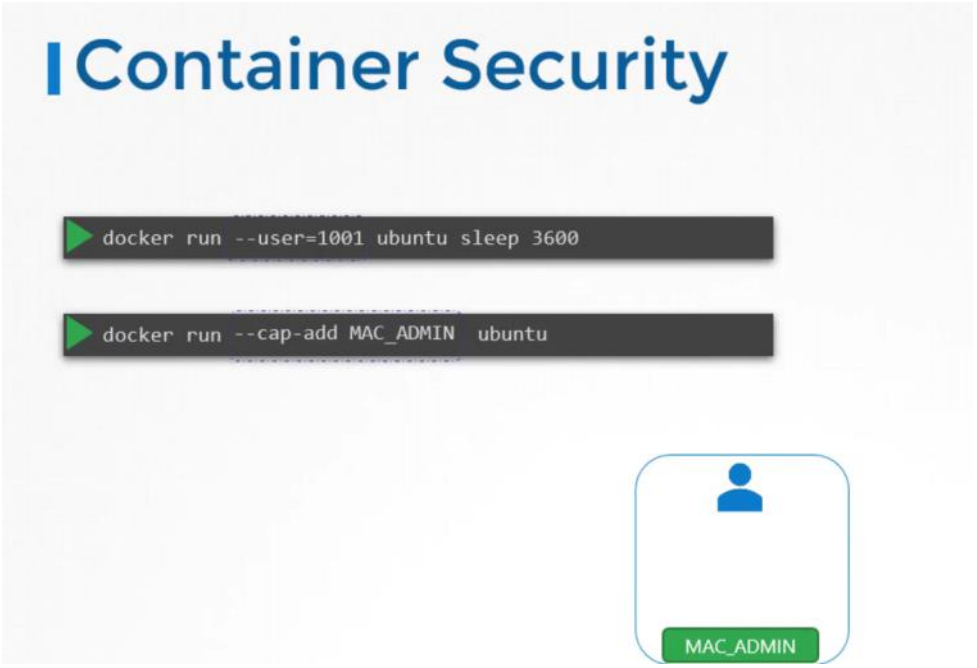
/usr/include/linux/capability.h

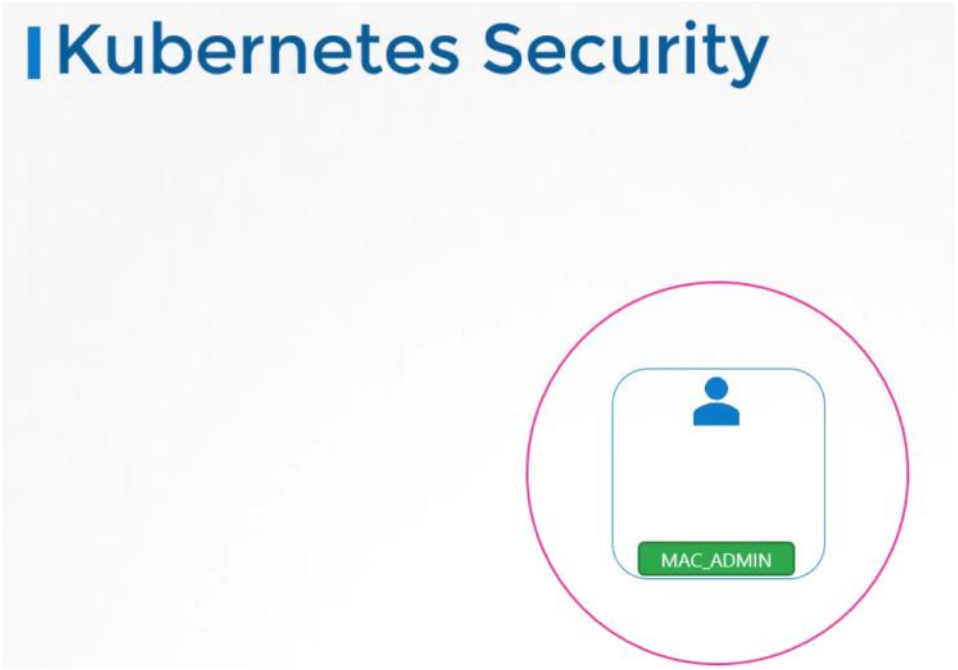

Linux Capabilities
docker run ubuntu
CHOWN
DAC
KILL
SETFCAP
SETPCAP
SETGID
SETUID
NET_BIND
NET_RAW
MAC_ADMIN
BROADCAST
NET_ADMIN
SYS_ADMIN
SYS_CHROOT
AUDIT_WRITE
MANY MORE


Linux Capabilities
docker run --cap-add MAC_ADMIN ubuntu
CHOWN
DAC
KILL
SETFCAP
SETPCAP
SETGID
SETUID
NET_BIND
NET_RAW
MAC_ADMIN
BROADCAST
NET_ADMIN
SYS_ADMIN
SYS_CHROOT
AUDIT_WRITE
MANY MORE

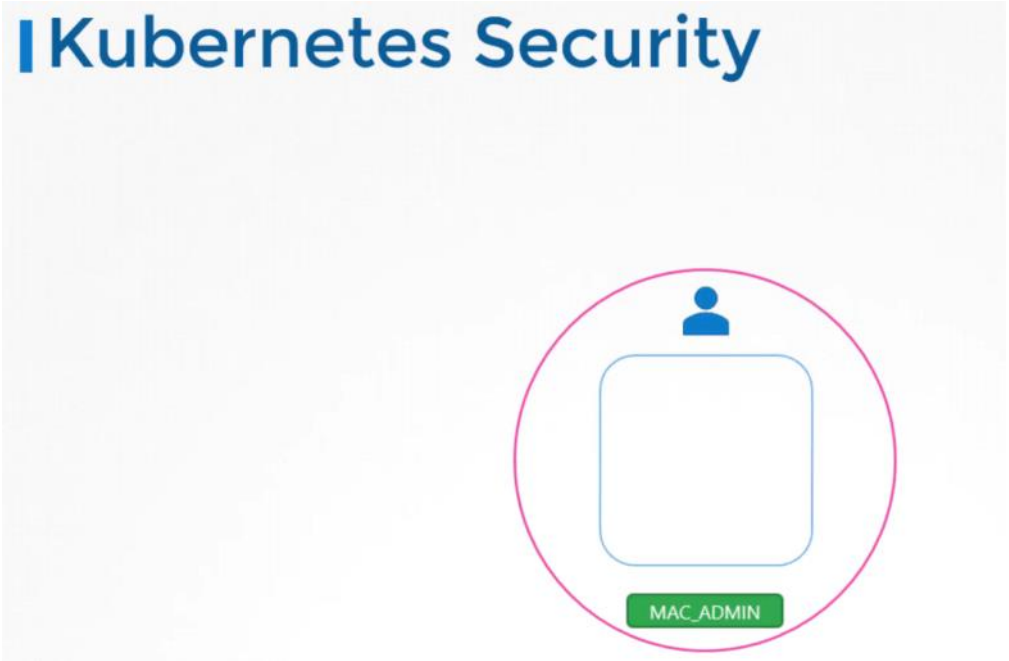

Linux Capabilities
docker run --cap-drop KILL ubuntu
CHOWN
DAC
KILL
SETFCAP
SETPCAP
SETGID
SETUID
NET_BIND
NET_RAW
MAC_ADMIN
BROADCAST
NET_ADMIN
SYS_ADMIN
SYS_CHROOT
AUDIT_WRITE
MANY MORE


Linux Capabilities
docker run --privileged ubuntu
CHOWN
DAC
KILL
SETFCAP
SETPCAP
SETGID
SETUID
NET_BIND
NET_RAW
MAC_ADMIN
BROADCAST
NET_ADMIN
SYS_ADMIN
SYS_CHROOT
AUDIT_WRITE
MANY MORE





CONTAINER LEVEL

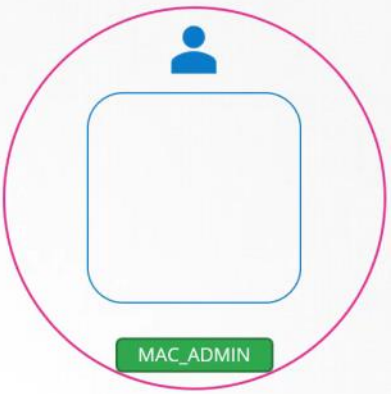


POD LEVEL


```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web-pod
spec:
 containers:
      - name: ubuntu
        image: ubuntu
        command: ["sleep", "3600"]
```

Security Context

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web-pod
spec:
 securityContext:
   runAsUser: 1000


 containers:
      - name: ubuntu
        image: ubuntu
        command: ["sleep", "3600"]
```



Security Context

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web-pod
spec:
  containers:
      - name: ubuntu
        image: ubuntu
        command: ["sleep", "3600"]
        securityContext:
          runAsUser: 1000
```

Security Context

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web-pod
spec:
  containers:
      - name: ubuntu
        image: ubuntu
        command: ["sleep", "3600"]
        securityContext:
          runAsUser: 1000
          capabilities:
              add: ["MAC_ADMIN"]
```

Note: Capabilities are only supported at the container level and not at the POD level

```
controlplane ~ ➜ kubectl exec ubuntu-sleeper -- whoami
root
```

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: multi-pod
spec:
  securityContext:
    runAsUser: 1001
  containers:
  -  image: ubuntu
     name: web
     command: ["sleep", "5000"]
     securityContext:
      runAsUser: 1002

  -  image: ubuntu
     name: sidecar
     command: ["sleep", "5000"]
```

So there's one at the pod level and then there's one at the container level.

So as we've learned, the container level is less security.

Context is going to override whatever is specified here.

And the sidecar container does not have a security context specified, so it's always going to use this.

```
    runAsUser: 1001
```