
CKS : Complete Certification Guide

Understanding Host OS Security
Concerns



Host OS Security

- Host Operating System security is very Important.
- If Attacker gain the access of Pod running on Worker Node, and then can gain the access of Host Machine.
 - Attacker can gain the access of other Running Pods on that Worker Node.
 - Attacker can gain the access of other Worker Nodes in Cluster.
 - Attacker Can gain the Access of Master Node and can Impact the complete Infra.
- It is very Important to Protect the Host OS from the Container running On it.

Host OS Security

- Container use Operating System Namespaces. OS Namespace is different from K8s Namespace.
- Container use OS Namespace to isolate itself from other containers on the Host Machine.

Host Operating System

Host NameSpace

Used by Application Directly
Running on Host OS.

Container NameSpace

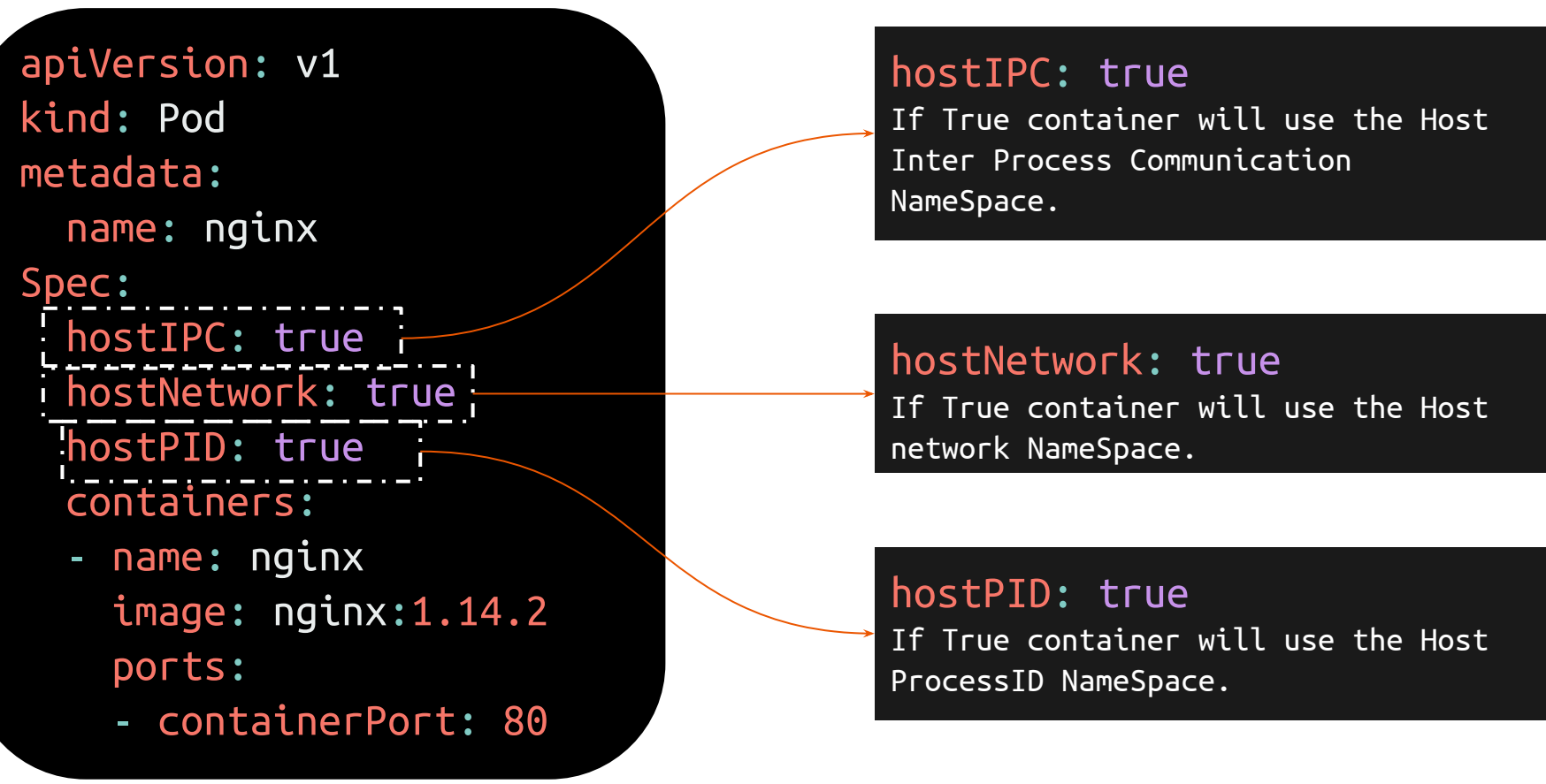
Container

Host OS Security

- You can configure Pods to use a Host Namespace instead, but this comes with Security Risk.
- It is advisable to avoid such practice to Schedule Pods in Host NameSpace.
- Because it provides more ability to attacker to Interact with OS and he can damage more.

K8s : Certification

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
Spec:
  hostIPC: true
  hostNetwork: true
  hostPID: true
  containers:
  - name: nginx
    image: nginx:1.14.2
    ports:
    - containerPort: 80
```



hostIPC: true

If True container will use the Host Inter Process Communication NameSpace.

hostNetwork: true

If True container will use the Host network NameSpace.

hostPID: true

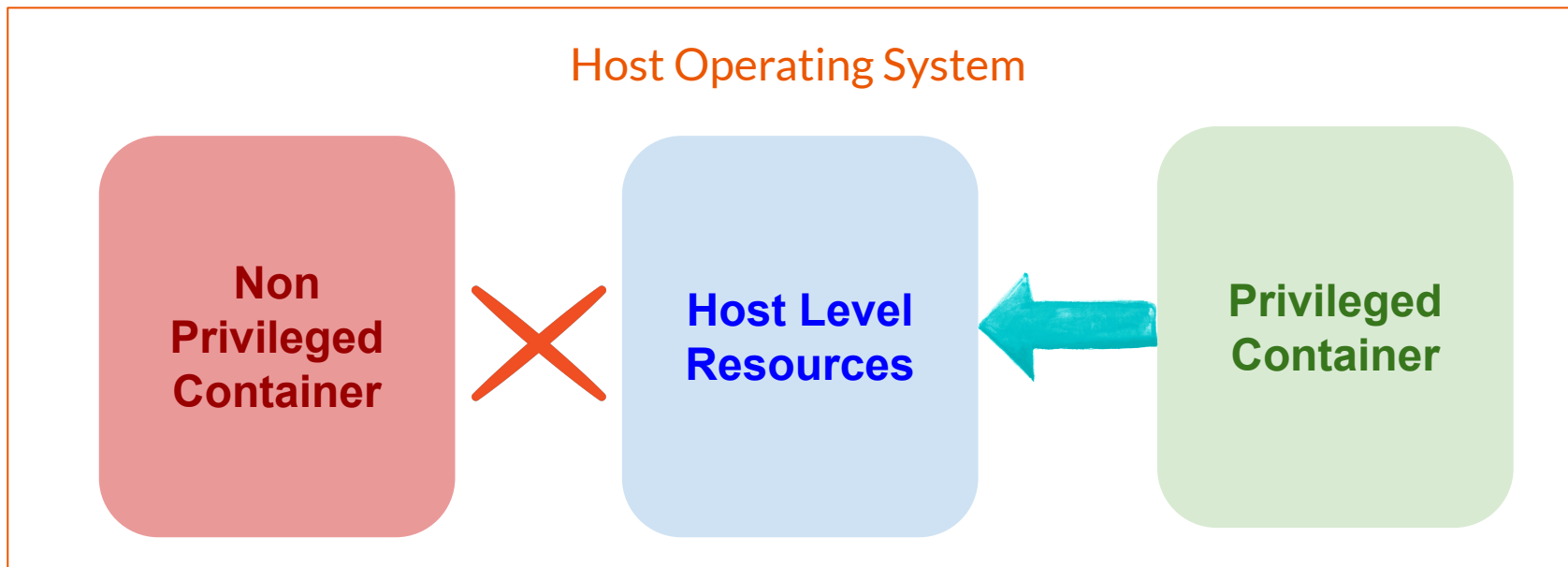
If True container will use the Host ProcessID NameSpace.

Host OS Security

- Use Setting like **hostIPC**, **hostNetwork**, **hostPID**, only when it is absolutely necessary.


Host OS Security

- Privileged Mode allow containers to access host-level resources and capabilities. Much like a non-container process running directly on the Host.



K8s : Certification

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
Spec:
  containers:
  - name: nginx
    image: nginx:1.14.2
    ports:
    - containerPort: 80
    securityContext:
      privileged: true
```



If True container will run in privileged mode.

By Default this mode is **false**.

Host OS Security

- Use Setting like `securityContext[].privilegedMode: true`, only when it is absolutely necessary.

Thank You...

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