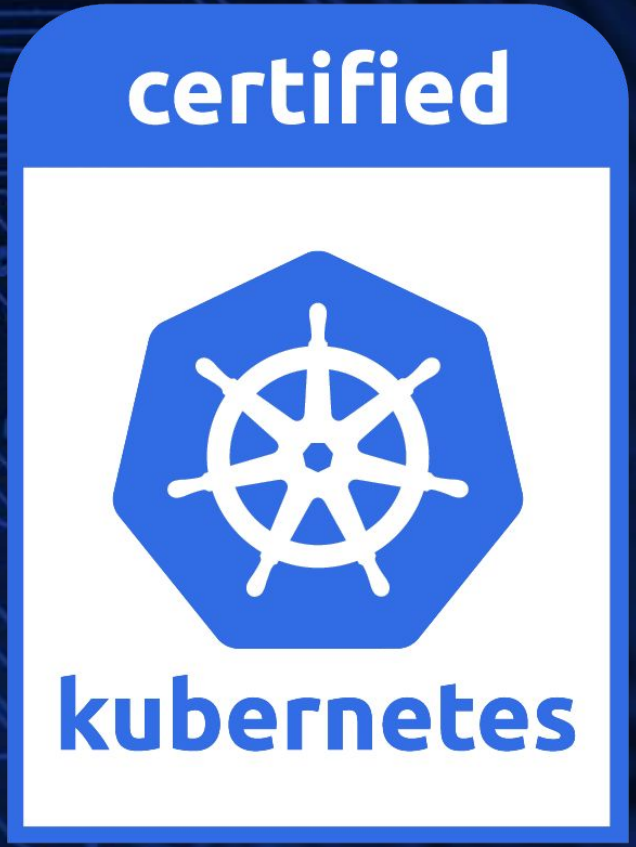
CKA/CKAD : Complete Certification Guide

Kubernetes Pod Security Context



LevelUp360 : anshulc55@icloud.com

- **Security Context :** Security context defines privileges for individual pods or containers. You can use security context to grant containers or pods permissions such as the right to access an external file or run in privileged mode.

- If Security Context is defined at Pod and Container level then Container level Security Context will take precedence over the Pod.

- **Security Context Includes :**

- Discretionary Access Control: Permission to access an object, like a file, is based on user ID (UID) and group ID (GID).

- Security Enhanced Linux (SELinux): Objects are assigned security labels.

- Linux Capabilities: Give a process some privileges, but not all the privileges of the root user.

- AppArmor: Use program profiles to restrict the capabilities of individual programs.

- **Security Context Includes :**

- Seccomp: Filter a process's system calls.

- allowPrivilegeEscalation: Controls whether a process can gain more privileges than its parent process. This bool directly controls whether the no_new_privs flag gets set on the container process. allowPrivilegeEscalation is always true when the container is run as privileged.

- readOnlyRootFilesystem: Mounts the container's root filesystem as read-only.

CKA/CKAD Certification

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-without-security-context
spec:
  volumes:
  - name: sec-ctx-vol
    emptyDir: {}
  containers:
  - name: sec-ctx-demo
    image: busybox
    command: [ "sh", "-c", "sleep 1h" ]
    volumeMounts:
    - name: sec-ctx-vol
      mountPath: /data/demo
```

```
kubectl exec -it pod-without-security-context -- /bin/sh
```

```
/ # id
```

```
uid=0(root) gid=0(root) groups=10(wheel)
```

```
/ # ps
```

```
PID   USER     TIME  COMMAND
    1 root      0:00 sleep 1h
    8 root      0:00 /bin/sh
   14 root      0:00 ps
```

```
/ # ls -ld /data/demo
```

```
drwxrwxrwx    2 root     root          4096 Mar14 16:50 /data/demo
```

CKA/CKAD Certification

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  securityContext:
    runAsUser: 1000
    runAsGroup: 3000
    fsGroup: 2000
  volumes:
  - name: sec-ctx-vol
    emptyDir: {}
  containers:
  - name: sec-ctx-demo
    image: busybox
    command: [ "sh", "-c", "sleep 1h" ]
    volumeMounts:
    - name: sec-ctx-vol
      mountPath: /data/demo
    securityContext:
      allowPrivilegeEscalation: false
```

Thank You...

Don’t be the Same! Be Better!!!

LevelUp360 : anshulc55@icloud.com