SECURITY

Security

Security Contexts

Pods and containers within pods can be given specific security constraints to limit what processes running in containers can do. For example, the UID of the process, the Linux capabilities, and the filesystem group can be limited.

This security limitation is called a security context. It can be defined for the entire pod or per container, and is represented as additional sections in the resources manifests. The notable difference is that Linux capabilities are set at the container level.

For example, if you want to enforce a policy that containers cannot run their process as the root user, you can add a pod security context like the one below:

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  securityContext:
    runAsNonRoot: true
  containers:
  - image: nginx
    name: nginx
```

Then, when you create this Pod, you will see a warning that the container is trying to run as root and that it is not allowed. Hence, the Pod will never run. See the following command and its output:

```
$ kubectl get pods

NAME   READY  STATUS                                                RESTARTS
AGE
nginx  0/1    container has runAsNonRoot and image will run as root  0
 10s
```

To learn more, read the *Configure a Security Context for a Pod or Container* section in the Kubernetes documentation.