Network Policies and User Secruity Context

[Edition 4]

[Last Update 210216]

For any issues/help contact : ***support@k21academy.com***

Contents

1 INTRODUCTION

In a cluster using a Kubernetes Container Network Interface (CNI) plug-in that supports Kubernetes network policy, network isolation is controlled entirely by NetworkPolicy Custom Resource (CR) objects. In OpenShift Container Platform 4.1, OpenShift SDN supports using NetworkPolicy in its default network isolation mode.

To specify security settings for a Container, include the securityContext field in the Container manifest. The securityContext field is a SecurityContext object. Security settings that you specify for a Container apply only to the individual Container, and they override settings made at the Pod level when there is overlap. Container settings do not affect the Pod's Volumes.

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within your organization.

This guide Covers:

- Configuring Network Policies for Applications
- Configuring Container Security Context
- Authentication and Authorisation using RBAC

2 DOCUMENTATION

2.1 Kubernetes Documentation

1. Network Policies
   https://kubernetes.io/docs/concepts/services-networking/network-policies/
2. Configure a Security Context for a Pod or Container
   https://kubernetes.io/docs/tasks/configure-pod-container/security-context/
3. Using RBAC Authorization
   https://kubernetes.io/docs/reference/access-authn-authz/rbac/
4. Authorization Overview
   https://kubernetes.io/docs/reference/access-authn-authz/authorization/

2.2 Linux Commands and VIM Commands

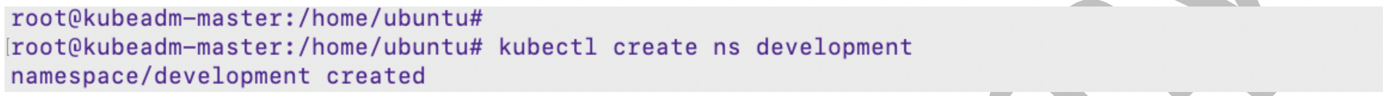
1. Basic Linux Commands
   https://maker.pro/linux/tutorial/basic-linux-commands-for-beginners
   https://www.hostinger.in/tutorials/linux-commands
2. Basic VIM Commands
   https://coderwall.com/p/adv71w/basic-vim-commands-for-getting-started
3. Popular VIM Commands
   https://www.keycdn.com/blog/vim-commands

3 AUTHENTICATION AND AUTHORISATION USING RBAC

3.1 Creating Namespace, User & User Credentials

1. Create a new namespace named development

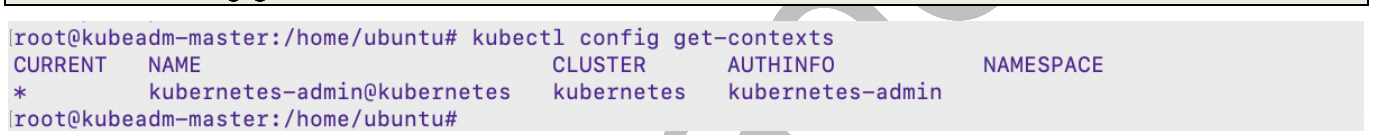
```
$ kubectl create ns development
```



```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# kubectl create ns development
namespace/development created
```

2. View the current clusters and context available. The context allows us to configure the cluster to use, namespace and user for kubectl commands in an easy and consistent manner.

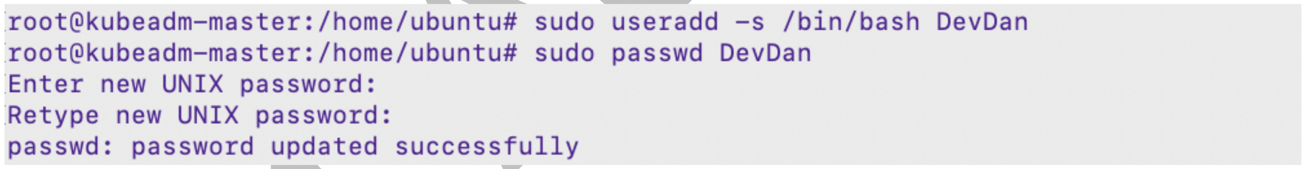
```
$ kubectl config get-contexts
```



```
root@kubeadm-master:/home/ubuntu# kubectl config get-contexts
CURRENT   NAME                          CLUSTER      AUTHINFO           NAMESPACE
*         kubernetes-admin@kubernetes   kubernetes   kubernetes-admin
root@kubeadm-master:/home/ubuntu#
```

3. Create a new user *DevDan* and assign a password to him

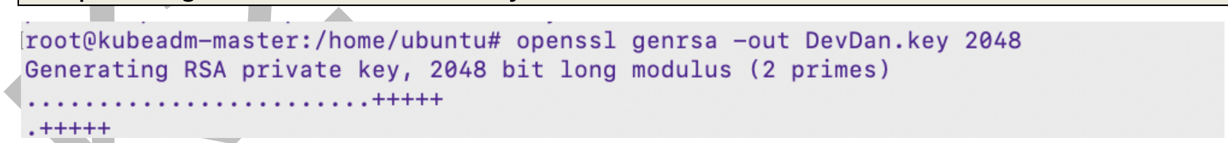
```
$ sudo useradd -s /bin/bash DevDan

$ sudo passwd DevDan
```



```
root@kubeadm-master:/home/ubuntu# sudo useradd -s /bin/bash DevDan
root@kubeadm-master:/home/ubuntu# sudo passwd DevDan
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

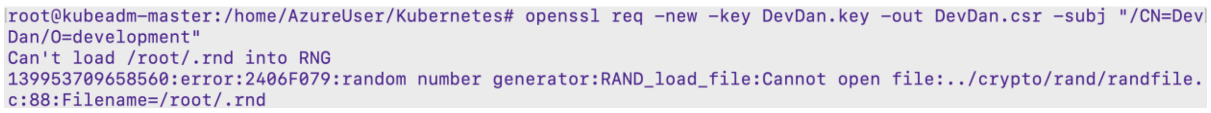
4. Generate a private key for DevDan and Certificate Signing Request (CSR) for DevDan

```
$ openssl genrsa -out DevDan.key 2048
```



```
root@kubeadm-master:/home/ubuntu# openssl genrsa -out DevDan.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
........................+++++
.+++++
```

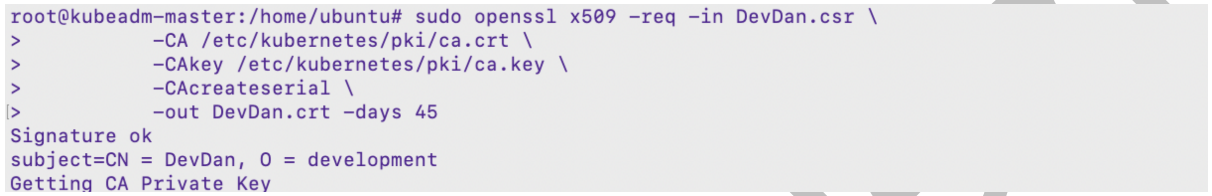
```
$ openssl req -new -key DevDan.key \
-out DevDan.csr -subj "/CN=DevDan/O=development"
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes# openssl req -new -key DevDan.key -out DevDan.csr -subj "/CN=Dev
Dan/O=development"
Can't load /root/.rnd into RNG
139953709658560:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.
c:88:Filename=/root/.rnd
```

5. Generate a self-signed certificate. Use the CA keys for the Kubernetes cluster and set the certificate expiration.

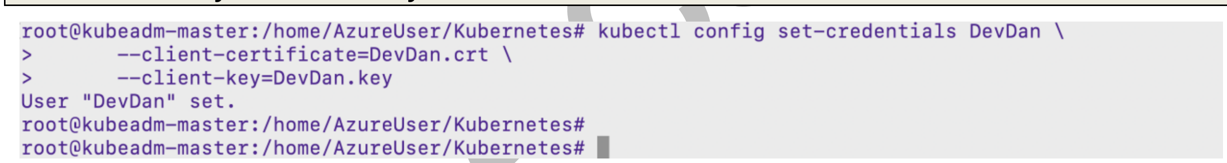
```
$ sudo openssl x509 -req -in DevDan.csr \
        -CA /etc/kubernetes/pki/ca.crt \
        -CAkey /etc/kubernetes/pki/ca.key \
        -CAcreateserial \
        -out DevDan.crt -days 45
```



```
root@kubeadm-master:/home/ubuntu# sudo openssl x509 -req -in DevDan.csr \
>           -CA /etc/kubernetes/pki/ca.crt \
>           -CAkey /etc/kubernetes/pki/ca.key \
>           -CAcreateserial \
>           -out DevDan.crt -days 45
Signature ok
subject=CN = DevDan, O = development
Getting CA Private Key
```

6. Update the access config file to reference the new key and certificate.

```
$ kubectl config set-credentials DevDan \
     --client-certificate=DevDan.crt \
     --client-key=DevDan.key
```

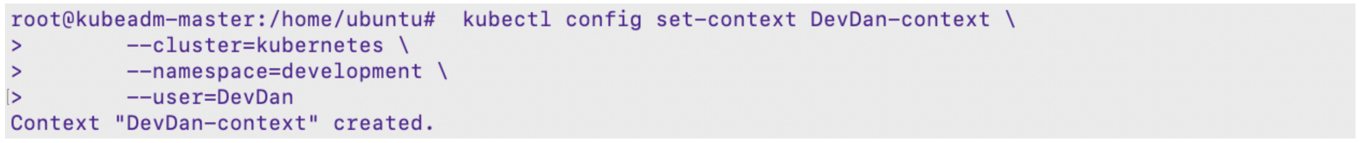


```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl config set-credentials DevDan \
>       --client-certificate=DevDan.crt \
>       --client-key=DevDan.key
User "DevDan" set.
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

3.2 Setting up Context for New User

1. Create context for DevDan user in the cluster and namespace

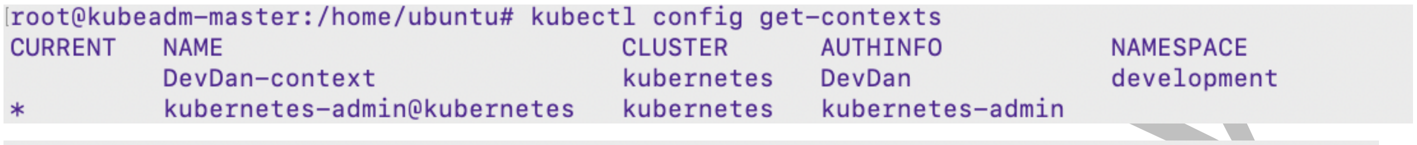
```
$ kubectl config set-context DevDan-context \
      --cluster=kubernetes \
      --namespace=development \
      --user=DevDan
```



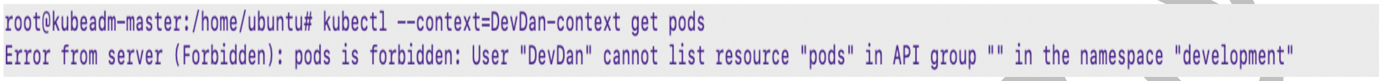
```
root@kubeadm-master:/home/ubuntu#  kubectl config set-context DevDan-context \
>         --cluster=kubernetes \
>         --namespace=development \
>         --user=DevDan
Context "DevDan-context" created.
```

2. Verify the context has been properly set. Attempt to view the Pods inside the DevDan-context. Be aware you will get an error.

```
$ kubectl config get-contexts
$ kubectl --context=DevDan-context get pods
```



```
root@kubeadm-master:/home/ubuntu# kubectl config get-contexts
CURRENT   NAME                          CLUSTER      AUTHINFO           NAMESPACE
          DevDan-context                kubernetes   DevDan             development
*         kubernetes-admin@kubernetes   kubernetes   kubernetes-admin
```

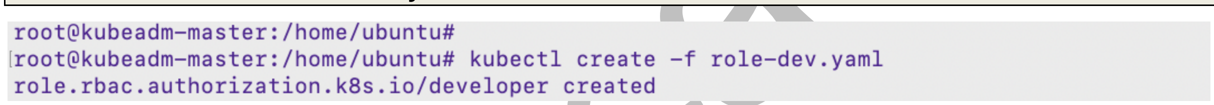


```
root@kubeadm-master:/home/ubuntu# kubectl --context=DevDan-context get pods
Error from server (Forbidden): pods is forbidden: User "DevDan" cannot list resource "pods" in API group "" in the namespace "development"
```

3.3 Create RBAC Role and Rolebinding

1. Create a YAML file to associate RBAC rights to a particular namespace and Role. Create the object. Check white space and for typos if you encounter errors.

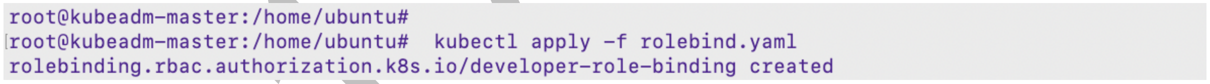
```
$ kubectl create -f role-dev.yaml
```



```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# kubectl create -f role-dev.yaml
role.rbac.authorization.k8s.io/developer created
```

2. Then we create will a RoleBinding to associate the Role we just created with a user. Create the object from the rolebind.yaml file.

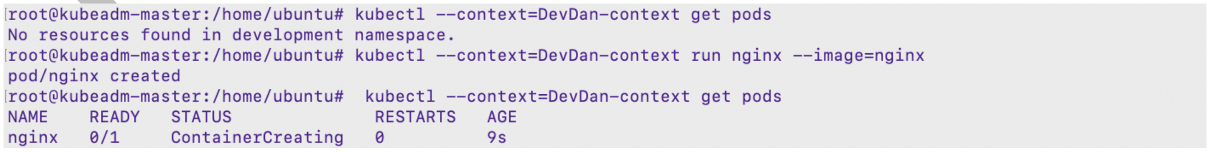
```
$ kubectl create -f rolebind.yaml
```



```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu#  kubectl apply -f rolebind.yaml
rolebinding.rbac.authorization.k8s.io/developer-role-binding created
```

3. Now let's try list pods and then creating a pod using DevDan-context

```
$ kubectl --context=DevDan-context get pods
$ kubectl --context=DevDan-context run nginx --image=nginx
$ kubectl --context=DevDan-context get pods
```



```
root@kubeadm-master:/home/ubuntu# kubectl --context=DevDan-context get pods
No resources found in development namespace.
root@kubeadm-master:/home/ubuntu# kubectl --context=DevDan-context run nginx --image=nginx
pod/nginx created
root@kubeadm-master:/home/ubuntu#  kubectl --context=DevDan-context get pods
NAME    READY   STATUS              RESTARTS   AGE
nginx   0/1     ContainerCreating   0          9s
```

3.4 Clean-up Resources Created this Section

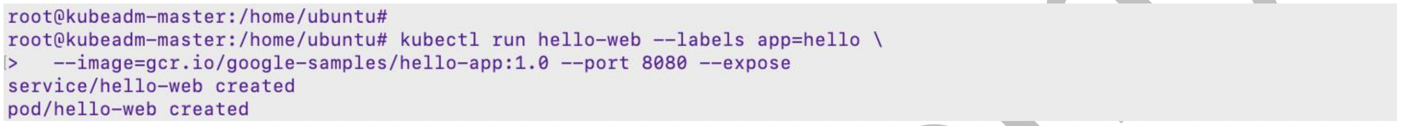
```
$ kubectl delete pod nginx -n development
$ kubectl delete -f rolebind.yaml
$ kubectl delete -f role-dev.yaml
$ kubectl delete ns development
```

4 CONFIGURING NETWORK POLICIES FOR APPLICATIONS

4.1 Restrict Incoming Traffic Pods

1. Run a simple web server application with label app=hello and expose it internally in the cluster

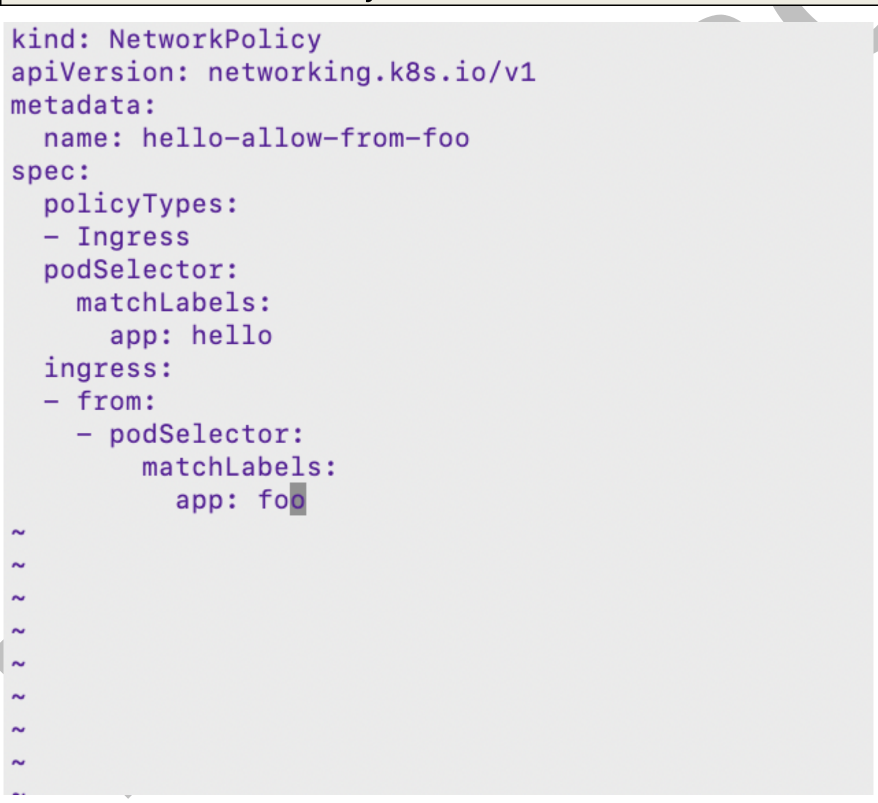
```
$ kubectl run hello-web --labels app=hello --image=gcr.io/google-samples/hello-app:1.0 --port
8080 --expose
```



```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# kubectl run hello-web --labels app=hello \
>   --image=gcr.io/google-samples/hello-app:1.0 --port 8080 --expose
service/hello-web created
pod/hello-web created
```

2. All inbound traffic by default is allowed. So let’s configure a NetworkPolicy to allow traffic to hello-web pods from only pods with label app=foo. All other incoming traffic will be blocked.

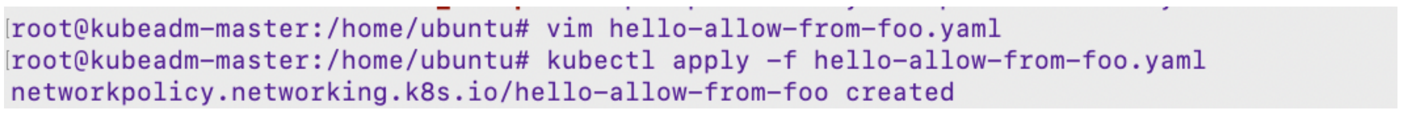
```
$ vi hello-allow-from-foo.yaml
```



```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: hello-allow-from-foo
spec:
  policyTypes:
  - Ingress
  podSelector:
    matchLabels:
      app: hello
  ingress:
  - from:
    - podSelector:
        matchLabels:
          app: foo
~
~
~
~
~
~
~
~
```

3. Apply this policy to the cluster with kubectl command

```
$ kubectl apply -f hello-allow-from-foo.yaml
```

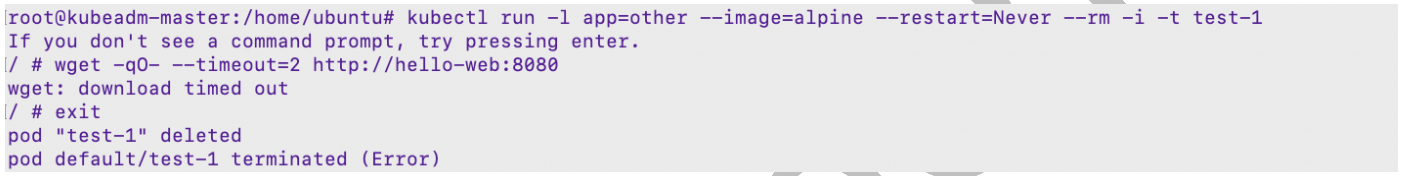


```
root@kubeadm-master:/home/ubuntu# vim hello-allow-from-foo.yaml
root@kubeadm-master:/home/ubuntu# kubectl apply -f hello-allow-from-foo.yaml
networkpolicy.networking.k8s.io/hello-allow-from-foo created
```

4.2 Validating Network Policy

1. Run a temporary Pod with a different label *(app=other)* and get a shell inside the Pod. Observe that the traffic is **not allowed** and therefore the request times out

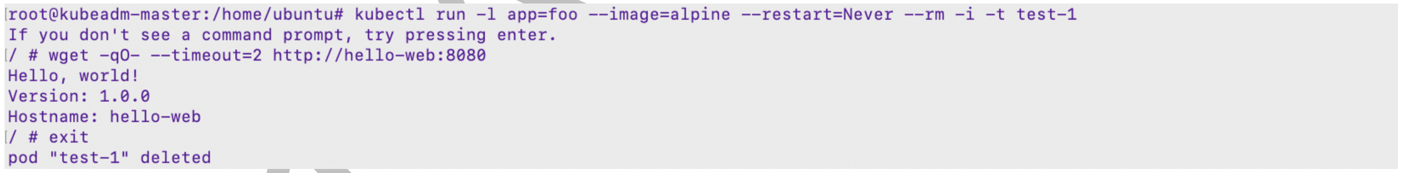
```
$ kubectl run -l app=other --image=alpine --restart=Never --rm -i -t test-1
# wget -qO- --timeout=2 http://hello-web:8080
# exit
```



```
root@kubeadm-master:/home/ubuntu# kubectl run -l app=other --image=alpine --restart=Never --rm -i -t test-1
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://hello-web:8080
wget: download timed out
/ # exit
pod "test-1" deleted
pod default/test-1 terminated (Error)
```

2. Run a temporary Pod with a different label (app=foo) and get a shell inside the Pod. Observe that the traffic is **allowed**

```
$ kubectl run -l app=foo --image=alpine --restart=Never --rm -i -t test-1
# wget -qO- --timeout=2 http://hello-web:8080
# exit
```



```
root@kubeadm-master:/home/ubuntu# kubectl run -l app=foo --image=alpine --restart=Never --rm -i -t test-1
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://hello-web:8080
Hello, world!
Version: 1.0.0
Hostname: hello-web
/ # exit
pod "test-1" deleted
```

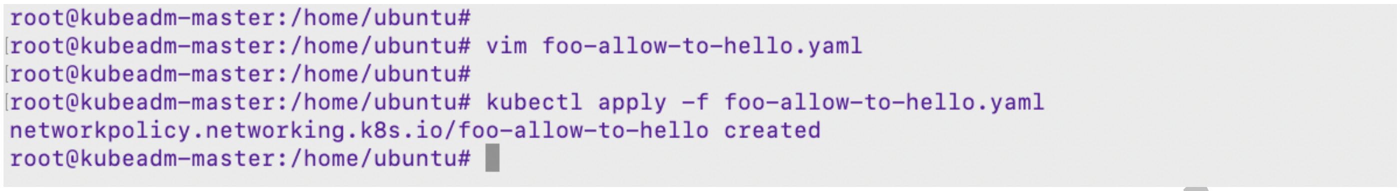
4.3 Restrict Outgoing Traffic from Pods

1. All outbound traffic by default is allowed. So let's configure a NetworkPolicy to allow traffic only from pods labelled as app=foo to send traffic only to pods with label app=hello. All other outgoing traffic from app=foo will be blocked.

```
$ vi foo-allow-to-hello.yaml
```

2. Apply this policy to the cluster with kubectl command

```
$ kubectl apply -f foo-allow-to-hello.yaml
```

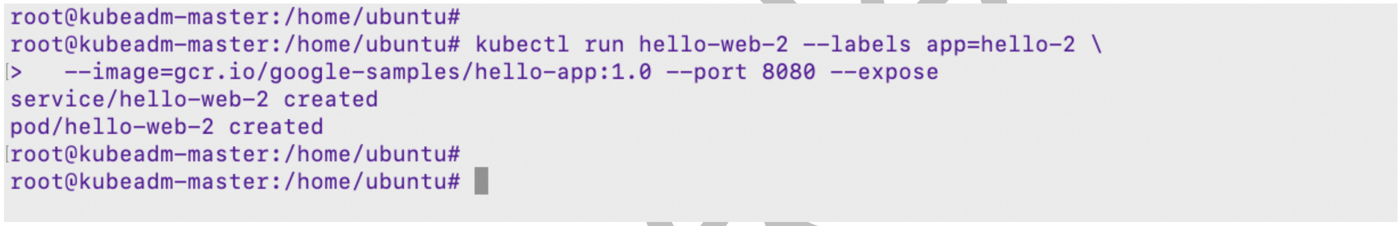


```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# vim foo-allow-to-hello.yaml
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# kubectl apply -f foo-allow-to-hello.yaml
networkpolicy.networking.k8s.io/foo-allow-to-hello created
root@kubeadm-master:/home/ubuntu#
```

4.4 Validating Network Policy

1. Run a temporary Pod with a different label (app=hello-2)

```
$ kubectl run hello-web-2 --labels app=hello-2 \
  --image=gcr.io/google-samples/hello-app:1.0 --port 8080 --expose
```



```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# kubectl run hello-web-2 --labels app=hello-2 \
>   --image=gcr.io/google-samples/hello-app:1.0 --port 8080 --expose
service/hello-web-2 created
pod/hello-web-2 created
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu#
```

2. Next, run a temporary Pod with app=foo label and get a shell prompt inside the container:

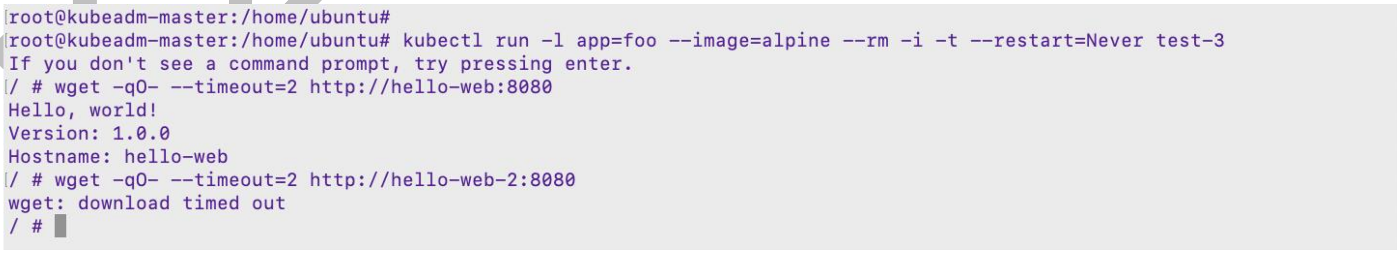
```
$kubectl run -l app=foo --image=alpine --rm -i -t --restart=Never test-3
```

3. Validate that the Pod can establish connections to hello-web:8080:

```
# wget -qO- --timeout=2 http://hello-web:8080
```

4. Validate that the Pod **cannot** establish connections to hello-web-2:8080:

```
# wget -qO- --timeout=2 http://hello-web-2:8080
```



```
root@kubeadm-master:/home/ubuntu#
root@kubeadm-master:/home/ubuntu# kubectl run -l app=foo --image=alpine --rm -i -t --restart=Never test-3
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://hello-web:8080
Hello, world!
Version: 1.0.0
Hostname: hello-web
/ # wget -qO- --timeout=2 http://hello-web-2:8080
wget: download timed out
/ #
```

4.5 Clean-up the resources created in this Section

```
$ kubectl delete -f foo-allow-to-hello.yaml
$ kubectl delete -f hello-allow-from-foo.yaml
```

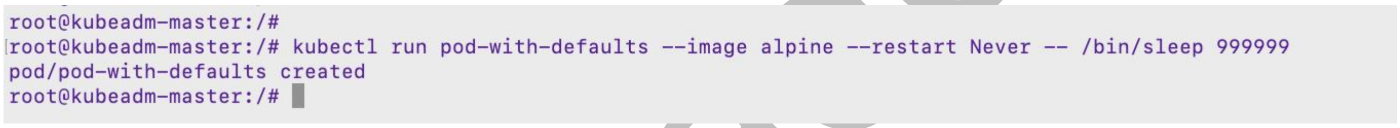
5 CONFIGURING CONTAINER SECURITY CONTEXT

5.1 Defining Security Contexts With Default User

Note: It allows you to lock down your containers, so that only certain processes can do certain things. This ensures the stability of your containers and allows you to give control or take it away. In this lesson, we'll go through how to set the security context at the container level and the pod level.

1. Run an alpine container with default security

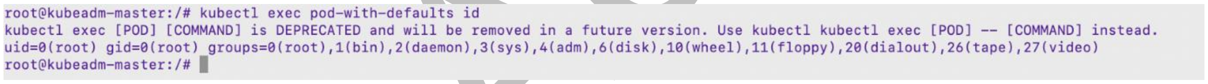
```
$ kubectl run pod-with-defaults --image alpine --restart Never -- /bin/sleep 999999
```



```
root@kubeadm-master:/#
root@kubeadm-master:/# kubectl run pod-with-defaults --image alpine --restart Never -- /bin/sleep 999999
pod/pod-with-defaults created
root@kubeadm-master:/#
```

2. Check the ID on the container:

```
$ kubectl exec pod-with-defaults id
```

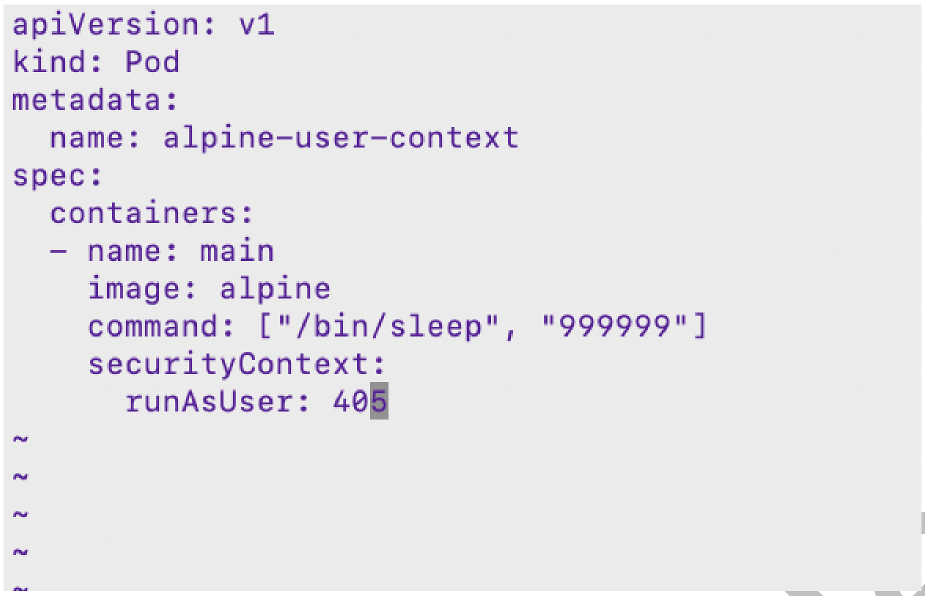


```
root@kubeadm-master:/# kubectl exec pod-with-defaults id
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
root@kubeadm-master:/#
```

5.2 Defining Security Contexts With Specific User

1. The YAML for a container that runs as a user. View the file security-cxt.yaml

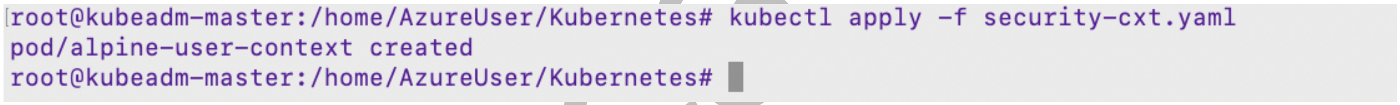
```
$ vim security-cxt.yaml
```



```
apiVersion: v1
kind: Pod
metadata:
  name: alpine-user-context
spec:
  containers:
  - name: main
    image: alpine
    command: ["/bin/sleep", "999999"]
    securityContext:
      runAsUser: 405
~
~
~
~
~
```

2. Create the resource from above yaml file

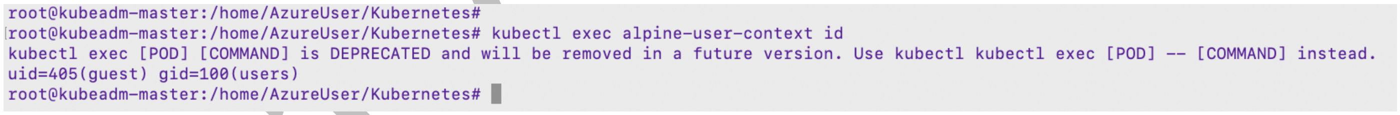
```
$ kubectl apply -f security-cxt.yaml
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl apply -f security-cxt.yaml
pod/alpine-user-context created
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

3. Check the user context

```
$ kubectl exec alpine-user-context id
```

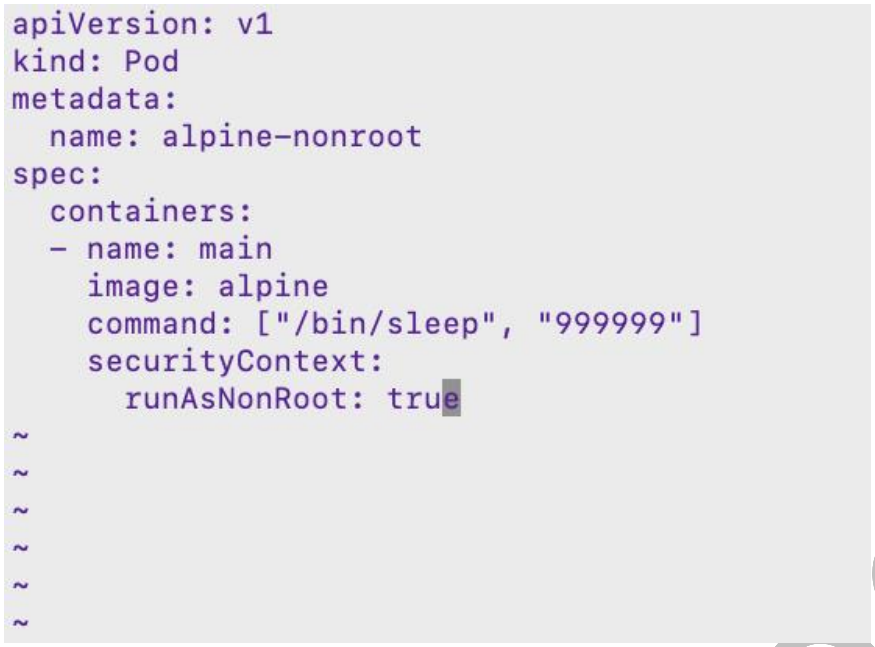


```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec alpine-user-context id
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
uid=405(guest) gid=100(users)
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

5.3 Defining Security Contexts With non-root User

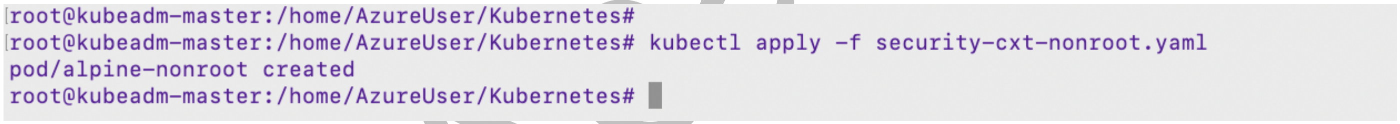
1. The YAML for a pod that runs the container as non-root:

```
$ vim security-cxt-nonroot.yaml
```


```
apiVersion: v1
kind: Pod
metadata:
  name: alpine-nonroot
spec:
  containers:
  - name: main
    image: alpine
    command: ["/bin/sleep", "999999"]
    securityContext:
      runAsNonRoot: true
~
~
~
~
~
~
```

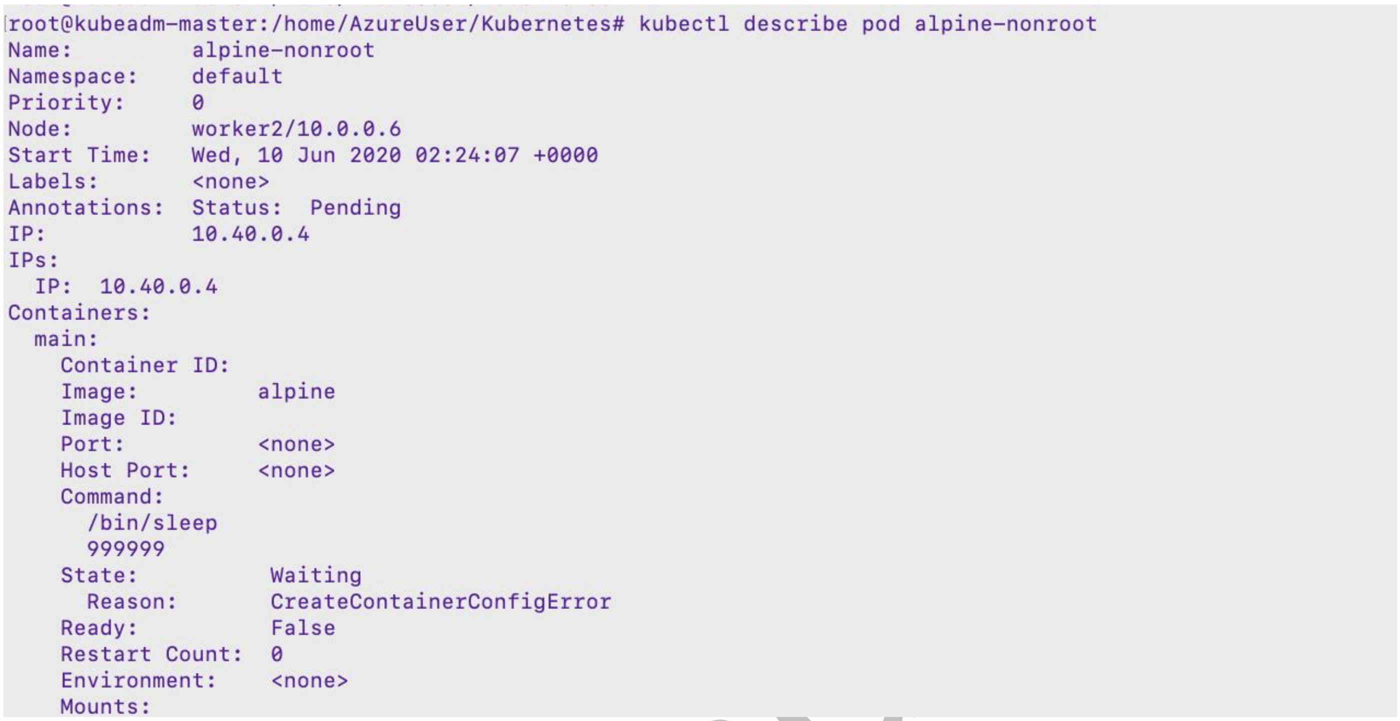
2. Create a pod that runs the container as non-root:

```
$ kubectl apply -f security-cxt-nonroot.yaml
```

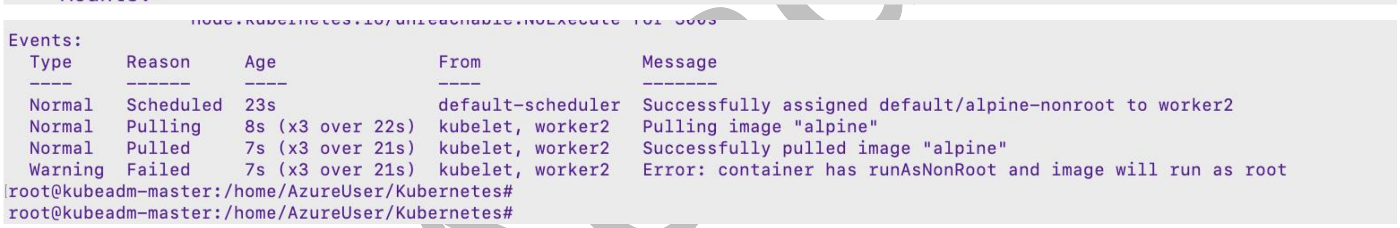

```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl apply -f security-cxt-nonroot.yaml
pod/alpine-nonroot created
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

3. View more information about the pod error:

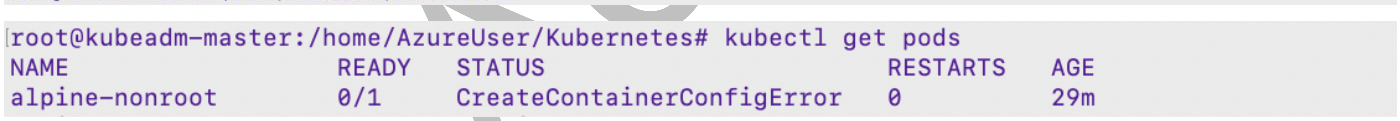
```
$ kubectl describe pod alpine-nonroot
$ kubectl get pods
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl describe pod alpine-nonroot
Name:         alpine-nonroot
Namespace:    default
Priority:     0
Node:         worker2/10.0.0.6
Start Time:   Wed, 10 Jun 2020 02:24:07 +0000
Labels:       <none>
Annotations:  Status:  Pending
IP:           10.40.0.4
IPs:
  IP:  10.40.0.4
Containers:
  main:
    Container ID:
    Image:         alpine
    Image ID:
    Port:          <none>
    Host Port:     <none>
    Command:
      /bin/sleep
      999999
    State:          Waiting
      Reason:       CreateContainerConfigError
    Ready:          False
    Restart Count:  0
    Environment:    <none>
    Mounts:
```



```
Events:
  Type     Reason     Age                From               Message
  ----     ------     ----               ----               -------
  Normal   Scheduled  23s                default-scheduler  Successfully assigned default/alpine-nonroot to worker2
  Normal   Pulling    8s (x3 over 22s)   kubelet, worker2   Pulling image "alpine"
  Normal   Pulled     7s (x3 over 21s)   kubelet, worker2   Successfully pulled image "alpine"
  Warning  Failed     7s (x3 over 21s)   kubelet, worker2   Error: container has runAsNonRoot and image will run as root
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

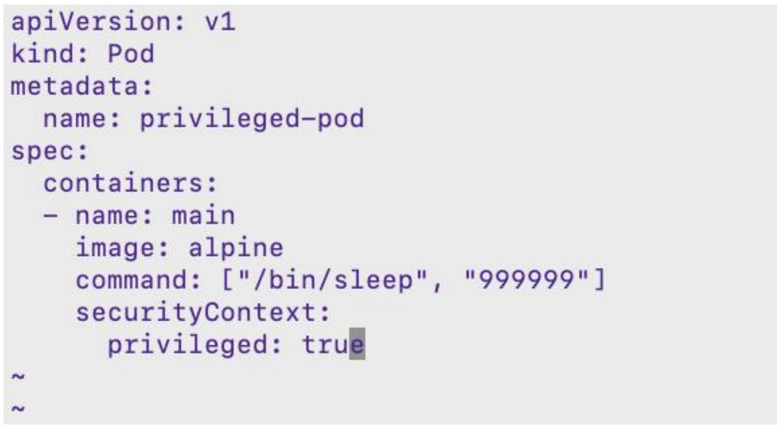


```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl get pods
NAME                     READY   STATUS                       RESTARTS   AGE
alpine-nonroot           0/1     CreateContainerConfigError   0          29m
```

5.4 Defining Security Contexts With Privileged Container POD

1. The YAML for a privileged container pod:

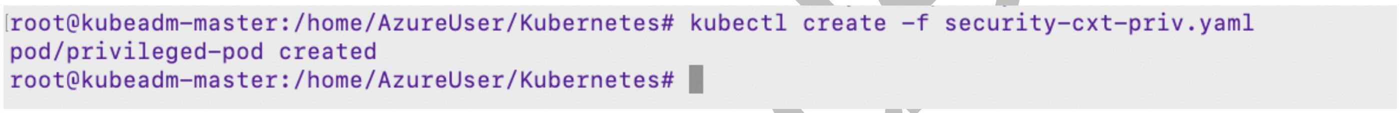
```
$ vim security-cxt-priv.yaml
```



```
apiVersion: v1
kind: Pod
metadata:
  name: privileged-pod
spec:
  containers:
  - name: main
    image: alpine
    command: ["/bin/sleep", "999999"]
    securityContext:
      privileged: true
~
~
```

2. Create the privileged container pod:

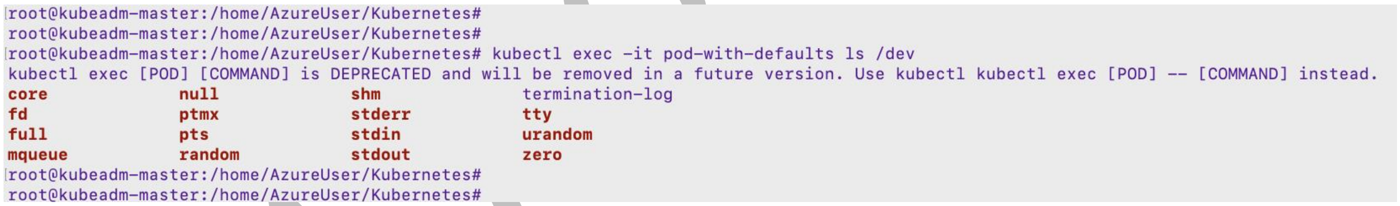
```
kubectl apply -f security-cxt-priv.yaml
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl create -f security-cxt-priv.yaml
pod/privileged-pod created
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

3. View the devices on the default container:

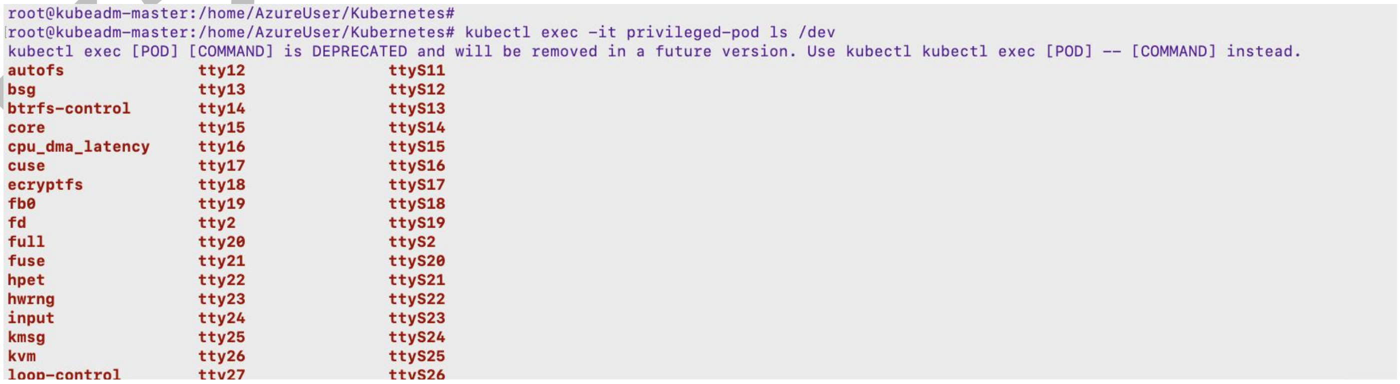
```
$ kubectl exec -it pod-with-defaults ls /dev
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it pod-with-defaults ls /dev
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
core            null            shm             termination-log
fd              ptmx            stderr          tty
full            pts             stdin           urandom
mqueue          random          stdout          zero
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

4. View the devices on the privileged pod container:

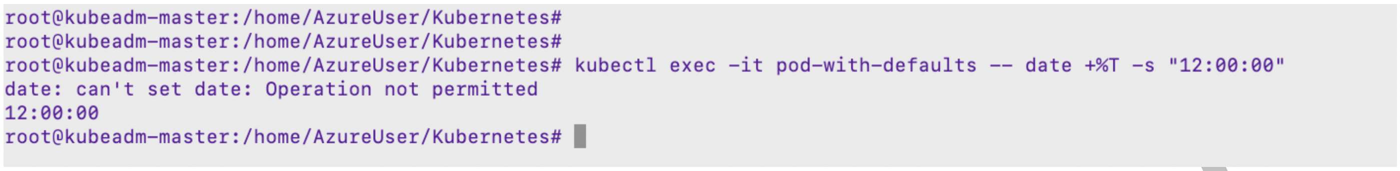
```
$ kubectl exec -it privileged-pod ls /dev
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it privileged-pod ls /dev
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
autofs              tty12               ttyS11
bsg                 tty13               ttyS12
btrfs-control       tty14               ttyS13
core                tty15               ttyS14
cpu_dma_latency     tty16               ttyS15
cuse                tty17               ttyS16
ecryptfs            tty18               ttyS17
fb0                 tty19               ttyS18
fd                  tty2                ttyS19
full                tty20               ttyS2
fuse                tty21               ttyS20
hpet                tty22               ttyS21
hwrng               tty23               ttyS22
input               tty24               ttyS23
kmsg                tty25               ttyS24
kvm                 tty26               ttyS25
loop-control        tty27               ttyS26
```

5. Try to change the time on a default container pod:

```
$ kubectl exec -it pod-with-defaults -- date +%T -s "12:00:00"
```

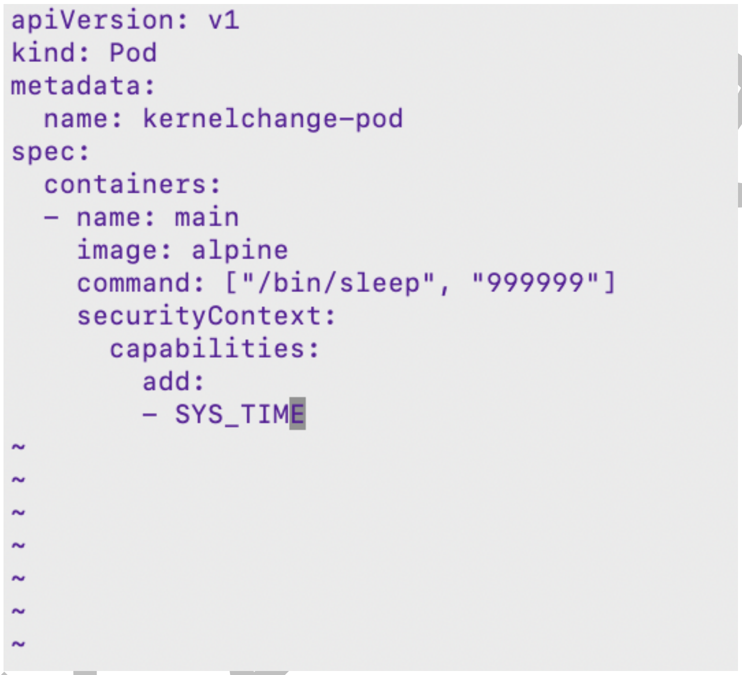


```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it pod-with-defaults -- date +%T -s "12:00:00"
date: can't set date: Operation not permitted
12:00:00
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

5.5 Defining Security Contexts With Privileged Container POD – add Capability

1. The YAML for a container that will allow you to change the time:

```
$ vim security-cxt-time.yaml
```



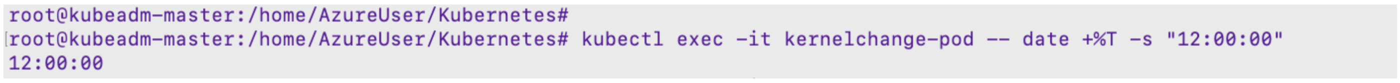
```
apiVersion: v1
kind: Pod
metadata:
  name: kernelchange-pod
spec:
  containers:
  - name: main
    image: alpine
    command: ["/bin/sleep", "999999"]
    securityContext:
      capabilities:
        add:
        - SYS_TIME
~
~
~
~
~
~
~
```

2. Create the pod that will allow you to change the container's time:

```
$ kubectl create -f security-cxt-time.yaml
```

3. Change the time on a container:

```
$ kubectl exec -it kernelchange-pod -- date +%T -s "12:00:00"
```

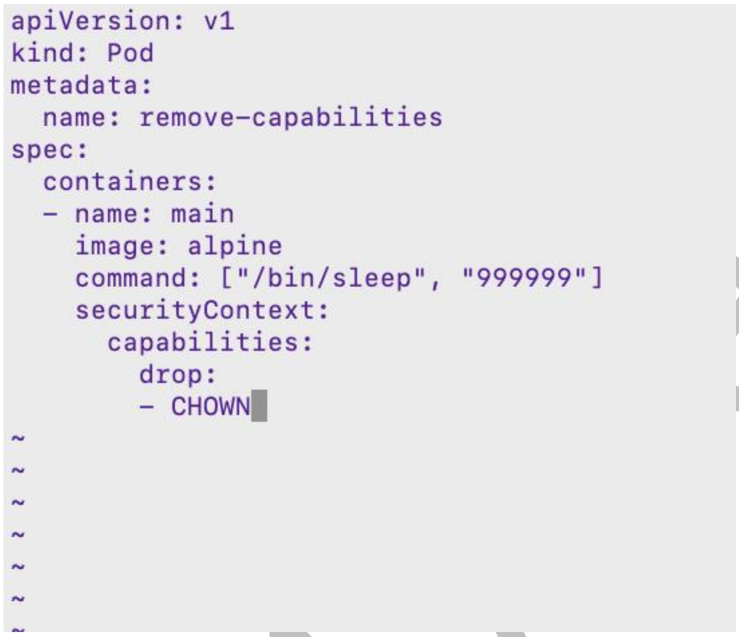


```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it kernelchange-pod -- date +%T -s "12:00:00"
12:00:00
```

5.6 Defining security contexts with privileged container pod – remove capability

1. The YAML for a container that removes capabilities:

```
$ vim security-cxt-rmcap.yaml
```



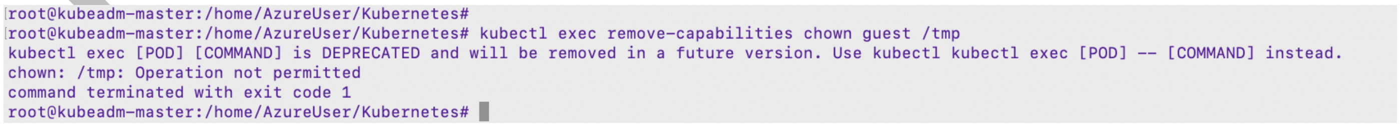
```
apiVersion: v1
kind: Pod
metadata:
  name: remove-capabilities
spec:
  containers:
  - name: main
    image: alpine
    command: ["/bin/sleep", "999999"]
    securityContext:
      capabilities:
        drop:
        - CHOWN
~
~
~
~
~
~
```

2. Create a pod that's container has capabilities removed:

```
$ kubectl apply -f security-cxt-rmcap.yaml
```

3. Try to change the ownership of a container with removed capability:

```
$ kubectl exec remove-capabilities chown guest /tmp
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec remove-capabilities chown guest /tmp
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
chown: /tmp: Operation not permitted
command terminated with exit code 1
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

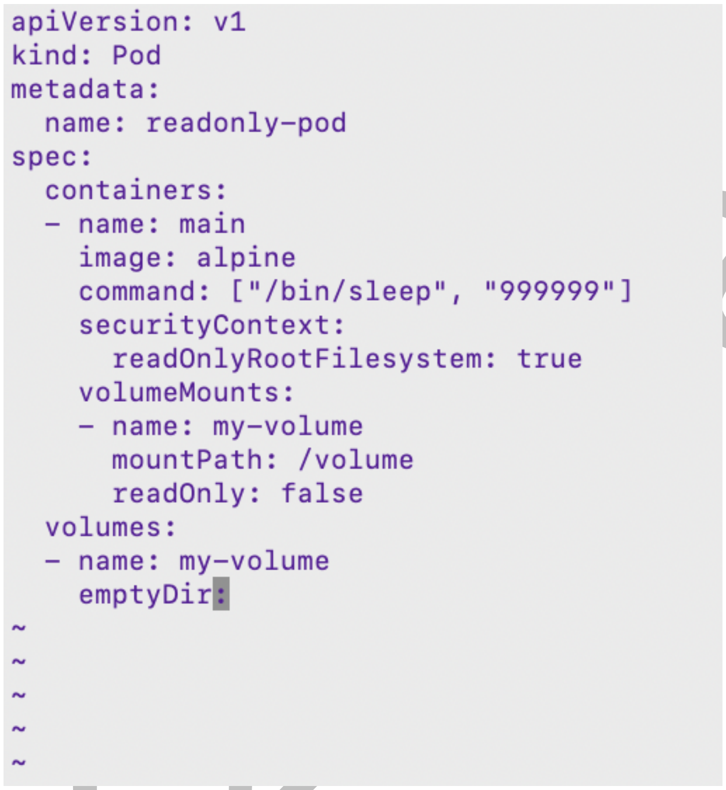
5.7 Defining security contexts with privileged container pod – ReadOnly

1. The YAML for a pod container that can’t write to the local filesystem:

```
$ vim security-cxt-readonly.yaml
```

2. Create a pod that will not allow you to write to the local container filesystem:

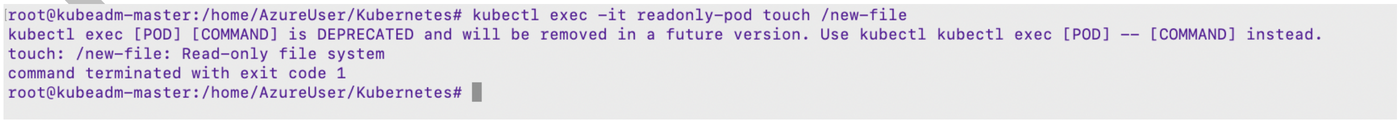
```
$ kubectl apply -f security-cxt-readonly.yaml
```



```
apiVersion: v1
kind: Pod
metadata:
  name: readonly-pod
spec:
  containers:
  - name: main
    image: alpine
    command: ["/bin/sleep", "999999"]
    securityContext:
      readOnlyRootFilesystem: true
    volumeMounts:
    - name: my-volume
      mountPath: /volume
      readOnly: false
  volumes:
  - name: my-volume
    emptyDir:
~
~
~
~
~
```

3. Try to write to the container filesystem:

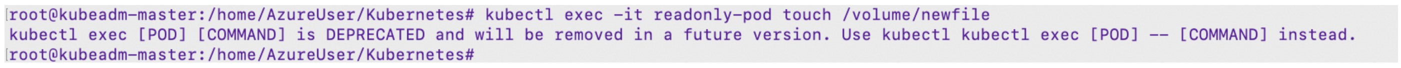
```
$ kubectl exec -it readonly-pod touch /new-file
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it readonly-pod touch /new-file
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
touch: /new-file: Read-only file system
command terminated with exit code 1
root@kubeadm-master:/home/AzureUser/Kubernetes# 
```

4. Create a file on the volume mounted to the container:

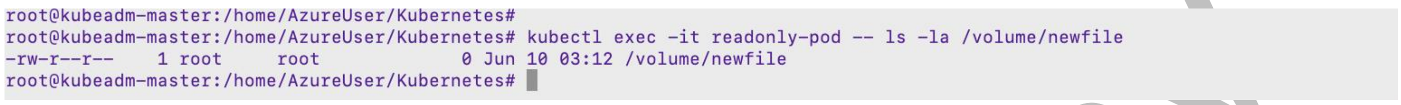
```
$ kubectl exec -it readonly-pod touch /volume/newfile
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it readonly-pod touch /volume/newfile
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec [POD] -- [COMMAND] instead.
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

5. View the file on the volume that's mounted:

```
$ kubectl exec -it readonly-pod -- ls -la /volume/newfile
```



```
root@kubeadm-master:/home/AzureUser/Kubernetes#
root@kubeadm-master:/home/AzureUser/Kubernetes# kubectl exec -it readonly-pod -- ls -la /volume/newfile
-rw-r--r--    1 root     root             0 Jun 10 03:12 /volume/newfile
root@kubeadm-master:/home/AzureUser/Kubernetes#
```

6 SUMMARY

In this guide we Covered:

- Configuring Network Policies for Applications
- Configuring Container Security Context
- Authentication and Authorisation using RBAC