

## Multi-Tenant Kubernetes Security

```
Activities Workstation master@master-vm: ~/k8s-multi-tenant/tenant-a

master@master-vm:~/Desktop$ kubectl get nodes
NAME          STATUS    ROLES    AGE   VERSION
master-vm     Ready     control-plane 100m   v1.28.15
worker1-vm    Ready     <none>    44m   v1.28.15
worker2-vm    NotReady  <none>    36m   v1.28.15

master@master-vm:~/Desktop$ kubectl apply -f https://docs.projectcalico.org/manifests/calico.yaml
poddisruptionbudget.policy/calico-kube-controllers created
serviceaccount/calico-kube-controllers created
serviceaccount/calico-node created
configmap/calico-config created
customresourcedefinition.apitensions.k8s.io/bgpconfigurations.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/bgppeers.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/blockaffinities.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/caliconodestatuses.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/clusterinformations.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/felixconfigurations.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/globalnetworkpolicies.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/globalnetworksets.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/hostendpoints.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/ipamblocks.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/ipamconfigs.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/ipamhandles.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/ippools.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/tpreservations.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/kubecontrollersconfigurations.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/networkpolicies.crd.projectcalico.org created
customresourcedefinition.apitensions.k8s.io/networksets.crd.projectcalico.org created
clusterrole.rbac.authorization.k8s.io/calico-kube-controllers created
clusterrole.rbac.authorization.k8s.io/calico-node created
clusterrolebinding.rbac.authorization.k8s.io/calico-kube-controllers created
clusterrolebinding.rbac.authorization.k8s.io/calico-node created
daemonset.apps/calico-node created
deployment.apps/calico-kube-controllers created
master@master-vm:~/Desktop$ kubectl create namespace tenant-a
namespace/tenant-a created
master@master-vm:~/Desktop$ kubectl create namespace tenant-b
namespace/tenant-b created
master@master-vm:~/Desktop$ mkdir -p ~/k8s-multi-tenant/tenant-a
master@master-vm:~/Desktop$ mkdir -p ~/k8s-multi-tenant/tenant-b
master@master-vm:~/Desktop$ cd ~/k8s-multi-tenant
master@master-vm:~/k8s-multi-tenant$ cd ~/k8s-multi-tenant/tenant-a
master@master-vm:~/k8s-multi-tenant/tenant-a$ nano tenant-a-app.yaml
master@master-vm:~/k8s-multi-tenant/tenant-a$ kubectl apply -f tenant-a-app.yaml
deployment.apps/tenant-a-app created
service/tenant-a-service created

master@master-vm:~/k8s-multi-tenant/tenant-a$ ls
kubectl tenant-a-app.yaml
master@master-vm:~/k8s-multi-tenant/tenant-a$ nano tenant-a-restrict.yaml
master@master-vm:~/k8s-multi-tenant/tenant-a$ kubectl apply -f tenant-a-restrict.yaml
error: the path "tenant-a/tenant-a-restrict.yaml" does not exist
master@master-vm:~/k8s-multi-tenant/tenant-a$ pwd
/home/master/k8s-multi-tenant/tenant-a
master@master-vm:~/k8s-multi-tenant/tenant-a$ kubectl apply -f tenant-a-restrict.yaml
networkpolicy.networking.k8s.io/tenant-a-restrict created
master@master-vm:~/k8s-multi-tenant/tenant-a$
```

```
Activities Workstation Master Worker1 Worker2
master@master-vm: ~/k8s-multi-tenant/tenant-b

master@master-vm:~/k8s-multi-tenant/tenant-a$ pwd
/home/master/k8s-multi-tenant/tenant-a
master@master-vm:~/k8s-multi-tenant/tenant-a$ kubectl apply -f tenant-a-restrict.yaml
networkpolicy.networking.k8s.io/tenant-a-restrict created
master@master-vm:~/k8s-multi-tenant/tenant-a$ cd ~/k8s-multi-tenant/tenant-b
master@master-vm:~/k8s-multi-tenant/tenant-b$ nano tenant-b-app.yaml
deployment.apps/tenant-b-app created
service/tenant-b-service created
master@master-vm:~/k8s-multi-tenant/tenant-b$ nano tenant-b-restrict.yaml
networkpolicy.networking.k8s.io/tenant-b-restrict created
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl get networkpolicy -n tenant-b
NAME          POD-SELECTOR  AGE
tenant-b-restrict  app=tenant-b-app  43s
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl get nodes
NAME          STATUS    ROLES    AGE   VERSION
master-vm     Ready     control-plane  117m  v1.28.15
worker1-vm    Ready     <none>      61m   v1.28.15
worker2-vm    NotReady  <none>      53m   v1.28.15
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl describe networkpolicy tenant-b-restrict -n tenant-b
Name:         tenant-b-restrict
Namespace:    tenant-b
Created on:   2025-03-15 14:06:26 +0530 IST
Labels:       <none>
Annotations:  <none>
Spec:
  PodSelector:  app=tenant-b-app
  Allowing ingress traffic:
    To Port: <any> (traffic allowed to all ports)
    From:
      PodSelector: app=tenant-b-app
  Not affecting egress traffic
  Policy Types: Ingress
master@master-vm:~/k8s-multi-tenant/tenant-b$
```

```
Activities Workstation Master Worker1 Worker2
master@master-vm: ~/k8s-multi-tenant/tenant-b

master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl apply -f tenant-b-app.yaml
deployment.apps/tenant-b-app created
service/tenant-b-service created
master@master-vm:~/k8s-multi-tenant/tenant-b$ nano tenant-b-restrict.yaml
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl apply -f tenant-b-restrict.yaml
networkpolicy.networking.k8s.io/tenant-b-restrict created
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl get networkpolicy -n tenant-b
NAME          POD-SELECTOR  AGE
tenant-b-restrict  app=tenant-b-app  43s
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl get nodes
NAME          STATUS    ROLES    AGE   VERSION
master-vm     Ready     control-plane  117m  v1.28.15
worker1-vm    Ready     <none>      61m   v1.28.15
worker2-vm    NotReady  <none>      53m   v1.28.15
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl describe networkpolicy tenant-b-restrict -n tenant-b
Name:         tenant-b-restrict
Namespace:    tenant-b
Created on:   2025-03-15 14:06:26 +0530 IST
Labels:       <none>
Annotations:  <none>
Spec:
  PodSelector:  app=tenant-b-app
  Allowing ingress traffic:
    To Port: <any> (traffic allowed to all ports)
    From:
      PodSelector: app=tenant-b-app
  Not affecting egress traffic
  Policy Types: Ingress
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl run test-pod --image=alpine -n tenant-b --restart=Never -- sleep 3600
pod/test-pod created
master@master-vm:~/k8s-multi-tenant/tenant-b$ kubectl exec -it test-pod -n tenant-b -- wget --spider tenant-a-service.tenant-a
Connecting to tenant-a-service.tenant-a (10.110.185.140:80)
wget: can't connect to remote host (10.110.185.140): Operation timed out
command terminated with exit code 1
master@master-vm:~/k8s-multi-tenant/tenant-b$
```