



Certified Kubernetes Administrator Prep

Configure Network Policies

Kubernetes Network Policies

- Specification of how groups of pods may communicate
- Use labels to select pods and define rules
- Implemented by the network plugin
- Pods are non-isolated by default
- Pods are isolated when a Network Policy selects them



Kubernetes Network Policies Example

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
    - Ingress
    - Egress
```

```
ingress:
  - from:
      - ipBlock:
          cidr: 172.17.0.0/16
          except:
            - 172.17.1.0/24
      - namespaceSelector:
          matchLabels:
            project: myproject
    - podSelector:
        matchLabels:
          role: frontend
```

```
ports:
  - protocol: TCP
    port: 6379
egress:
  - to:
      - ipBlock:
          cidr: 10.0.0.0/24
    ports:
      - protocol: TCP
        port: 5978
```



Example Default Isolation Policy

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: default-deny
spec:
  podSelector: {}
  policyTypes:
    - Ingress
```



Explicitly Allow All Traffic Sample YAML

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all
spec:
  podSelector: {}
  ingress:
  - {}
```



Explicitly Deny Outgoing Traffic Sample YAML

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: default-deny
spec:
  podSelector: {}
  policyTypes:
    - Egress
```



Explicitly Allow All Outgoing Traffic Sample YAML

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all
spec:
  podSelector: {}
  egress:
    - {}
```



Explicitly Stop ALL Traffic Sample YAML

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: default-deny
spec:
  podSelector: {}
  policyTypes:
    - Ingress
    - Egress
```



Conclusion

- Specification of how groups of pods may communicate
- Use labels to select pods and define rules
- Implemented by the network plugin
- Pods are non-isolated by default
- Pods are isolated when a Network Policy selects them

