Calico CNI

Popis

Calico představujee síťovou komponentu, implementující CNI (Container Networking Interface), která poskytuje možnost komunikace meži jednotlivými kontejnery. Obsahuje také nástroje pro dodatečnou bezpečnost díky možnosti kontroly komunikace mezi pody, např. skrz NetworkPolicy.

Instalace

Postup

1. calico-operator.yaml - instalace CRD a operátora. Je třeba installovat přes "kubectl create" (nikoliv apply)
2. calico-ippools.yaml - definice parametrů pro Calico
3. calico-install.yaml - konfigurace Installation CRD (instalace instance Calica).

OPTIONAL calico-apiserver.yaml - konfigurace Apiserveru pro možnost ovládání Calico přes kubectl

Soubory

calico-apiserver.yaml

calico-ippools.yaml

calico-operator.yaml

calico-install.yaml

```
# tvlakub11
k create -f /root/calico/calico-operator.yaml

k create -f /root/calico/calico-ippools.yaml

k create -f /root/calico/calico-install.yaml
```

Očekávaný stav

tigera-operator namespace (obsahuje Calico operátora)

```
[root@tvlakub11:/home/exdmachacek/cluster]# k get all -n tigera-operator
NAME                                   READY   STATUS    RESTARTS      AGE
pod/tigera-operator-5dbb946747-9nvt7   1/1     Running   8 (13m ago)   4d20h

NAME                              READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/tigera-operator   1/1     1            1           4d20h

NAME                                         DESIRED   CURRENT   READY   AGE
replicaset.apps/tigera-operator-5dbb946747   1         1         1       4d20h
```

calico-apiserver namespace (obsahuje Calico API server)

```
[root@tvlakub11:/home/exdmachacek/cluster]# k get all -n calico-apiserver
NAME                                    READY   STATUS    RESTARTS      AGE
pod/calico-apiserver-79b757694f-jrdds   1/1     Running   1 (18m ago)   4d20h
pod/calico-apiserver-79b757694f-wgrp4   1/1     Running   1 (18m ago)   4d20h

NAME                 TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
service/calico-api   ClusterIP   10.104.124.240   <none>        443/TCP   4d20h

NAME                               READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/calico-apiserver   2/2     2            2           4d20h

NAME                                          DESIRED   CURRENT   READY   AGE
replicaset.apps/calico-apiserver-79b757694f   2         2         2       4d20h
```

calico-system namespace (obsahuje Calico agenty)

```
[root@tvlakub11:/home/exdmachacek/cluster]# k get all -n calico-system
NAME                                          READY   STATUS    RESTARTS      AGE
pod/calico-kube-controllers-6558f8856d-mptf9   1/1     Running   1 (19m ago)   4d20h
pod/calico-node-ck77s                          1/1     Running   1 (29m ago)   2d21h
pod/calico-node-h8m2l                          1/1     Running   1 (29m ago)   2d22h
pod/calico-node-r6dw8                          1/1     Running   1 (28m ago)   4d20h
pod/calico-node-vbggj                          1/1     Running   1 (19m ago)   4d20h
pod/calico-node-xrvjd                          1/1     Running   1 (12m ago)   4d16h
pod/calico-typha-59dcfc9f44-6xm2q              1/1     Running   2 (12m ago)   4d16h
pod/calico-typha-59dcfc9f44-trdk7              1/1     Running   2 (15m ago)   4d20h
pod/calico-typha-59dcfc9f44-w67r6              1/1     Running   1 (29m ago)   2d21h
pod/csi-node-driver-2xk4h                      2/2     Running   2 (29m ago)   2d21h
pod/csi-node-driver-dbgdh                      2/2     Running   2 (12m ago)   4d16h
pod/csi-node-driver-fsrgc                      2/2     Running   2 (19m ago)   4d20h
pod/csi-node-driver-mb4t5                      2/2     Running   2 (28m ago)   4d20h
pod/csi-node-driver-qpk57                      2/2     Running   2 (29m ago)   2d22h

NAME                                      TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/calico-kube-controllers-metrics   ClusterIP   None            <none>        9094/TCP   4d20h
service/calico-typha                      ClusterIP   10.104.188.39   <none>        5473/TCP   4d20h

NAME                             DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR
AGE
daemonset.apps/calico-node       5         5         5       5            5           kubernetes.io/os=linux
4d20h
daemonset.apps/csi-node-driver   5         5         5       5            5           kubernetes.io/os=linux
4d20h

NAME                                      READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/calico-kube-controllers   1/1     1            1           4d20h
deployment.apps/calico-typha              3/3     3            3           4d20h

NAME                                                 DESIRED   CURRENT   READY   AGE
replicaset.apps/calico-kube-controllers-6558f8856d   1         1         1       4d20h
replicaset.apps/calico-typha-59dcfc9f44              3         3         3       4d20h
```

Wireguard

Pro potřeby šifrování komunikace mezi jednotlivými uzly je využívána technologie Wireguard. Nastavení pro IPv4 je provedeno skrz úpravu CRD FelixConfiguration. Předpokladem instalace je existence balíků kmod-wireguard a wireguard-tools.

Instalace

```
kubectl patch felixconfiguration default --type='merge' -p '{"spec":{"wireguardEnabled":true}}'
```

Validace

Vygenerování wireguardPublicKey pro jednotlivé uzly.

```
calicoctl get nodes --allow-version-mismatch tvlakub11.pmb.cz -o yaml
apiVersion: projectcalico.org/v3
kind: Node
metadata:
  ..
  name: tvlakub11.pmb.cz
  resourceVersion: "1750962"
  uid: 2fcd9188-a98b-4783-9a05-98f70b9c1af2
spec:
  addresses:
  - address: 172.18.204.190/22
    type: CalicoNodeIP
  - address: 172.18.204.190
    type: InternalIP
  bgp:
    ipv4Address: 172.18.204.190/22
    ipv4IPIPTunnelAddr: 172.17.228.0
  orchRefs:
  - nodeName: tvlakub11.pmb.cz
    orchestrator: k8s
  wireguard:
    interfaceIPv4Address: 172.17.228.7
status:
  podCIDRs:
  - 172.17.0.0/24
  wireguardPublicKey: obaTOc3MYXGl9ruS2/iIhQKEhBF6xkw8WbIjgUbnSCc=
```