Konfigurace nódu

Postup pro přípravu nódu

Cílem je připravit nový uzel pro napojení do kubernetes cluster ať už jako master (tj. součást Control Plane), tak jako worker (tj. Data Plane). Návody počítají s OS CentOS a připraveným truststore obsahující certifkáty PPF Banky.

Dokumentace

https://kubernetes.io/docs/setup/production-environment/container-runtimes/

Povolení bridged traffic

Umožnění IPtables "vidět" bridget traffic.

bridge traffic

```
cat <<EOF | sudo tee /etc/modules-load.d/k8s.conf
overlay
br_netfilter
EOF

sudo modprobe overlay
sudo modprobe br_netfilter

cat <<EOF | sudo tee /etc/sysctl.d/k8s.conf
net.bridge.bridge-nf-call-iptables  = 1
net.bridge.bridge-nf-call-ip6tables = 1
net.ipv4.ip_forward                 = 1
EOF

sudo sysctl --system
```

Důvod

Kubernetes kube-proxy používá iptables pro směrování dotazů na příslušné kontejnery. Aby toto bylo možné, tak je nutné zapnout přesměrování IPv4 traffic přes virtual bridge mezi vnitřní kubernetes sítí a sítí, kam je nód připojen. Díky tomu se mohou předávat requesty kontejnerů mezi nódy. Pro tyto účely je nutno zapnout moduly br_netfilter a overlay, persistovat toto nastavení i přes případné restarty v /etc/modules-load.d/k8s.conf a /etc/sysctl.d/k8s.conf.

Instalace balíčků

Instalace příslušných balíčků

kubeadm

```
dnf install -y containerd.io kubeadm kubectl
```

Důvod

- **kubeadm** - nástroj vytvořený tak, aby poskytoval `kubeadm init` a `kubeadm join` pro vytváření clusterů Kubernetes. Provádí akce nezbytné pro zprovoznění a spuštění minimálního životaschopného clusteru. Podle návrhu se stará pouze o bootstrapping, ne o poskytování strojů. Stejně tak není zahrnuta instalace různých užitečných doplňků, jako je Kubernetes Dashboard, monitorovací řešení a doplňky specifické pro cloud.
- **kubectl** - Nástroj příkazového řádku Kubernetes, kubectl, vám umožňuje spouštět příkazy proti clusterům Kubernetes. Kubectl můžete použít k nasazení aplikací, kontrole a správě prostředků clusteru a zobrazení protokolů. Další informace včetně úplného seznamu operací kubectl naleznete v referenční dokumentaci kubectl.
- **containerd** - containerd je běhové prostředí kontejneru, které spravuje životní cyklus kontejneru na fyzickém nebo virtuálním počítači (hostiteli). Je to proces démona, který vytváří, spouští, zastavuje a ničí kontejnery. Je také schopen stahovat obrazy kontejnerů z registrů kontejnerů, připojovat úložiště a povolit vytváření sítí pro kontejner.
- **kubelet** - Kubelet je primární kubernetes agent, který běží na každém uzlu. Může zaregistrovat uzel na apiserveru pomocí jednoho z: název hostitele; příznak pro přepsání názvu hostitele; nebo specifická logika pro poskytovatele cloudu. Nainstalováno jako dependeny pro kubeadm

Kubelet a Containerd.io běží jako Linux služby a jsou řízené přes systemctl.

CRI konfigurace

Je nutno upravi konfiguraci CRI. Důvodem je zajištění stahování tzv. pause kontejnerů z proxy image repository, který se v PPF Bance používá.

Containerd

```
cat <<EOF | sudo tee /etc/containerd/config.toml
version = 2
enabled_plugins = ["cri"]
[plugins."io.containerd.grpc.v1.cri"]
  sandbox_image = "nexus.pmb.cz:5511/pause:3.9"
EOF

systemctl enable --now containerd
```

Důvod

Pause kontejnery jsou kontejnery, které jsou defaultně spouštěny v CRI pro alokaci síťového rozhraní (IP adresy), cgroup a namespace pro možnost následného spuštění samotného business kontejneru. Ač tyto kontejnery nejsou vidět v seznamu podů, tak při pohledu z nódu je lze vidět. Zobrazit běžící kontejnery v containerd lze přes příkaz ctr -n k8s.io containers list (k8s.io je namespace pro všechny kontejnery spravované v kubernetes). Detailní popis - https://www.ianlewis.org/en/almighty-pause-container

```
[root@tvlaworker13:/home/exdmachacek]# ctr -n k8s.io containers list
CONTAINER
IMAGE                                                    RUNTIME
19d54bde9567c13168bf64499968da8d7332a7bad4ba71f96400f7a702220138    nexus.pmb.cz:5511/kube-proxy:v1.
27.3                     io.containerd.runc.v2
27d3915d82db1a29ec799fbb4c278a3037292498533a08dc980befd417385183    nexus.pmb.cz:5511/pause:
3.9                              io.containerd.runc.v2
2da033bf713497ee306c058e1851534512f3ad495030cdb3fa63995e3b713c13    nexus.pmb.cz:5502/calico/node:v3.
26.1                     io.containerd.runc.v2
3236d11d8541921c55a5c96ee8037ff0454114af41d4e91aa2bd7aded8e9c992    nexus.pmb.cz:5511/pause:
3.9                              io.containerd.runc.v2
3291b8744ed28157369aa18a20d5999f29b2d216865639e2e426f2d50e138c0b    nexus.pmb.cz:5511/pause:
3.9                              io.containerd.runc.v2
3480f787272680e6bc9ab70508afcd531cb498f0bcaf13b5c94f863e0fc4f8da    nexus.pmb.cz:5502/calico/cni:v3.
26.1                     io.containerd.runc.v2
440352285c9e340c1d869a3b2ce2324064e6185d7b8701ad7c46e730ba8945dd    nexus.pmb.cz:5502/metallb/speaker:v0.
13.10                io.containerd.runc.v2
6f135b624876eddb46a3179bdfdfee2936c10bfee765267e2a6367bfda5eca44    nexus.pmb.cz:5511/pause:
3.9                              io.containerd.runc.v2
b10959610e3b1a3646807d8f61db6660e68f25e25f7e3daee58aaa658f55b75a    nexus.pmb.cz:5502/calico/csi:v3.
26.1                     io.containerd.runc.v2
bd76df207a5a40a28a699cde901a1342150f0642bbc90258baa4ca8050e84d91    nexus.pmb.cz:5502/calico/node-driver-
registrar:v3.26.1    io.containerd.runc.v2
e2cc11751c7cb1b9f5be34a93595fd549a01e37771c7f44eb414a2b7be45b80b    nexus.pmb.cz:5502/calico/pod2daemon-flexvol:
v3.26.1       io.containerd.runc.v2
```

Zapnutí kubelet

```
systemctl enable --now kubelet
```