

阿里云 × CLOUD NATIVE
COMPUTING FOUNDATION

云原生技术公开课

第 26 讲

理解 CNI 和 CNI 插件

溪恒 阿里巴巴技术专家



关注“阿里巴巴云原生”公众号
获取第一手技术资料



上节回顾

Kubernetes Pod网络是如何联通的

- **Pod**之间可以无**NAT**的互相联通
- **Pod**网络打通由各种网络虚拟化能力来实现

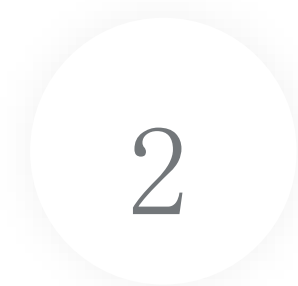
Kubernetes Service是如何工作的

- **Service**的概念和原理
- 用**IPVS**自己动手实现**Service**



CNI是啥

.....



Kubernetes中如何使用

.....



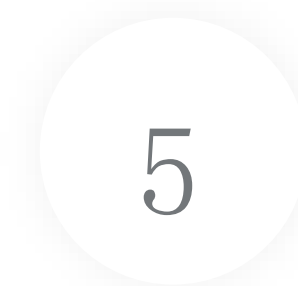
哪个CNI 插件适合我

.....



如何开发自己的CNI插件

.....



课后思考实践

CNI 是啥

- **Container Network Interface**, 容器网络的**API**接口
- **Kubelet**通过这个标准的**API**调用不同的网络插件实现配置网络
- **CNI**插件：一系列实现了**CNI API**接口的网络插件

Calico



Weave Net

Terway



1

CNI是啥

.....

2

Kubernetes中如何使用

.....

3

哪个CNI插件适合我

.....

4

如何开发自己的CNI插件

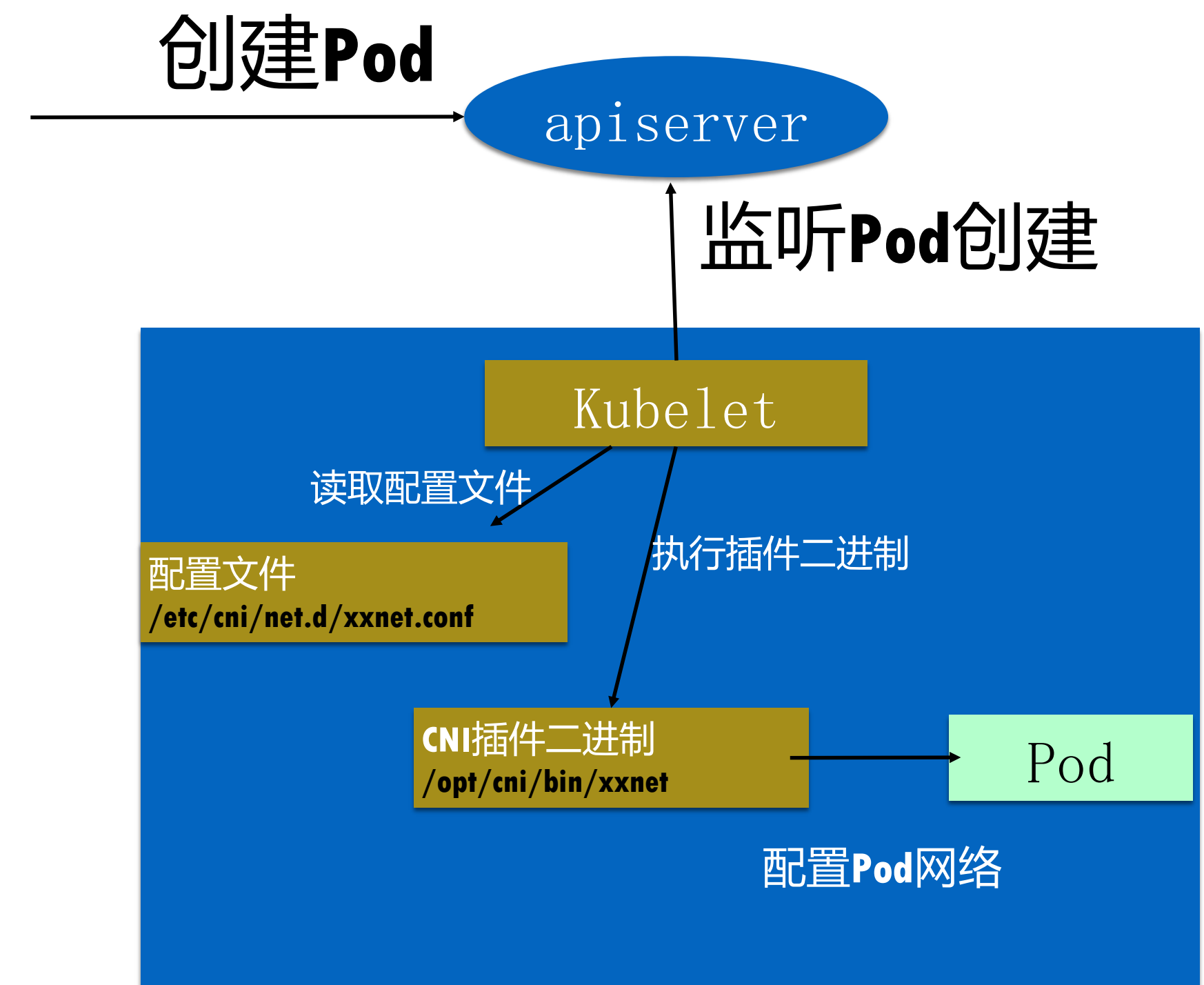
.....

5

课后思考实践

Kubernetes中如何使用

1. 配置**CNI**配置文件 (`/etc/cni/net.d/xxnet.conf`)
2. 安装**CNI**二进制插件 (`/opt/cni/bin/xxnet`)
3. 在这个节点上创建**Pod**
4. **Kubelet**会根据**CNI**配置文件执行**CNI**插件
5. **Pod**的网络就配置完成了



Kubernetes中如何使用

安装个**CNI**插件要这么步骤?

好在如果只是使用**CNI**插件的话, 大部分**CNI**插件的提供者都可以一键安装

例如**Flannel**安装:

Deploying flannel manually

Flannel can be added to any existing Kubernetes cluster though it's simplest to add `flannel` before any pods using the pod network have been started.

```
For Kubernetes v1.7+ kubectl apply -f https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube-flannel.yml
```

只需要一个命令, 配置和二进制自动安装配置

See [Kubernetes](#) for more details.

Flannel会通过**Demonset**自动把配置和二进制拷贝到**Node**的配置文件夹中

1

CNI是啥

.....

2

Kubernetes中如何使用

.....

3

哪个CNI插件适合我

.....

4

如何开发自己的CNI插件

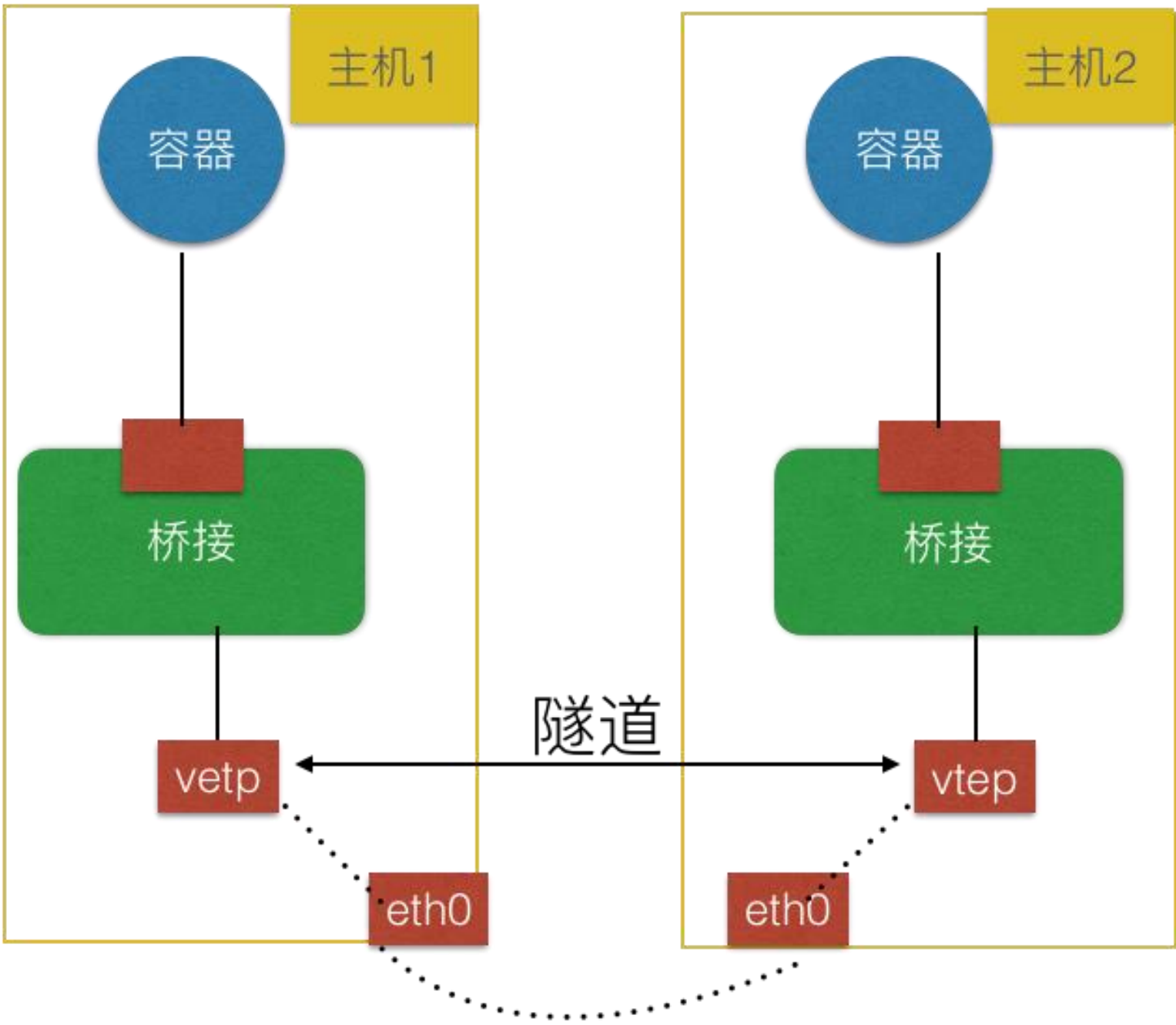
.....

5

课后思考实践

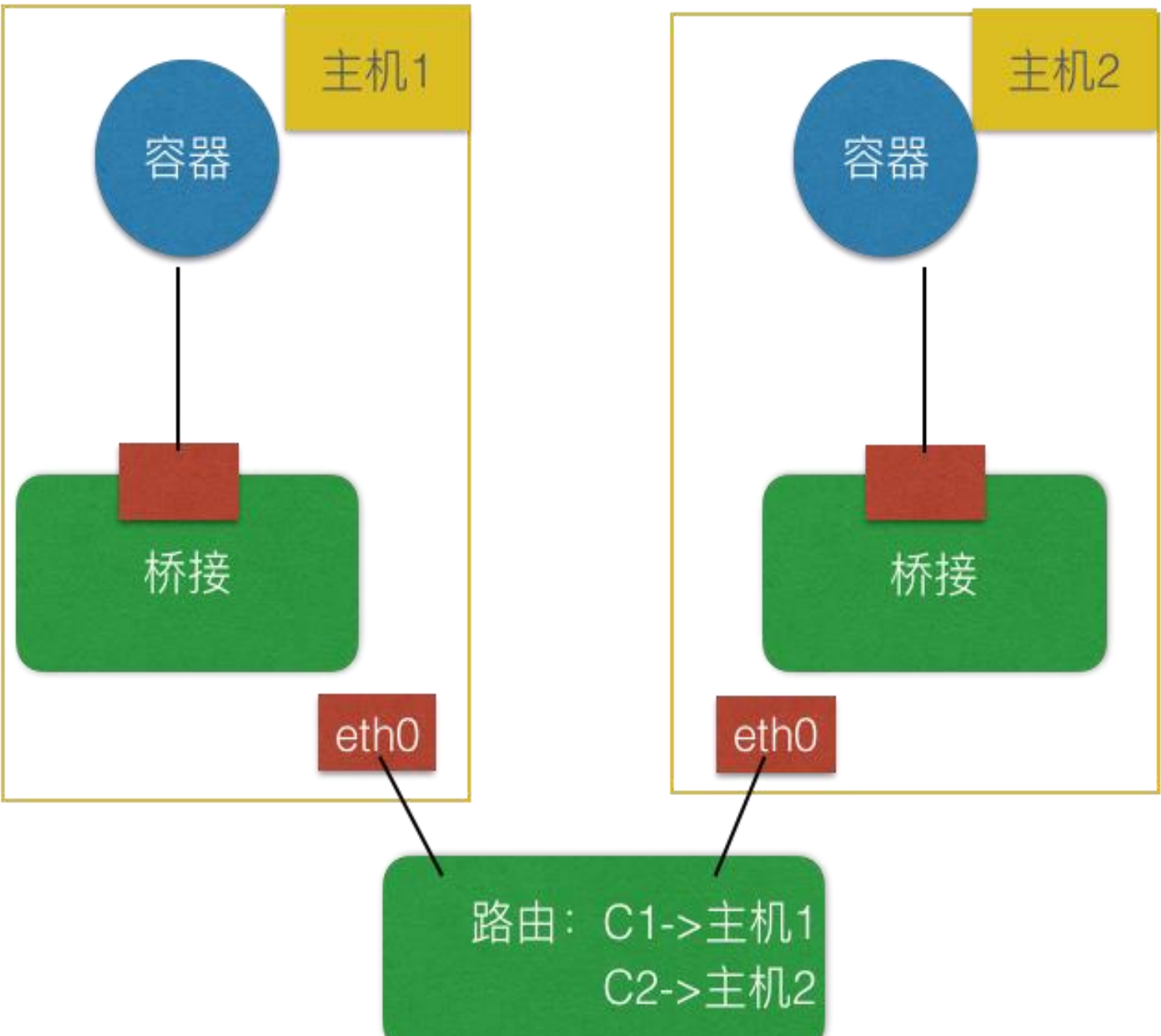
哪个CNI插件适合我

CNI插件通常有三种实现模式



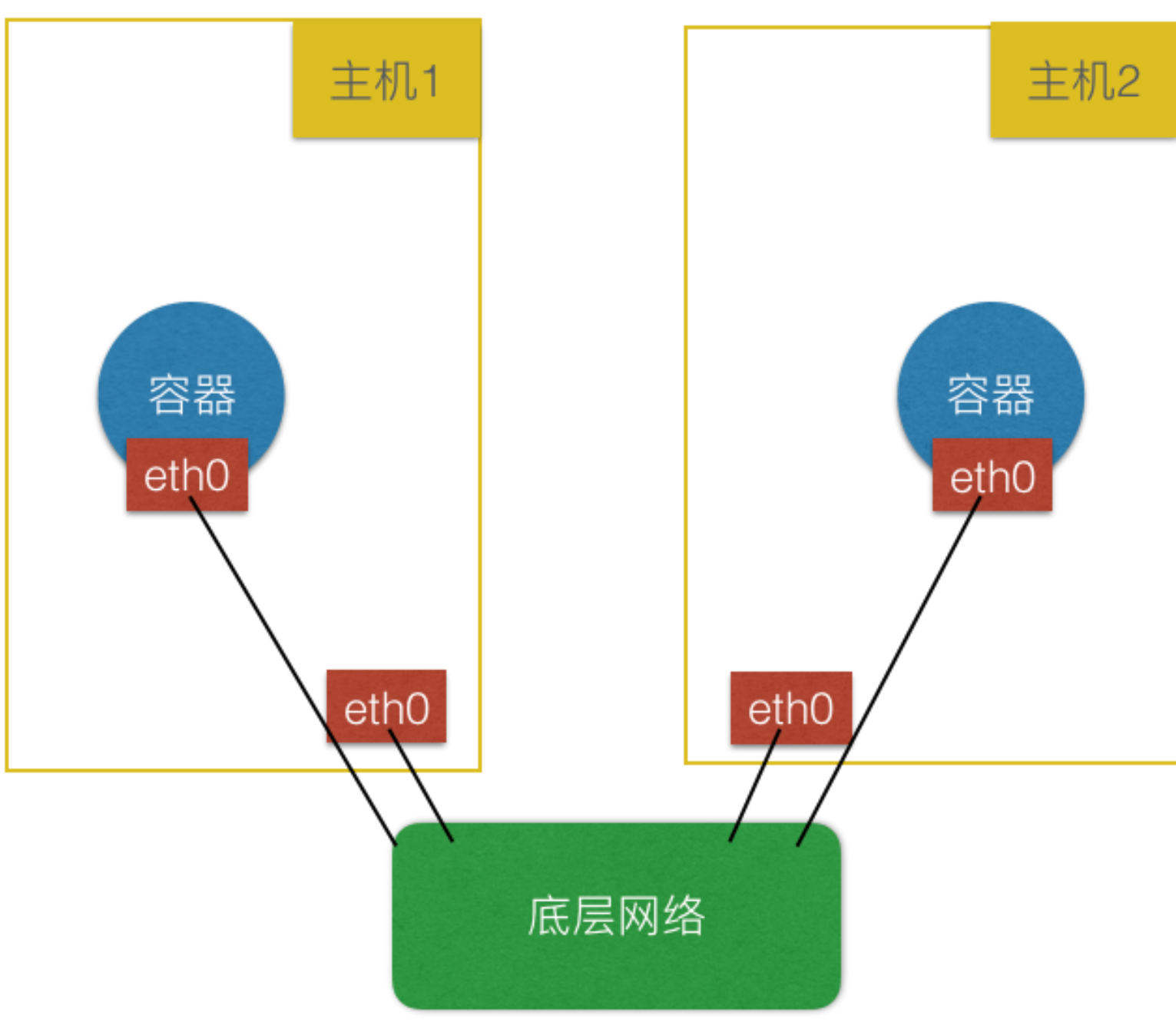
Overlay

靠隧道打通，不依赖底层网络



路由

靠路由打通，部分依赖底层网络

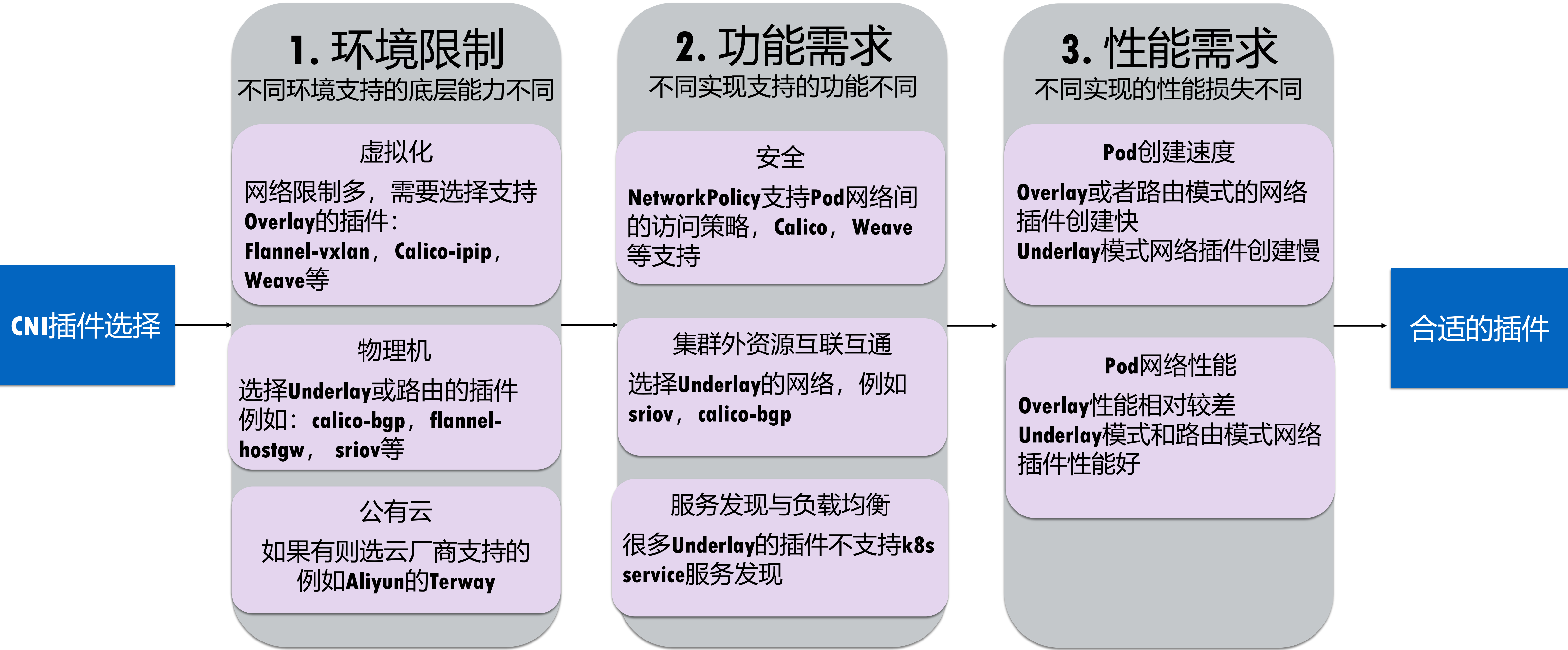


Underlay

靠底层网络能力打通，强依赖底层

哪个CNI插件适合我

社区那么多插件，需要如何选择？适合的才是最好的，从下面去考虑



1

CNI是啥

.....

2

Kubernetes中如何使用

.....

3

哪个CNI插件适合我

.....

4

如何开发自己的CNI插件

.....

5

课后思考实践

如何开发自己的CNI插件

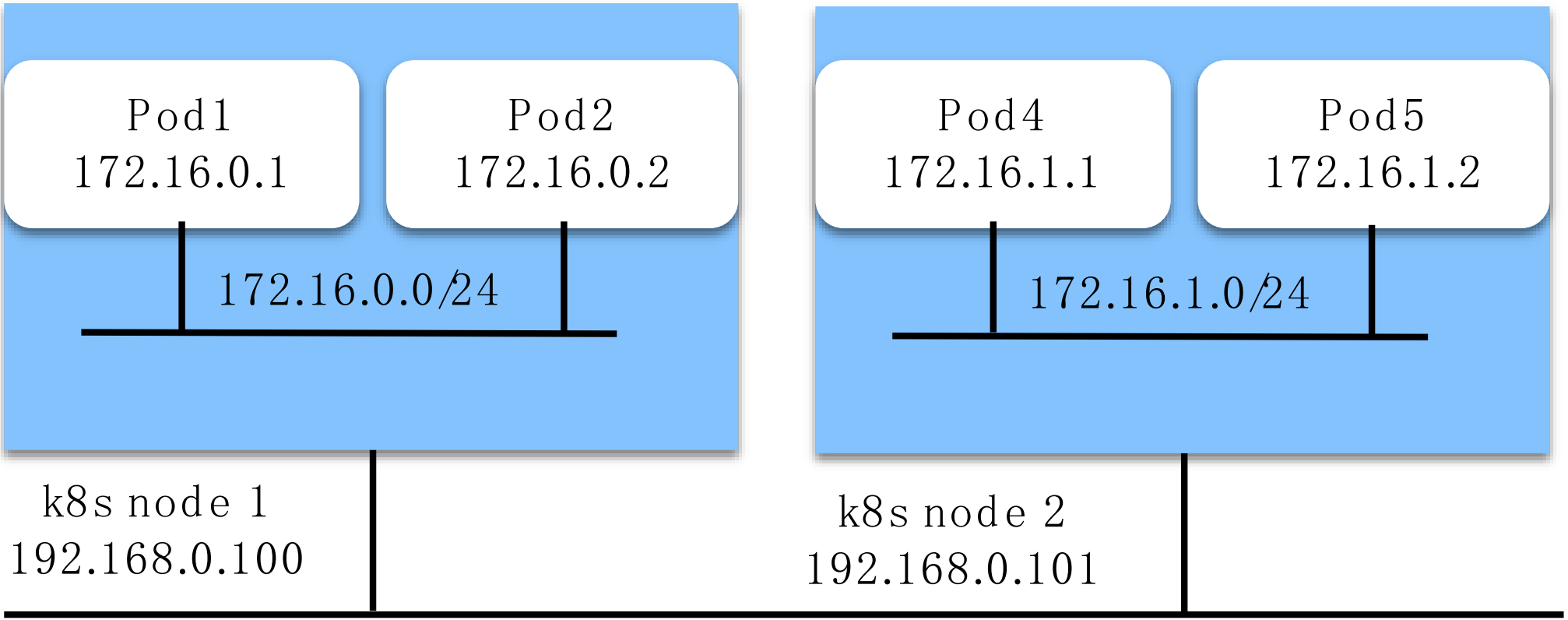
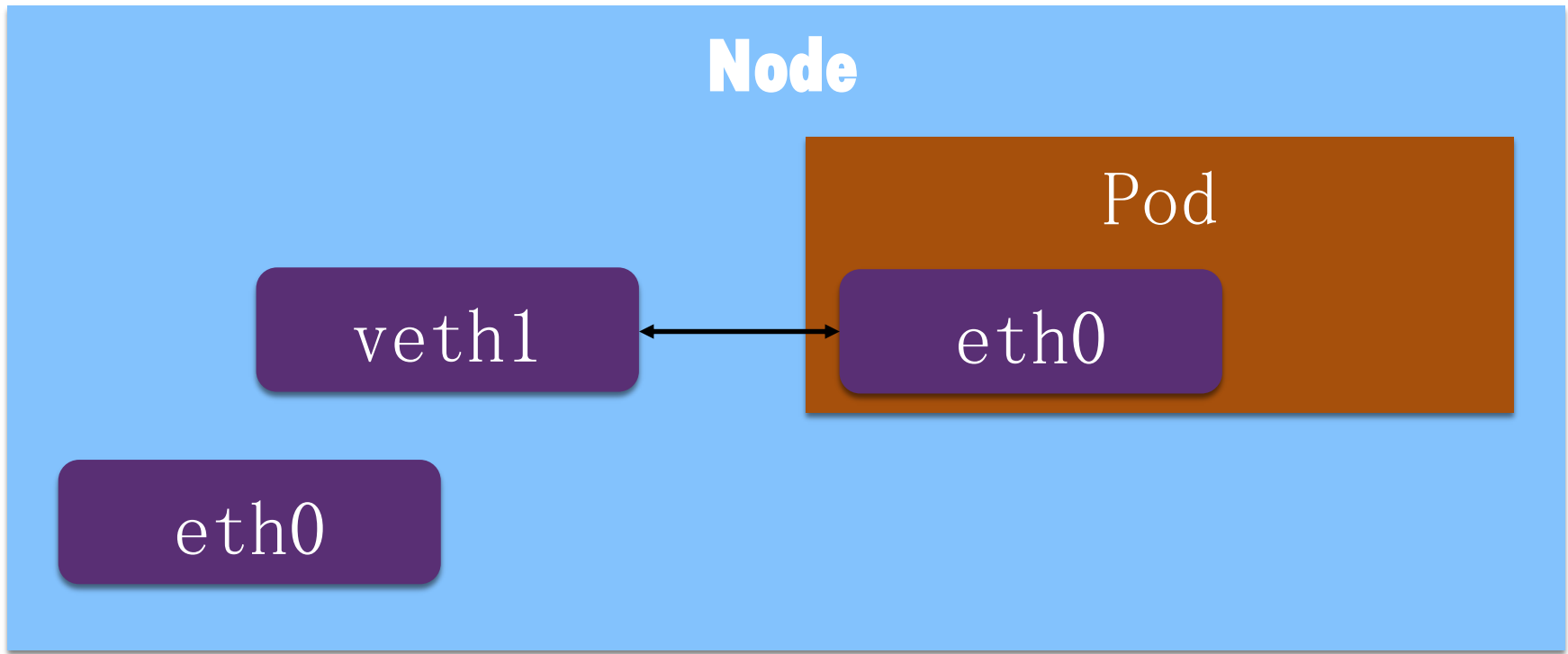
CNI插件实现通常需要两个部分：

- 一个二进制的**CNI**插件去配置**Pod**的网卡和**IP**等 —————> 给**Pod**插上网线
- 一个**Daemon**进程去管理**Pod**之间的网络打通 —————> 给**Pod**连上网络

如何开发自己的CNI插件

给Pod插上网线

1. 给Pod准备虚拟网卡
 - 创建“veth”虚拟网卡对
 - 将一端的网卡挪到Pod中
2. 给Pod分配IP地址
 - 给Pod分配集群中唯一的IP地址
 - 一般会把Pod网段按Node分段
 - 每个Pod再从Node段中分配IP
3. 配置Pod的IP和路由
 - 给Pod的虚拟网卡配置分配到的IP
 - 给Pod的网卡上配置集群网段的路由
 - 在宿主机上配置到Pod的IP地址的路由到对端虚拟网卡上



如何开发自己的CNI插件

给Pod连上网络： 让每一个Pod的IP在集群中都能被访问到

1. **CNI Daemon**进程学习到集群所有Pod的IP和其所在节点
 - 通常通过请求**K8S APIServer**拿到现有Pod的IP地址和节点
 - 监听**K8S APIServer**新的Node和Pod的创建自动配置
2. **CNI Daemon**配置网络来打通Pod的IP的访问
 - 创建到所有Node的通道：
Overlay隧道，**VPC**路由表，**BGP**路由等
 - 将所有Pod的IP地址跟其所在Node的通道关联起来
Linux路由，**Fdb**转发表，**OVS**流表等

1

CNI是啥

.....

2

Kubernetes中如何使用

.....

3

哪个CNI插件适合我

.....

4

如何开发自己的CNI插件

.....

5

课后思考实践

课后思考实践

- 在自己公司的网络环境中，选择哪种网络插件最适合？
- 尝试自己实现一个**CNI**插件

谢谢观看

THANK YOU



关注“阿里巴巴云原生”公众号
获取第一手技术资料

