



# 微服务的容器化实践

灵雀云 邢海涛





# 议程

---

**01** 微服务容器化实践

**02** 用户案例

---

# 微服务容器化实践

## ■ 镜像管理

- Docker Registry, Harbor, JHipster

## ■ 容器编排

- Kubernetes, Mesos, Docker Swarm



# 用户案例

**开发环境**，桌面微服务访问K8s集群内依赖，WireMock？

**测试环境**，k8s集群内微服务互访

# 用户案例 – 根本问题

主机网络和容器网络**可能**不通

因为Kubernetes只定义规范，导致网络方案太多

因为跨节点的容器网络不通：

- 容器地址重复
- 容器地址不可达



# 方案 – Networking ( 1 )

	Overlay	L3 Routing	Underlay
描述	把二层报文封装在IP报文之上进行传输	通过三层路由的方式向IP报文传输到目的宿主机	直接使用底层网络的IP，与宿主机在同一个网络里进行通讯
网络要求	底：IP可达	二层可达或BGP可达	二层可达
性能	中：封包、拆包	高：路由转发	高：几乎没有损耗
IP类型	虚拟IP	虚拟IP	物理IP
静态IP	不支持	不支持	支持（灵雀云）
场景	对性能要求不高的； 网络环境不灵活的	大多数场景	对性能要求高的； 需要和现有业务直接通信； 需要静态IP



# 方案 – Networking ( 2 )

## Underlay: MacVLAN / IpVLAN

- 性能好； MacVlan独立MAC地址， IpVlan共享MAC地址
- IpVlan 在 IaaS 中更灵活，如：VMWare 无需混杂模式，及解除 VM 的 MAC 限制
- IpVlan 可以节省Mac地址资源，降低 L2 的压力 或 switch 的 Port Security



# 方案 – Networking ( 3 )

## Underlay: MacVLAN / IpVLAN

- 网络管理平面不能很好的分割
- IpVlan 需要 Kernel 升级到 4.2
- IpVlan 可能的 IPv6 问题：可能会自动生成相同的 IPv6 地址（静态分配或禁用SLAAC）
- VMWare Vsphere 需要开放混杂模式
- 容器网络安全（Network Policy）没有提供，需要依赖外部网络



# 方案 – Networking ( 4 )

## L3 Routing: Flannel – HostGateway

- 集群可以跨 VLAN ( 但需要外部按照各节点网段配静态路由 )
- 节省二层 IP 和 MAC
- 集群内支持 Network Policy , 按标签、按 IP
- 利于弹性伸缩
- 外部访问策略可以基于 LB 的 IP/Port , 也可以基于 Pod IP



# 方案 – Networking ( 5 )

## L3 Routing: Flannel – HostGateway

- 不支持固定 IP (通过主机标签可固定 IP 段)
- 只能用于二层直接可达的网络
- 广播风暴的问题，网络规模通常比较小



# 方案 – Networking ( 6 )

## Overlay: Flannel – VxLAN

- 集群可以跨 VLAN
- 节省二层 IP 和 MAC
- 集群内支持 Network Policy , 按标签、按 IP
- 利于弹性伸缩



# 方案 – Networking ( 7 )

## Overlay: Flannel – VxLAN

- 不支持固定 IP (通过主机标签可固定 IP 段)
- 集群外访问策略只能基于 LB 的 IP/Port
- 目前集群的 LB 对外只有一个 IP，如果需要独占的附加服务 IP，需要开发实现



# 方案 – Telepresence ( 1 )

## Telepresence - CNCF沙箱项目

- 本地服务完全访问远程群集中的其他服务
- 本地服务完全访问Kubernetes环境变量， secrets和ConfigMap
- 远程服务完全访问本地服务
- 仅支持MacOS 和 Linux



# 方案 – Telepresence ( 2 )

## Telepresence原理

- 实现一个双向的网络代理：远程集群定制的代理, 及本代理
- 使用sshfs实现卷代理



# 方案 - 微服务网关（1）

用户的需求：本地服务到远程服务的访问，可以是单向的



# 方案 - 微服务网关 (2)

- 远程服务通过微服务网关暴露到主机网络
- 为Spring Cloud应用定制profile: desktop
- 根据profile转换RestTemplate的服务调用URI
- Desktop profile只获取不注册到Eureka



# 方案 - 微服务网关（3）

- 本地服务如何访问本地依赖？



# 总结

- 有时候不得不深入细节，什么才是完美答案？





—  
**THANK YOU**

**DD**CHINA