

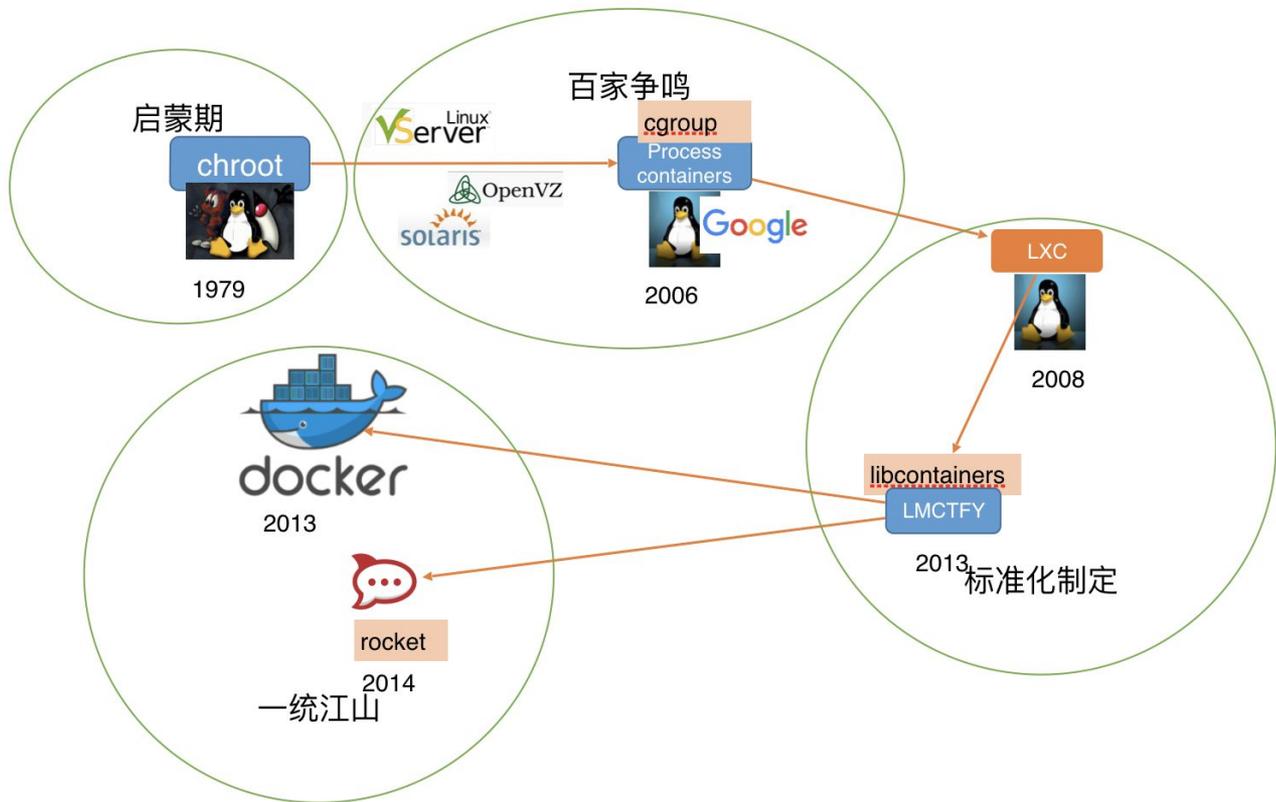
Caas与IaaS网络融合实践

By niusmallnan

议程

1. Caas正突入云服务领域
2. Caas网络的需求和隐患
3. 解决之道与实践指南
4. Q&A

容器历史演进，技术日渐成熟



容器(Docker)解决什么问题



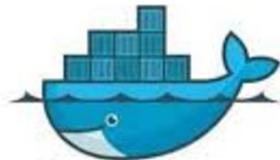
美国通用电气公司 (GE) 的经验是, 用了IaaS后, 部署VM只要15分钟, 而应用的部署配置却仍要3个星期以上。



Container as a service



AWS ECS



docker



MAGNUM

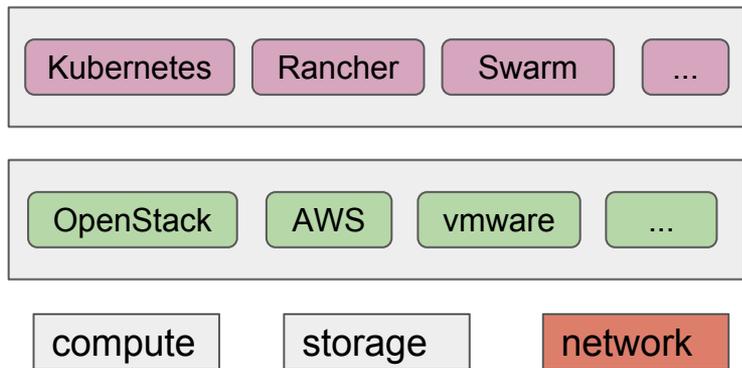
Containers as a Service



kubernetes



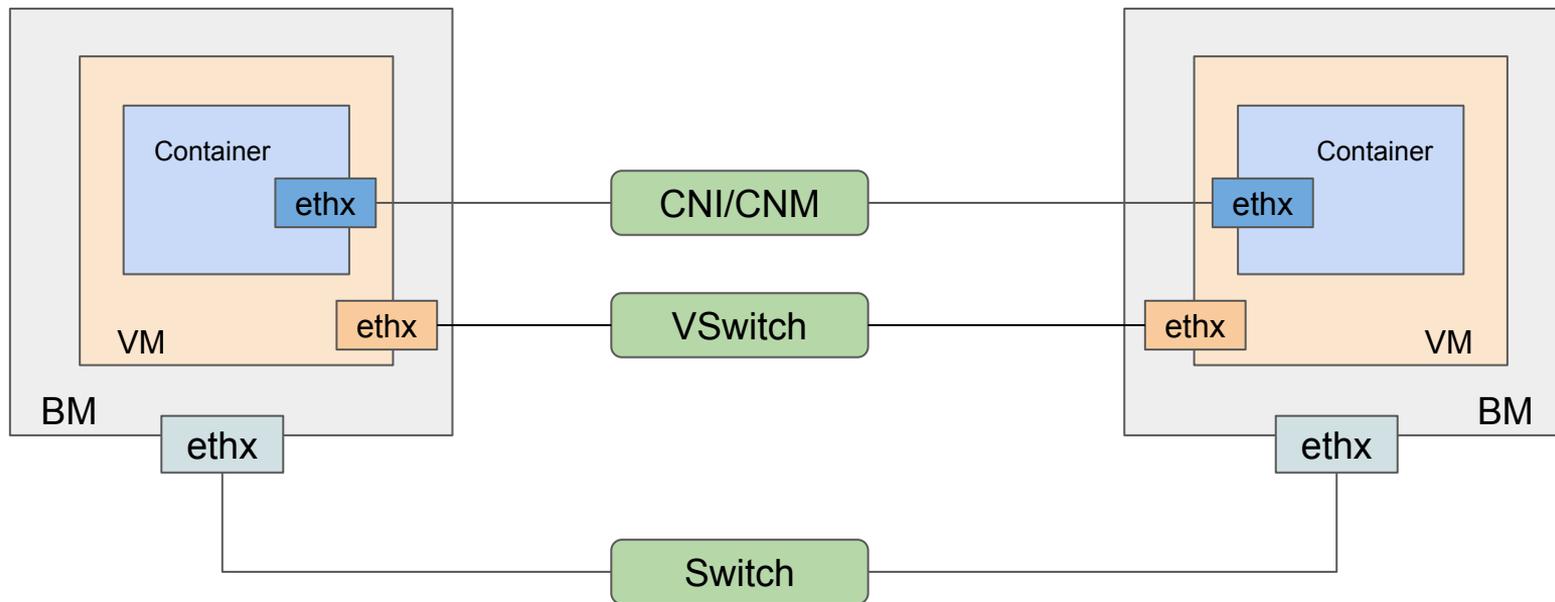
大部分Caas选择构建在IaaS之上



1. Caas的成熟度远没有达到可以管控物理资源
2. 功能角度, Caas只是对IaaS的补充, 无法替代
3. 主流的IaaS都在扩展对Caas的支持能力
4. 每一层架构都有自身的编排调度, 每一层都依托上一层提供的基础设施资源, 物理资源的实际使用率在不断递减

Caas网络的需求和隐患

全局网络概览



构建Caas网络两种模式

Caas内自治:

这种模式下, Caas不用关心底层设施服务, 完全依靠自身编排引擎对网络的管理。

好处:

对于用户来说, 管理非常简单, 无需各种干预。

劣势:

对于用户来说, 几乎不可控, 有些网络性能较差, 且很难与基础设施服务联动。

代表:

overlay(vxlan/ipsec)、Calico

依托IaaS:

这种模式下, 网络资源依然是依托IaaS来分配, Caas只是资源的使用方。

好处:

完全可控, 物理使用率比较高

劣势:

需要用户本身有较高的水准, 使用起来相对困难。

代表:

Kuryr(OpenStack)
结合CNI/CNM进行自定义

以Rancher为例 (Caas内自治)



Catalog: Library
Category: Networking
Support: Officially Certified

VXLAN Networking

Rancher networking plugin using VXLAN overlay.

Open Ports

Traffic to and from hosts requires UDP port **4789** to be open.

Template Version

v0.0.5

Select a version of the template to deploy

Configuration Options

Docker Bridge*

docker0

Name of Docker Bridge. Default is 'docker0'

Subnet*

10.42.0.0/16

The subnet to use for the managed network.

MTU for the network*

1500

Adjust the MTU for the network, according

Enable Debug Logs*

True False

This will enable very verbose debug logs.

以Rancher为例(依托IaaS)

Configuration Options

FLAT Bridge*

flatbr0

Name of Flat Bridge. Default is 'flatbr0'

MTU for the network*

1500

Adjust the MTU for the network, according to your needs. Ex: GCE(1460), AWS(1500), etc

Start IP Address*

172.22.101.110

The subnet to use for the managed network.

Gateway*

172.22.101.1

Container default gateway.

Subnet PrefixSize for IPAM*

24

Subnet PrefixSize for IPAM

FLAT Interface*

eth0

Name of Flat interface. Default is 'eth0'

Subnet*

172.22.101.0/24

The subnet to use for the managed network.

END IP Address*

172.22.101.240

The subnet to use for the managed network.

Enable Debug Logs*

True False

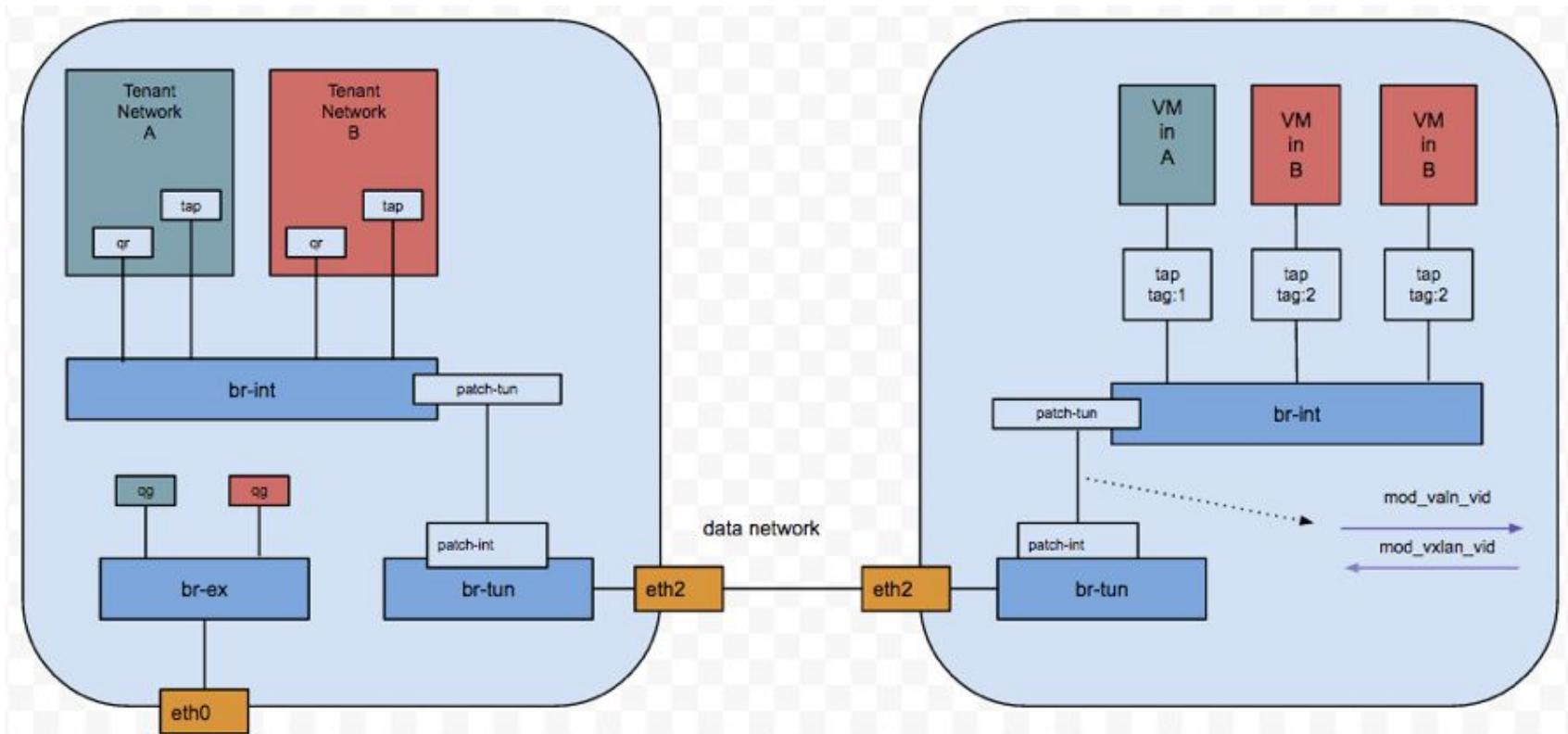
This will enable very verbose debug logs.

来自社区与用户的声音

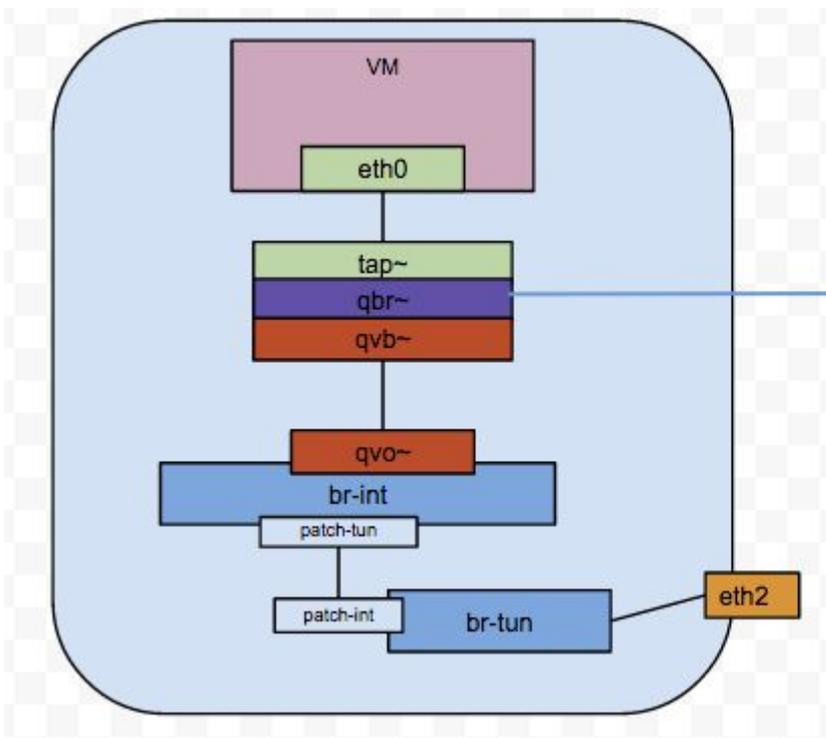
1. Caas还在不断演化中，用户还没有形成固定模式的使用习惯，IaaS上的遗留习惯依然会保留
2. 一容器一IP，很多时候还是像虚拟机一样使用容器
3. 如何构建高性能Caas网络
4. ...

与IaaS网络融合的解决之道 Rancher & OpenStack

OpenStack VM网络



OpenStack Security Group

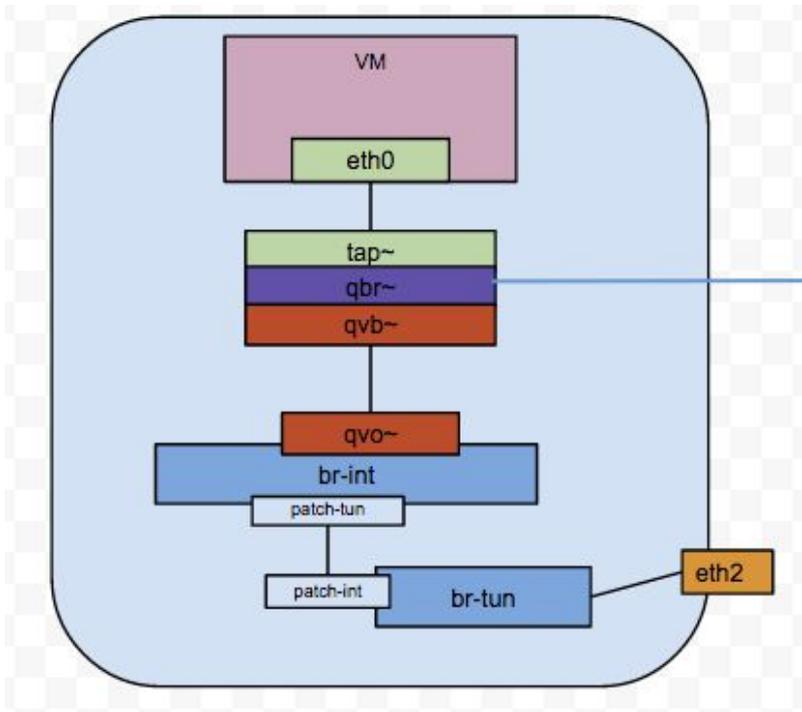


安全组作用位置

Caas网络痛点

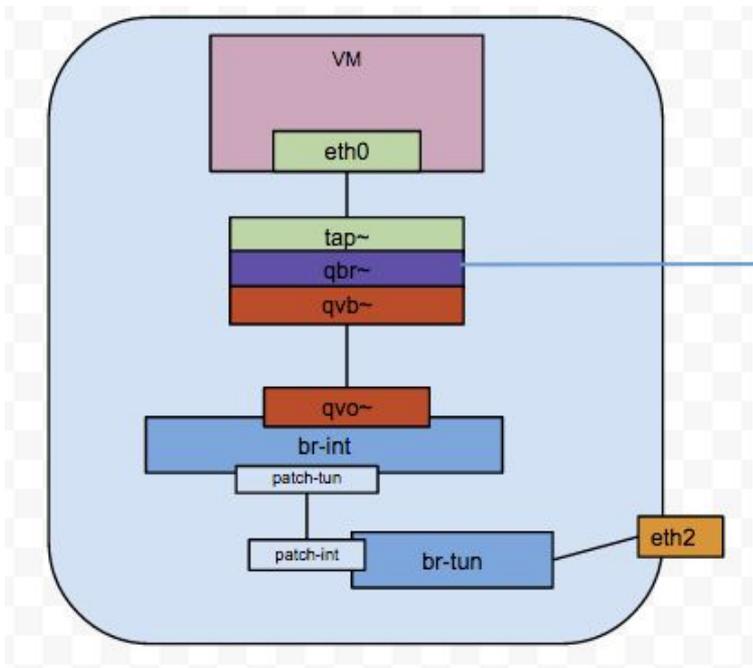
1. 需要嫁接在IaaS网络之上
2. Overlay on Overlay损耗巨大
3. 构建与IaaS subnet在同一网络中，需要“伪造”IP和MAC
4. “伪造”IP和MAC数据包默认不被通过

Disable Port Security



1. 安全规则accept all
2. 所有流量全通，所以安全组失效

Port Address Pairs



1. 默认只通过VM中eth0的ip和mac流量 (anti-spoofing)
2. Address pairs就是可以额外添加允许通过的ip和mac

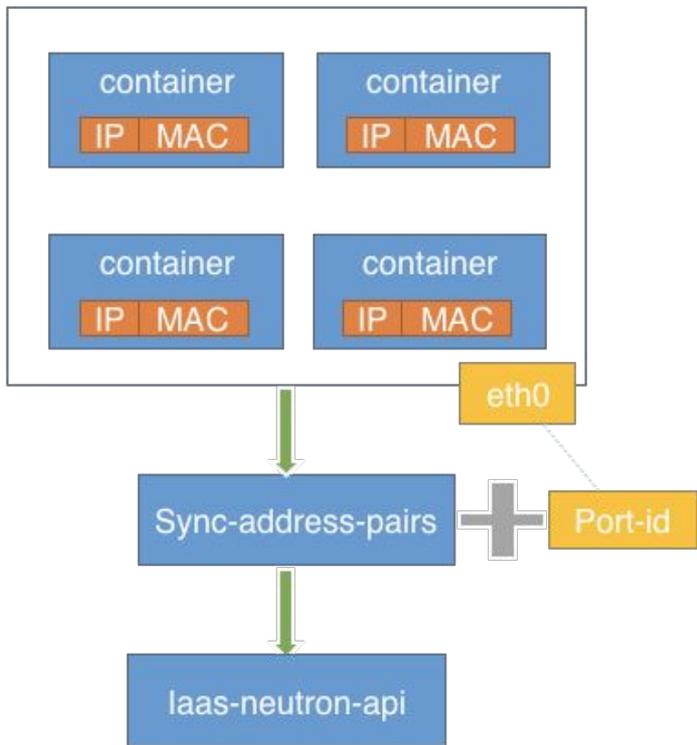
```
# neutron port-create net1 --allowed-address-pairs type=dict list=true
mac_address=<mac_address>,ip_address=<ip_cidr>
```

```
computel:~$ iptables -L neutron-openvswi-sebf586a5-a -n -v
```

```
Chain neutron-openvswi-sebf586a5-a (1 references)
```

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	RETURN	all	--	*	*	10.0.1.100	0.0.0.0/0	MAC FA:16:3E:42:A1:D4
47	0	RETURN	all	--	*	*	10.0.1.10	0.0.0.0/0	MAC FA:16:3E:42:A1:C4
3	252	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

容器扁平网络嫁接方案(Rancher)



方案一:

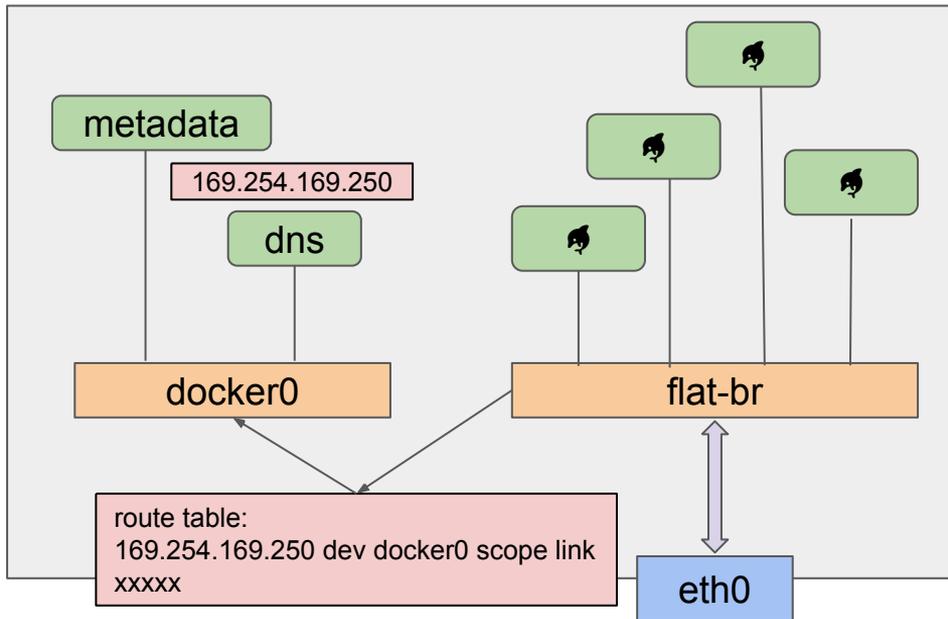
Caas内的服务程序自动将容器的ip&mac动态的设置到laas port中 (手动测试验证已经通过):

1. laas 的api能否支持这种频繁调用是个瓶颈
2. 每个laas port支持多少address pairs是个关键

方案二:

laas层面能够支持安全组存在的情况下, 可以伪造IP和MAC, 目前OpenStack的原型并不能很好的支持, 需要laas定制

虚拟机内部网络结构



AWS的关键设置

<input type="checkbox"/>	try-rancher-k8s-1	i-05e4ecb3d3ccec78	t2.medium
<input type="checkbox"/>	try-rancher-ingress	i-064dfc7a1d3b5184d	t2.small
<input checked="" type="checkbox"/>	try-vxlan-1	i-0664a49cb5ce97d3f	t2.small
<input type="checkbox"/>	try-rancher-nginx	i-0d2a383412493	t2.small
<input type="checkbox"/>	try-rancher-redis	i-084edd81d90d7	t2.small

- 连接
- 获取 Windows 密码
- 启动更多类似项
- 实例状态 ▶
- 实例设置 ▶
- 映像 ▶
- 联网 ▶
- CloudWatch 监控 ▶

- 更改安全组
- 附加网络接口
- 分离网络接口
- 解除弹性 IP 地址的关联
- 更改源/目标。检查
- 管理私有 IP 地址

启用源/目标检查

您确信要对包含以下详细信息的实例禁用源/目标检查吗？

实例: i-0664a49cb5ce97d3f (try-vxlan-1)
网络接口: eni-0bdb6953
状态: 已启用

取消

是，请禁用

Disable src/dst check

Caas网络插件式管理

 <p>PROJECT CALICO</p> <p>Calico</p> <p>A Pure Layer 3 Approach to Virtual Networking for Highly Scalable Data Centers</p> <p>View Details</p>	 <p>Rancher Labs</p>  <p>RANCHER NETWORK POLICY MANAGER</p> <p>Network Policy Manager</p> <p>Manager that applies Rancher network policies.</p> <p>View Details</p>	 <p>OPENVPN[®]</p> <p>OpenVPN HTTP Basic</p> <p>OpenVPN for Rancher with HTTP Basic authentication</p> <p>View Details</p>	 <p>OPENVPN[®]</p> <p>OpenVPN HTTP Digest</p> <p>OpenVPN for Rancher with HTTP Digest authentication</p> <p>View Details</p>
 <p>OPENVPN[®]</p> <p>OpenVPN Rancher</p> <p>OpenVPN for Rancher with "Rancher local" authentication</p> <p>View Details</p>	 <p>RANCHER FLAT NETWORK</p> <p>Rancher Flat Networking</p> <p>Rancher Networking plugin using Flat Networking.</p> <p>View Details</p>	 <p>Rancher Labs</p>  <p>RANCHER IPSEC</p> <p>Rancher IPsec</p> <p>Already Deployed</p>	 <p>Rancher Labs</p>  <p>RANCHER VXLAN</p> <p>Rancher VXLAN</p> <p>Rancher Networking plugin using VXLAN overlay.</p> <p>View Details</p>

Q&A