云联万维
YUNION

OneCloud虚机网络

周有松 @yousong

2019-10-26

内容提要

- OneCloud的网络模型
- 传统二层网络 vs. 软件定义网络
- 虚机网络功能介绍
  - metadata服务
  - DHCP主机网络配置
  - 防火墙
- SDN Agent的工作原理
  - 虚机事件管理
  - 服务升级和可维性

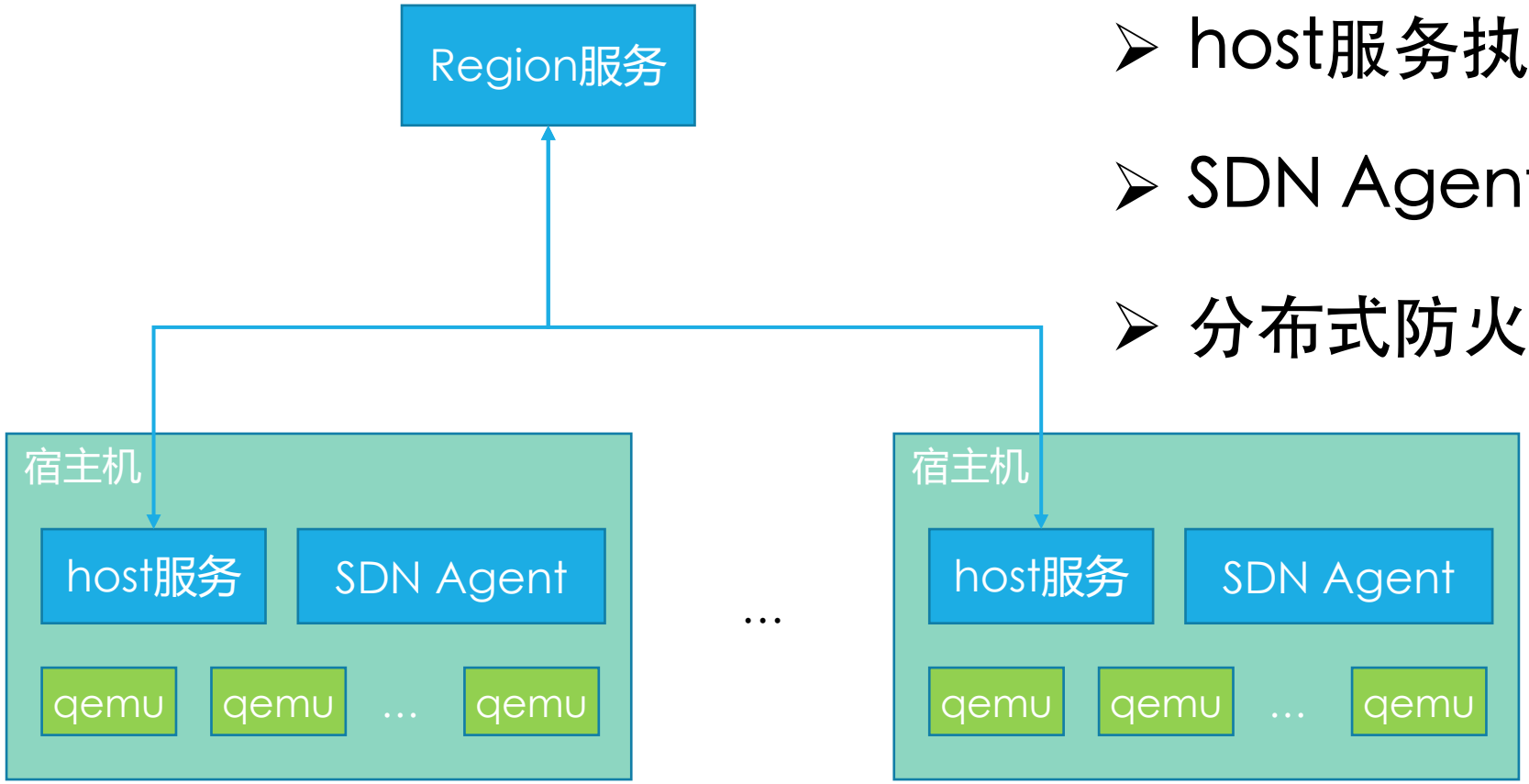
01

OneCloud网络模型

OneCloud的网络模型 – 控制流

云联万维 YUNION

- Region提供API服务
- host服务执行虚机生命周期管理
- SDN Agent负责虚机网络配置
- 分布式防火墙、DHCP



OneCloud的网络模型 – 数据结构

云联万维 YUNION

- Wire: 二层网络
  - 不同VLAN
  - 区域：管理网、业务网
- Network: 二层网络中的子网
  - 定义地址范围、网关信息等
  - 虚机可以attach, detach到多个子网：虚拟网卡
- 宿主机与wire的关联关系
- 调度器：虚机只可运行在wire条件满足的宿主机上

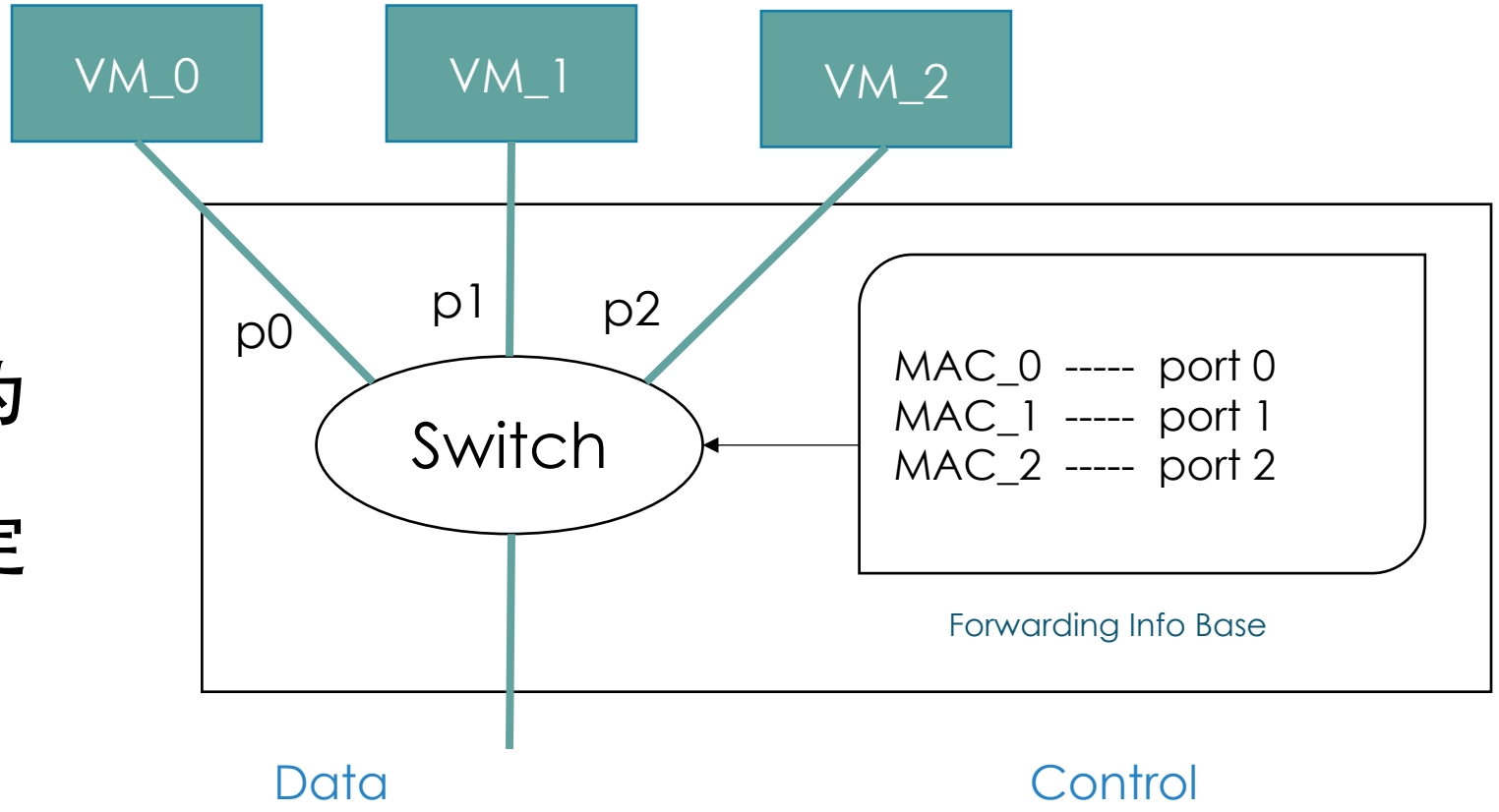
02

传统网络 vs. 软件定义网络

传统二层网络

特征

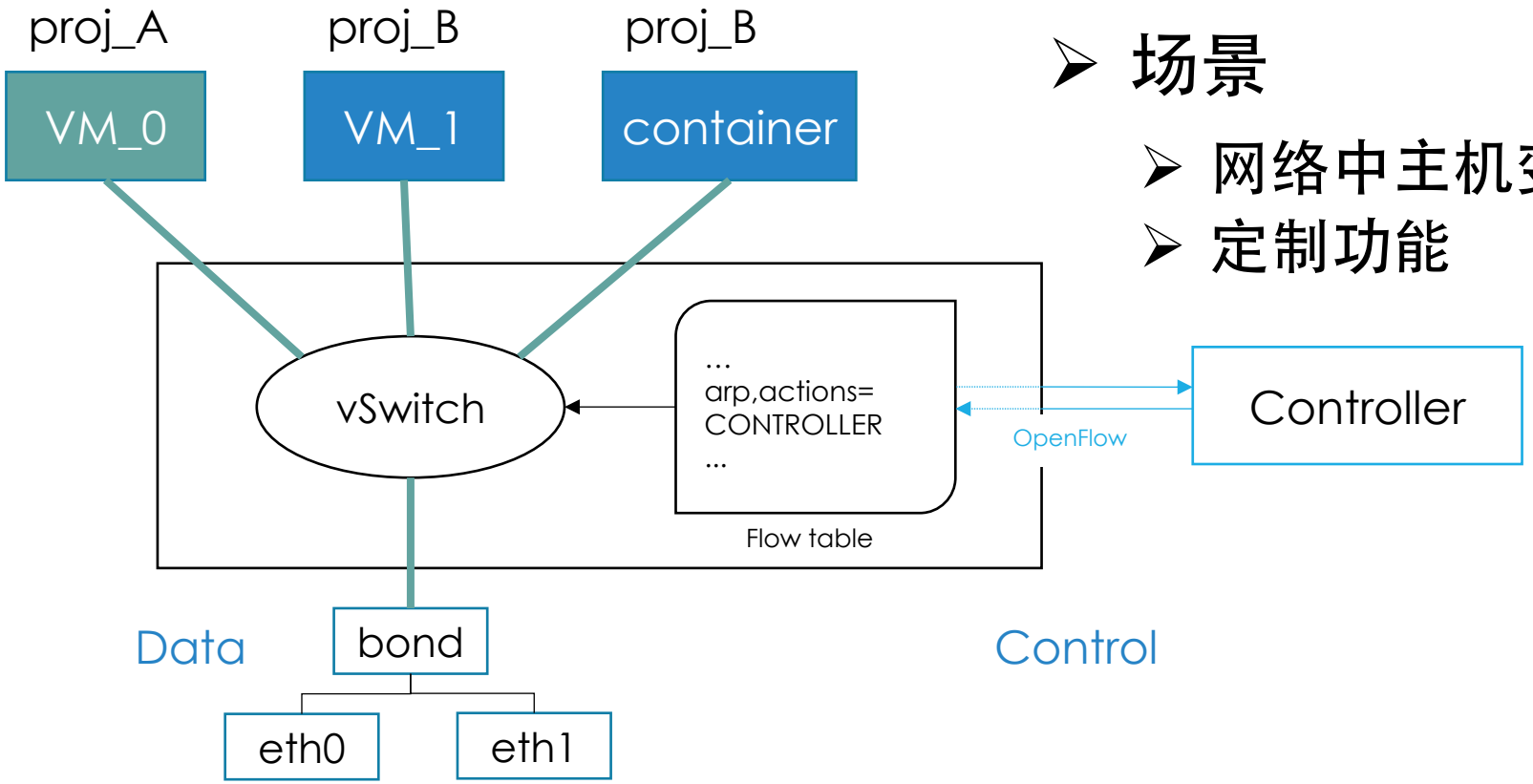
- 转发表决定转发行为
- 转发的行为模式固定



软件定义网络

云联万维 YUNION

- 特征
  - 可编程的控制面
  - 流表：<match, action>
- 场景
  - 网络中主机变更频繁
  - 定制功能



03

虚机网络功能介绍

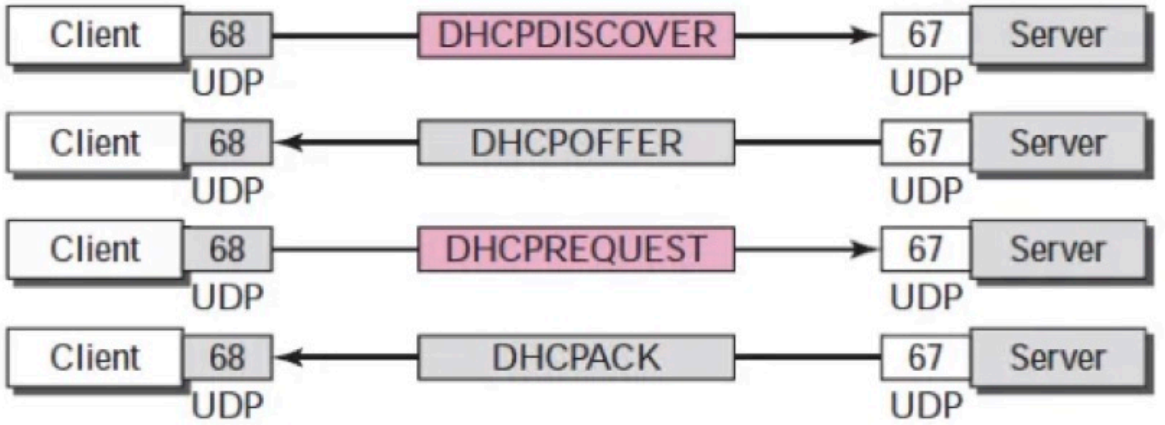
metadata服务

云联万维 YUNION

- 我是谁、我在哪里、我要做什么
- 提供关于虚机自身的描述信息
  - 实例ID
  - 网络配置：IP地址、MAC地址
- 利用cloud-init，实现定制化创建
  - 添加用户、组
  - 安装、升级软件包
  - 管理日志输出、监控等

```
+ curl http://169.254.169.254/latest/
meta-data
user-data
+ curl http://169.254.169.254/latest/meta-data
ami-launch-index
block-device-mapping/
hostname
instance-id
instance-type
local-hostname
local-ipv4
mac
public-hostname
public-ipv4
network_config/
placement/
security-groups/
+ curl http://169.254.169.254/latest/meta-data/instance-id
8344a066-053b-4769-baa9-b2aa7b03c686
+ curl http://169.254.169.254/latest/meta-data/hostname
titan
+ curl http://169.254.169.254/latest/meta-data/mac
00:22:54:e4:50:dc
+ curl http://169.254.169.254/latest/meta-data/local-ipv4
10.168.222.136
```

DHCP – 举例



- 从虚机发出的DHCP请求
  - 匹配： udp,in_port="vnet222-140",tp_src=68,tp_dst=67
  - 动作： mod_tp_dst:8067,LOCAL
- 从DHCP服务给虚机的回复
  - 匹配： udp,in_port=LOCAL,dl_dst=00:22:39:4c:6c:e9,tp_src=8067,tp_dst=68
  - 动作： mod_tp_src:67,output:"vnet222-140”

防火墙

云联万维 YUNION

- 方向：以虚机为中心，控制出、入两个方向
- 行为：allow, deny
- 匹配条件
  - 网段：cidr
    - 出：匹配目的地址
    - 入：匹配源地址
  - 协议：tcp, udp, icmp, any
  - 端口：“80,22”、“8000-8080”，不指定即any
- 举例
  - in:allow 0.0.0.0/0 tcp 22,80,3389
  - In:deny 0.0.0.0/0 udp 123

防火墙 – stateful

云联万维 YUNION

- 有状态 vs. 无状态：in:deny any

```
dl_dst=MAC_VM,ip actions=drop
```

- 需要netfilter conntrack记录连接状态，每块虚拟网卡一个 conntrack zone

```
                +invalid  actions=drop
+ingress, +new           actions=check_sec_IN
+ingress, +known         actions=accept
```

04

SDN Agent的工作原理

SDN Agent工作原理

云联万维 YUNION

- 在宿主机上，虚机的生命周期有专门的host服务管理
  - 写入、更新虚机描述文件
    - /opt/cloud/workspace/servers/<server-UUID>/desc
  - 管理虚机进程及其关联资源
- 通过内核inotify接口，实时监控虚机配置变化
- 根据虚机描述文件，确定应下发的流表集合
- 比较实际流表与期望流表差异，做出变更

SDN Agent工作原理 – 效果

云联万维 YUNION

- 网络功能为独立模块
  - 流表管理
    - metadata服务
    - dhcp服务
    - k8s service
  - 虚拟网卡QoS
- 不用担心API调用可能产生的失败、错过、重复
- 流表状态可预测
  - 内容可控，可分析
  - 升降版本不会出现多余、缺失
  - 不鼓励人工操作流表内容