

Linux Clusters Institute: OpenStack Neutron

Yale, August 13th – 17th 2018

John Michael Lowe | Senior Cloud Engineer
Indiana University
jomlowe@iu.edu



Neutron

- SDN or not
- Network Namespaces
- Components
- Security groups
- Virtual Routers
- Troubleshooting methods
- Additional items

SDN or Not

- Software Defined Networking the treatment of layer 2 and layer 3 is manipulated programmatically
- OpenVSwitch is the most commonly used SDN with OpenStack
- SDN offload onto NICs and Switches via DPDK (Data Path Development Kit) is becoming popular
- The simplicity, flexibility, and reliability of using in kernel bridging and overlay networks outweighs features of SDN in most cases

Network Namespaces

- One of the 7 namespaces in the Linux kernel
- Isolated
 - Interfaces
 - Iptables
 - Routing tables
 - IP address assignments
- Try it yourself
 - `ip netns add foo`
 - `ip netns list`
 - `ip link add veth0 type veth peer name veth1`
 - `ip link set veth1 netns foo`
 - `ip netns exec foo ip link list`

Components

- neutron-server
- neutron-linuxbridge-agent
- neutron-metadata-agent
- neutron-l3-agent
- neutron-dhcp-agent

Components: Neutron Server

- Serves API requests, database requests
- Configuration Files
 - /etc/neutron/neutron.conf
 - /etc/neutron/plugins/ml2/ml2_conf.ini
- Runs on controller

Components: Linuxbridge Agent

- Creates kernel bridges and adds needed interfaces
- Mapping from interfaces to OpenStack physical network names done in this agents configuration files
- Configuration files
 - /etc/neutron/neutron.conf
 - /etc/neutron/plugins/ml2/ml2_conf.ini
 - /etc/plugins/ml2/linuxbridge_agent.ini
- Runs on network and compute

Components: L3 Agent

- Creates a network namespace for NAT, floating ip addresses, routing IPV6
- Works together with L2 agent
- Configuration files
 - /etc/neutron/neutron.conf
 - /etc/neutron/l3_agent.ini
- Runs on network node (compute in DVR w/ OVS)

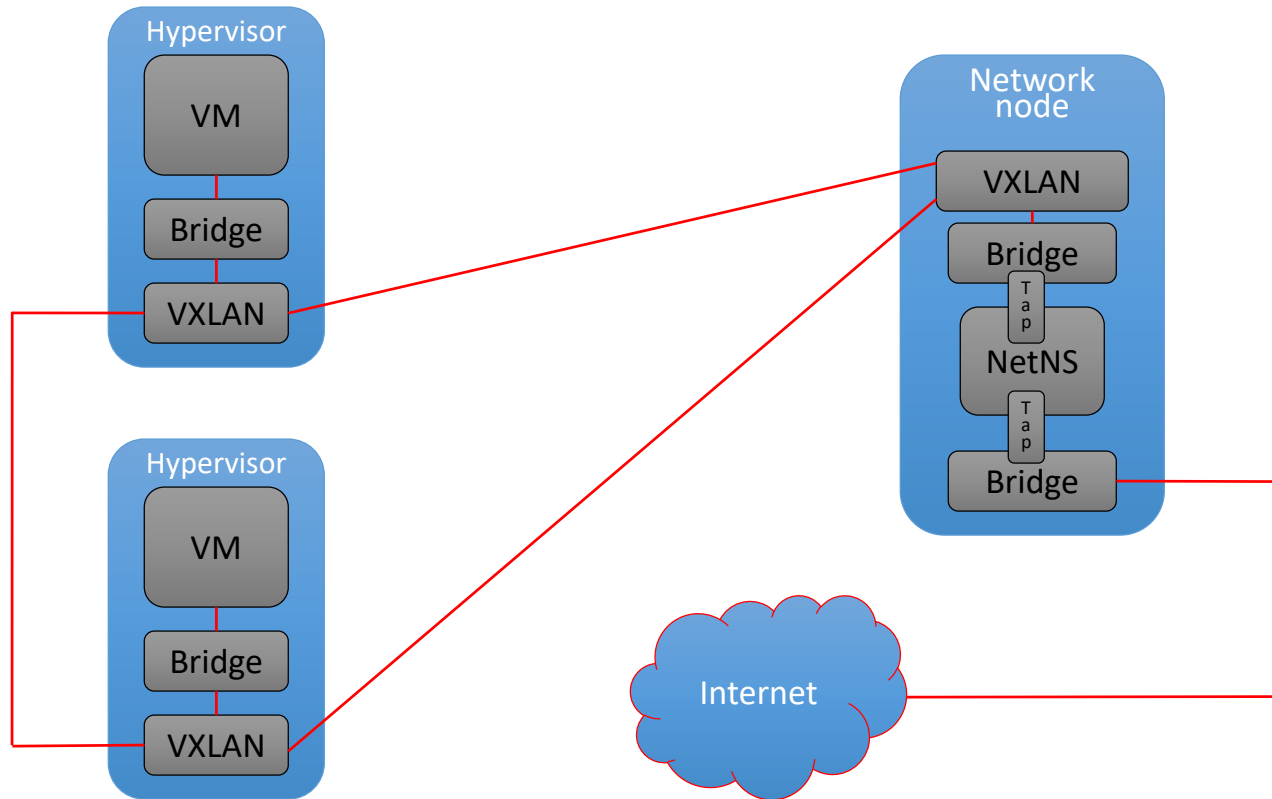
Components: Metadata Agent

- Proxies metadata requests from <http://169.254.169.254> to compute service via haproxy and DNAT rules in virtual router
- Configuration files
 - /etc/neutron/neutron.conf
 - /etc/neutron/metadata_agent.ini
- Runs on network node

Components: DHCP Agent

- Runs Dnsmasq in a network namespace to serve dhcp and caching dns requests
- Configuration files
 - /etc/neutron/neutron.conf
 - /etc/neutron/dhcp_agent.ini
- Runs on network node

Neutron Networking



Security Groups

- Set of iptables explicit allow rules (default disallow) applied to outside of an instance's interfaces
- Applied by linuxbridge agent
- The default group has a rule allowing all traffic in from any other instance with the same security group applied
- The default group allows all IPv4 and IPv6 traffic out

Virtual Routers

- In HA mode they run keepalived inside the network namespace for failover, faster than dead agent detection and rescheduling
- With OVS and Distributed Virtual Router traffic flow is asymmetrical, in the network node and out the compute
- One of two network namespaces used

Troubleshooting Methods

- Enter the namespace

```
ip netns exec qrouter-<router id> bash
```

```
ip netns exec qdhcp-<network id> bash
```

- Tcpdump

```
tcpdump -I <bridge name> -n
```

- Ip link list

```
ip -d link list
```

Example output snippet: “vxlan id 446 group 239.0.0.62 dev bond0”

Resources

- Admin Guide
<https://docs.openstack.org/neutron/latest/admin/>
- Deployment Guide
<https://docs.openstack.org/neutron/latest/install/>

Questions