



VMware NSX-T Data Center Plugin for OpenStack Neutron Release Notes

VMware NSX-T Data Center Plugin for OpenStack Neutron | Feb 2018

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- [Release Compatibility](#)
- [What's New in VMware NSX-T Data Center Plugin for OpenStack Neutron](#)
- [NSX-T OpenStack Neutron Plugin 2.4 Limitations](#)
- [Resolved Issues](#)
- [Known Issues](#)

Release Compatibility

- Compatible with OpenStack Rocky and OpenStack Queens
- Compatible with VIO 5.1, VIO 5.1.0.1, VIO 4.1.2.1 and RHOSP 13 (other vendor OpenStack versions might be added subsequently).

See the *VMware NSX OpenStack Plugin Installation & Configuration Guide* and *NSX-T Data Center Installation Guide* for more details on compatibility and system requirements.

What's New in VMware NSX-T Data Center Plugin for OpenStack Neutron

- Support of Rocky and Queens.
- Support of Management Plane Clustering.
The OpenStack Neutron Plugin takes advantage of the new ability to have a cluster of managers. It can consume the three managers REST API endpoints without an external VIP for additional performance and higher availability.
- Support of Barbican.
The OpenStack Neutron Plugin now supports Barbican. Barbican is a REST API designed for the secure storage, provisioning and management of secrets such as passwords, encryption keys and X.509 Certificates. This allows to manage certificate for the Load Balancer as a Service in order to do HTTPS termination. This is a feature currently supported in VIO environment only.

- Improvement of deployment by Red Hat OpenStack 13 Director, supporting automated deployment of NSX-T neutron plugin in RHOSP containerized control plane.

View Release Notes for previous versions:

- [NSX-T 2.3](#)
- [NSX-T 2.2](#)
- [NSX-T 2.1](#)
- [NSX-T 2.0](#)
- [NSX-T 1.1](#)

NSX-T OpenStack Neutron Plugin 2.4 Limitations

- A configured edge uplink profile “Transport VLAN” and deployed vlan network, when both have the same VLAN ID set, can have disruptive side-effects, and should not be configured this way. Any configured VLAN ID overlapping between “Transport VLAN” and deployed vlan network would cause the seen issues with MDProxy and DHCP, not just 0.
- Cannot add more than one subnet to network.
- Cannot add two T1 routers to same logical switch.
- Can associate a maximum of nine Security Groups per port. This limitation is due to the maximum tags/port in a platform, which is 15, and only nine are available for SG.
- Metadata only supports ports 3000-9000.
- IPv6 is not currently supported by the NSX-T OpenStack Neutron plugin.
- QoS currently supports "Shaping" and “DSCP Marking” (not "CoS Marking" nor “Minimum BW”) for ESXi and KVM.
- QoS is enforced for traffic leaving the hypervisor (not intra-hypervisor).
- FWaaS is not enforced for E/W traffic across downlink interfaces on the same Neutron router.
- Distributed Firewall is not enforced for workload on Enhanced DataPath logical switch.

Resolved Issues

- **Fixed Issue 2232265: On NSX-T Tier0 router deletion will fail with the following error message: Entity first_tier0_router(LogicalRouter/xxxxx) cannot be deleted as it is being referenced by entity(s): Neutron VPN service for T0 router xxxxx(IPSecVPNService/yyyyy)**
Cannot delete T0 router if it was attached to OpenStack VPN service, even if the service has now been deleted. This implies users need to perform one additional step to remove the Tier0 router.
- **Fixed Issue 2246682: Neutron will refuse to create subnets in the 100.64.0.0/16 range**
The range 100.64.0.0/16 cannot be used since it is used by default for NSX-T Transit Network for Tier-1 routers. Even if the operator changes this range in NSX-T, Neutron's behavior will not change.

The reserved range has now been made configurable.

- **Fixed Issue 2261710: neutron lbaas-loadbalancer-stats <lb_name> might fail with 500 response code**

Sometimes load balancing statistics cannot be retrieved. For some listener the statistics of the corresponding are simply not available, but the error causes a failure in retrieving any statistic for the Load Balancer.

This has been fixed by considering null statistics for NSX-T virtual server with no statistic info.

- **Fixed Issue 2290057: The firewall policy is removed, but the corresponding rules are still enforced**

Removing a policy from a firewall security group does not remove rules on NSX-T. The bug fix takes into account policy changes when determining if and where an update should be processed.

- **Fixed Issue 2291561: Rules expected to be enforced for traffic going through LB VIP are instead being ignored**

Users might expect to sure LB traffic with Edge firewall, but this will not work at all.

To reproduce this issue, create edge firewall rules that are supposed to apply to traffic coming from a LB VIP. For instance try and add a DENY rule for all traffic coming from the VIP. Traffic will still flow; the rule will never be hit.

NSX-T at the moment does not enforce Edge Firewall on LB VIPs.

- **Fixed Issue 2294190: FWaaS rules where both an ingress and a destination are specified will not be created**

The firewall will go in ERROR status. The log will report a detailed error explanation. The driver refuses to create ingress rules with explicit destination or egress rules with explicit source.

To reproduce, simply create an ingress rule with an explicit destination, an egress rule with an explicit source, or any rule with both.

Known Issues

- **FWaaS rules are not enforced as expected. Some rules that work correctly with the NSX-v driver or the reference implementation driver seem to be ignored by NSX-T Edge Firewall.**

Firewall behavior for NSX-T differs from NSX-v and reference implementation: fwaas is done after NAT for ingress, before NAT for egress.

Workaround: Ensure rules are defined in a way that consider the fact that egress rules are enforced before SNAT occurs, and ingress rules after DNAT occurred.

The following notes apply to both ALLOW and DENY rules.

Ingress FWaaS rules

Source behind NO-SNAT router

- The source IP should be the internal server IP or the internal subnet CIDR

Source behind SNAT router

- If the source server is associated with a floating IP, use floating IP address
- Otherwise use source router's gateway IP

External source

- Use actual source IP address or CIDR

Destination

- As NSX-T Edge firewall is enforced after NAT, use either internal server IP or internal subnet CIDR

Egress FWaaS rules

Source IP

- As NSX-T Edge firewall is enforced before NAT in this case, use either internal server IP or internal subnet CIDR

Destination IP

- External destination, use actual source IP or CIDR
- Destination behind NO-SNAT router, the destination IP should be the internal server IP or the internal subnet CIDR
- Destination behind SNAT router, the destination server must be exposed via a floating IP. That floating IP should be used as the destination IP for the FWaaS rule.

- **VM boots, correctly gets IP from the DHCP server, but cannot send/receive any traffic; the actual VM IP differs from the one reported by Neutron**

When DHCP relay is enabled spoofguard might block outbound traffic from VMs.

Workaround: Disable port security on every network.

- **Explicitly adding DFW rule for allowing traffic from the LB VIP has no effect**
OpenStack configures NSX-T Virtual Servers with SNAT automap mode. This has been necessary to satisfy the use case where the LB connection happens from a client located behind the same Tier-1 router as the target members.

In this mode the source IP for the traffic coming from the load balancer is not the VIP itself, but an address on the internal transit work. This does not create any problem to OpenStack integration.

Workarounds:

- 1) whitelist traffic into the security group.
- 2) Find on NSX-T the IP on the transit network the LB VS uses. Create a DFW rule that includes at least this address.
- 3) whitelist traffic from the internal subnet CIDR.

- **After setting the default pool for a listener, no traffic is received by the LB VIP.**

Updating default pool or a listener, even if allowed by Neutron-LBaas, is an action that is not implemented in the NSX-T. As a result, even if the pool on the NSX-T virtual server will be correctly updated, the NSX-T LBS will not be updated with the VS id.

Therefore if the VS is not already associated with a LBS, the association will not be created.

1) Remove the pool from the listener, or delete it.

2) Set the listener on the pool, or create a new pool setting the listener id.

Copyright © 2022 VMware, Inc. All rights reserved.