Overview

This chapter contains the following sections:

- Cisco Nexus 1000V for KVM and OpenStack, page 1
- Information About Port Profiles, page 2
- Live Policy Changes, page 2
- Atomic Inheritance, page 3
- Rollbacks to a Consistent Configuration, page 3
- Interface Quarantines, page 3
- VLAN Ranges for Trunking and Access Port Profiles, page 3

Cisco Nexus 1000V for KVM and OpenStack

The Cisco Nexus 1000V for KVM consists of two main components:

- Virtual Ethernet Module (VEM)—A software component that is deployed on each KVM host. Each VM on the host is connected to the VEM through virtual Ethernet (vEth) ports.
- Virtual Supervisor Module (VSM)—The Management component that controls multiple VEMs and helps in the definition of VM-focused network policies. It is deployed either as a virtual appliance on any KVM host or on the Cisco Cloud Services Platform appliance.

Each of these components is tightly integrated with the OpenStack environment:

- The VEM is a hypervisor-resident component and is tightly integrated with the KVM architecture.
- The VSM is integrated with OpenStack using the OpenStack Neutron Plug-in.
- The OpenStack Neutron API has been extended to include two additional user-defined resources:
  - Network profiles as logical groupings of network segments.

Note In Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.2), network profiles are created automatically for each network type. Network profile creation by administrators is not supported.

- Policy profiles group port policy information, including security.

Using OpenStack, you create VMs, networks, and subnets on the Cisco Nexus 1000V for KVM, by defining components such as the following:

- Tenants
- Network segments, such as VLANs, VLAN trunks, and VXLANs
- IP address pools (subnets)

Using the Cisco Nexus 1000V for KVM VSM, you create port profiles (called policy profiles in OpenStack), which define the port policy information, including security settings.

When a VM is deployed, a port profile is dynamically created on the Cisco Nexus 1000V for KVM for each unique combination of policy port profile and network segment. All other VMs deployed with the same policy to this network reuse this dynamic port profile.

Note You must consistently use OpenStack for all VM network and subnet configuration. If you use *both* OpenStack and the VSM to configure VM networks and subnets, the OpenStack and the VSM configurations can become out-of-sync and result in faulty or inoperable network deployments.

Information About Port Profiles

A port profile is a collection of interface-level configuration attributes that are combined to create a port classification on the OpenStack controller. Using port profiles allows you, as the system administrator, to configure a consistent network policy on the virtual Ethernet (vEthernet) and physical Ethernet interfaces across all of the hosts managed by the Cisco Nexus 1000V Virtual Supervisor Module (VSM) . Both Ethernet and vEthernet port profiles are created on the VSM and published to the VEMs. However, vEthernet port profiles are also pushed to the OpenStack controller.

Live Policy Changes

Port profiles are not static entities but dynamic policies that can change as network needs change. Changes to active port profiles are applied to each switch port that is using the profile, which simplifies the process of applying new network policies or changing an existing policy.

Atomic Inheritance

To maintain a consistent configuration among the interfaces in a port profile, the entire port profile configuration is applied to its member interfaces (this process is sometimes referred to as inheritance).

Rollbacks to a Consistent Configuration

When you update the configuration in a port profile, its member interfaces are also updated. If the configuration fails, the port profile and its member interfaces are rolled back to the last known good configuration for the port profile.

Interface Quarantines

Port profile interfaces are sectioned off and shut down when a port profile configuration is in error. This process is called an Interface Quarantine.

If you create a port profile with a command error, such as a private VLAN mapping error or service policy map error, and then attempt to apply this port profile to an interface, the interface shuts down. The error is not copied to the interface and a system message is generated with details of the error. In this case, you must correct the error in the port profile, return the interface to service, and apply the corrected port profile to the interface.

VLAN Ranges for Trunking and Access Port Profiles

You can configure VLANs only on Ethernet port profiles, not vEthernet policy profiles. Use the information in the following table while configuring trunking and access port profiles. In accordance with the IEEE 802.1Q standard, up to 4094 VLANs are supported.

Table 1: VLAN Ranges

VLAN Numbers	Range	Usage
1	Normal	Cisco default. You can use this VLAN, but you cannot modify or delete it.
2—1005	Normal	You can create, use, modify, and delete these VLANs.

VLAN Numbers	Range	Usage
1006—4094	Extended	You can create, name, and use these VLANs. You cannot change the following parameters: • The state is always active. • The VLAN is always enabled. You cannot shut down these VLANs.
3968—4047 and 4094	Internally allocated	These 80 VLANs, plus VLAN 4094, are allocated for internal device use. You cannot create, delete, or modify any VLANs within the block reserved for internal use.