Overview

This chapter contains the following sections:

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 kernel-based virtual machine (VM) 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 are logical groupings of network segments.
  - 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.

CDP

The Cisco Discovery Protocol (CDP) runs over the data link layer and is used to advertise information to all attached Cisco devices and to discover and view information about attached Cisco devices. CDP runs on all Cisco-manufactured equipment.

Domains

You must create a domain ID for Cisco Nexus 1000V. This process is part of the initial setup of the Cisco Nexus 1000V when you are installing the software. If you need to create a domain ID later, use the **saves-domain** command.

You can establish Layer 3 Control in your VSM domain, which means that your VSM is Layer 3 accessible and able to control hosts that reside in a separate Layer 2 network.

Configuration Management

The Cisco Nexus 1000V enables you to change the switch name, configure messages of the day, and display, save, and erase configuration files.

File Management

Using a single interface, you can manage the file system including:

- Flash memory file systems
- Network file systems (TFTP and FTP)
- Any other endpoint for reading or writing data (such as the running configuration)

User Management

You can identify the users who are currently connected to the device and send a message to either a single user or all users.

NTP

The Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows you to correlate events when you receive system logs and other time-specific events from multiple network devices.

SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that you can use to use to monitor and manage devices in a network.

NetFlow

NetFlow gives visibility into traffic that transits the virtual switch by characterizing IP traffic based on its source, destination, timing, and application information. You can use this information to assess network availability and performance, assist in meeting regulatory requirements (compliance), and help with troubleshooting.

You can also use the Cisco Network Analysis Module (NAM) to monitor NetFlow data sources.

System Messages

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to a terminal session, a log file, and syslog servers on remote systems. System message logging is based on RFC 3164.

For more information about the system message format and the messages that the device generates, see the *Cisco Nexus 1000V Series NX-OS System Messages Reference*.

Troubleshooting

Ping and trace route are among the available troubleshooting tools. For more information, see the *Cisco Nexus 1000V for KVM Troubleshooting Guide*.