Overview

This chapter contains the following sections:

Information About Cisco Nexus 1000VE

The Cisco Nexus 1000VE is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter, for the virtualization administrator. This solution offloads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy.

The Cisco Nexus 1000VE is compatible with any upstream physical access layer switch that is compliant with the Ethernet standard, including the Catalyst 6500 series switch, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000VE is compatible with any server hardware that is listed in the VMware Hardware Compatibility List (HCL).

Note We recommend that you monitor and install the patch files for the VMware ESXi host software.

Information About the Cisco Nexus 1000VE Virtual Supervisor Module

The Virtual Supervisor Module (VSM) is the control plane of the Cisco Nexus 1000VE. It is deployed as a virtual machine.

You can install the VSM in either a standalone or active/standby high-availability (HA) pair. We recommend that you install two VSMs in an active-standby configuration for high availability.

VSM and VSE collectively represent the Cisco Nexus 1000VE. Cisco VSE is a module that switches data traffic.

The VSM, along with the VSEs that it controls, performs the following functions for the Cisco Nexus 1000VE system:

- Configuration

- Management
- Monitoring
- Diagnostics
- Integration with VMware vCenter Server

The VSM uses an external network fabric to communicate with the VSEs. The VSM runs the control plane protocols and configures the state of each VSE, but it never forwards packets. The physical NICs on the VSE server are the uplinks to the external fabric. VSEs switch traffic between the local virtual Ethernet ports that are connected to the VM vNICs but do not switch traffic to other VSEs. Instead, a source VSE switches packets to the uplinks that the external fabric delivers to the target VSE.

A single Cisco Nexus 1000VE instance, including dual-redundant VSMs and managed VSEs, forms a switch domain. Each Cisco Nexus 1000VE domain within a VMware vCenter Server must be distinguished by a unique integer called the domain identifier.

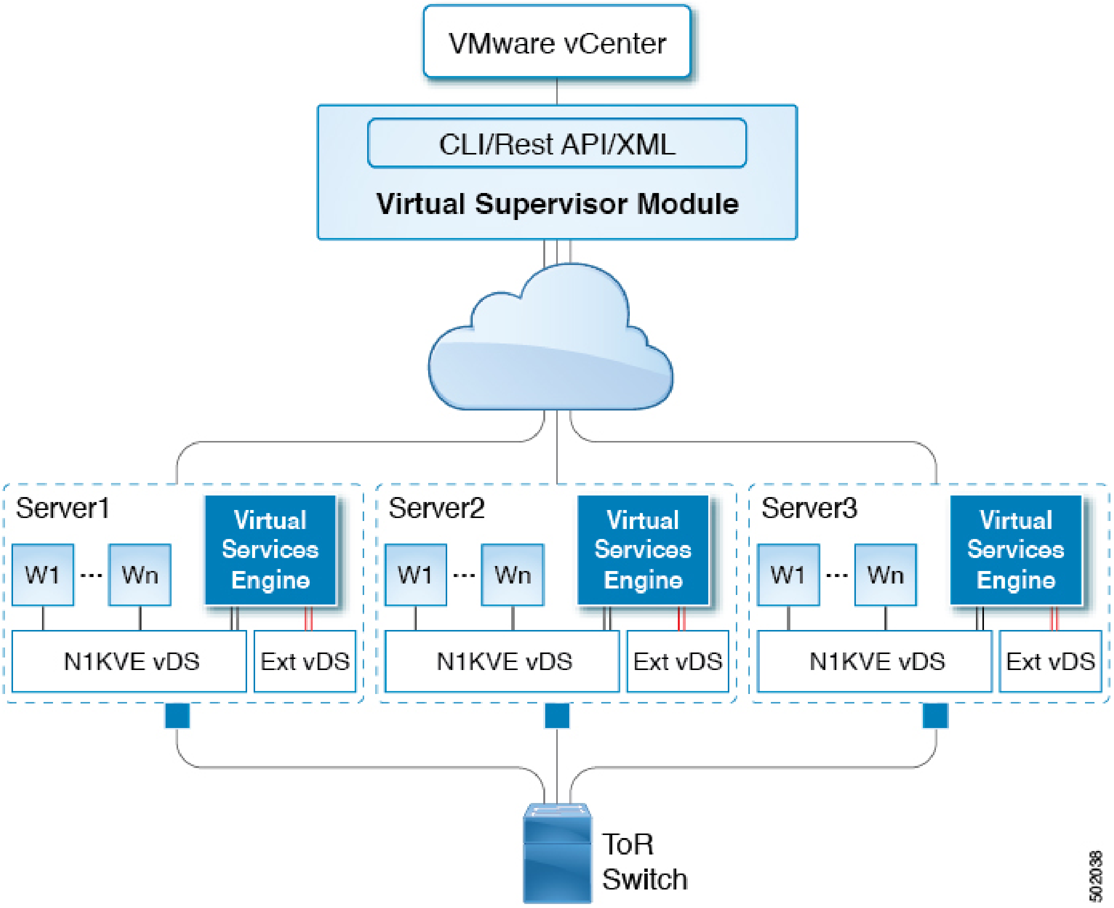
A single VSM can control up to 64 VSEs.

While using the VSG, it can control up to 32 VSES.

See the *Cisco Nexus 1000V Resource Availability Reference* for more information about scale limits.

The Cisco Nexus 1000VE architecture is shown in the following figure.

Figure 1: Cisco Nexus 1000VE Architecture



Information About the Virtual Service Engine

A VSE is deployed for each hypervisor instance and it performs the following functions::

- Advanced networking and security
- Switching between directly attached VMs
- Uplinking to the rest of the network

Note Only one version of the VSE can be installed on an ESXi host at any time.

Note Cisco Nexus 1000VE VSE does not support ESXi custom TCP/IP stack and control traffic through the custom TCP/IP stack.

In the Cisco Nexus 1000VE, the traffic is switched between VMs locally at each VSE instance. Each VSE also interconnects the local VM with the rest of the network through the upstream access-layer network switch (blade, top-of-rack, end-of-row, and so forth). The VSM runs the control plane protocols and configures the state of each VSE accordingly, but it never forwards packets.

In the Cisco Nexus 1000VE, the module slots 1 is for the primary VSM and module slot 2 is for the secondary VSM. Either module can act as active or standby. The first server or host is automatically assigned to module 3. The ports to which the virtual NIC interfaces connect are virtual ports on the Cisco Nexus 1000VE where they are assigned with a global number.

Information About VSM-to-VSE Communication

The VSM and the VSE can communicate over a Layer 3 network. These configurations are referred to as Layer 3 control modes.

Layer 3 Control Mode

Layer 3 control mode is the preferred method of communication between the VSM and the VSEs. In Layer 3 control mode, the VSEs can be in a different subnet than the VSM and from each other. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs.

Note You can configure IPv4 as transport mode for communication between VSE and VSM.

For more information about Layer 3 control mode, see the “Configuring the Domain” chapter in the *Cisco Nexus 1000VE System Management Configuration Guide*.

Information About System Port Profiles and System VLANs

System Port Profiles

System port profiles can establish and protect ports and VLANs that need to be configured before the VSE contacts the VSM.

When a server administrator adds a host to a DVS, its VSE must be able to contact the VSM. Because the ports and VLANs used for this communication are not yet in place, the VSM sends a minimal configuration, including the system port profiles and system VLANs, to vCenter Server, which then propagates it to the VSE.

When configuring a system port profile, you assign VLANs and designate them as system VLANs. The port profile becomes a system port profile and is included in the Cisco Nexus 1000VE opaque data. Interfaces that use the system port profile, which are members of one of the defined system VLANs, are automatically enabled and forward traffic when the VMware ESX starts even if the VSE does not have communication with the VSM. The critical host functions are enabled even if the VMware ESX host starts and cannot communicate with the VSM.

Caution VMkernel connectivity can be lost if you do not configure the relevant VLANs as system VLANs.

System VLANs

You must define a system VLAN in both the Ethernet and vEthernet port profiles to automatically enable a specific virtual interface to forward traffic outside the ESX host. If the system VLAN is configured only on the port profile for the virtual interface, the traffic is not forwarded outside the host. Conversely, if the system VLAN is configured only on the Ethernet port profile, the VMware VMkernel interface that needs that VLAN is not enabled by default and does not forward traffic.

The following ports must use system VLANs:

- Control and packet VLANs in the uplinks that communicate with the VSM.
- The Management VLAN in the uplinks and port profiles (that is, the Ethernet and vEthernet ports) and VMware kernel NICs used for VMware vCenter Server connectivity, Secure Shell (SSH), or Telnet connections.
- The VLAN that is used for remote storage access (iSCSI or NFS).

  Note We recommend this to configure vmknics for management, NFS/iSCSI, and vMotion on the external VDS instead of the Nexus 1000VE.

Caution You must use system VLANs sparingly and only as described in this section. Only 32 system port profiles are supported.

After a system port profile has been applied to one or more ports, you can add more system VLANs, but you can only delete a system VLAN after you remove the port profile from service. This action prevents you from accidentally deleting a critical VLAN, such as a host management VLAN or a VSM storage VLAN.

Note One VLAN can be a system VLAN on one port and a regular VLAN on another port in the same ESX host.

Installation Overview

Information About Installing the Cisco Nexus 1000VE Manually

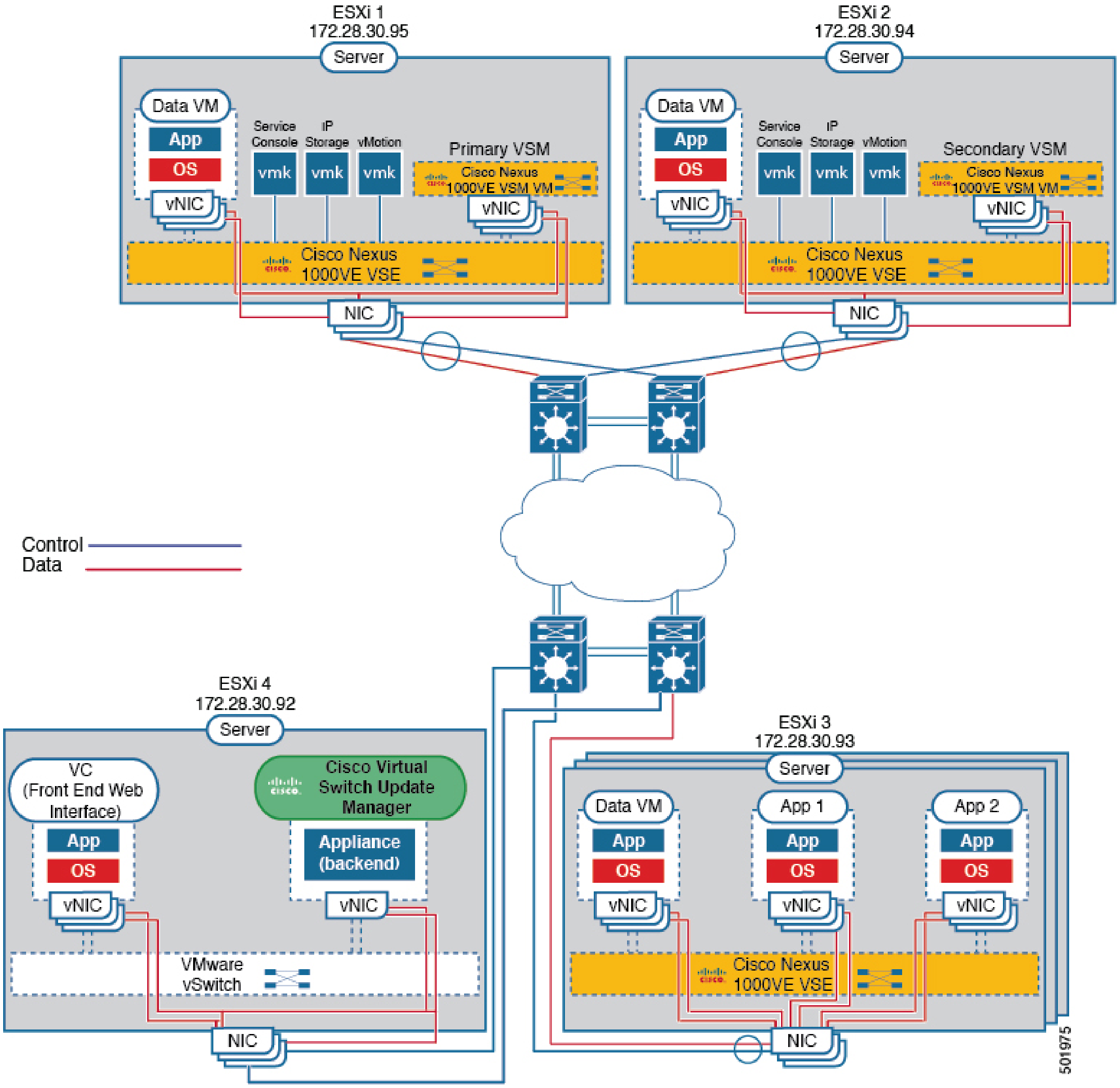
When you install the Cisco Nexus 1000VE manually, you download and install all of the necessary software. This installation method gives you the option of deploying Layer 3 connectivity between the VSM and VSEs. Layer 3 connectivity is the preferred method. For an example of the Layer 3 installation topology, see Topology for Layer 3 Control Mode, on page 6.

Recommended Topologies

Topology for Layer 3 Control Mode

Layer 3 control mode is the preferred method of communication between the VSM and VSEs. You can configure IPv4 addressing for Layer 3 control mode. This figure shows an example of a Layer 3 control mode topology (using IPv4 addressing) where redundant VSM VMs are installed. The software for the primary VSM is installed on ESXi 1, and the software for the secondary VSM is installed on ESXi 2.

Figure 2: Layer 3 Control Mode Topology Diagram


ESXi 1
172.28.30.95
Server
Data VM
App
OS
vNIC
Service Console
IP Storage
vMotion
vmk
vmk
vmk
Primary VSM
Cisco Nexus 1000VE VSM VM
vNIC
Cisco Nexus 1000VE VSE
NIC
ESXi 2
172.28.30.94
Server
Data VM
App
OS
vNIC
Service Console
IP Storage
vMotion
vmk
vmk
vmk
Secondary VSM
Cisco Nexus 1000VE VSM VM
vNIC
Cisco Nexus 1000VE VSE
NIC
Control
Data
ESXi 4
172.28.30.92
Server
VC (Front End Web Interface)
App
OS
vNIC
Cisco Virtual Switch Update Manager
Appliance (backend)
vNIC
VMware vSwitch
NIC
ESXi 3
172.28.30.93
Server
Data VM
App
OS
vNIC
App 1
App
OS
vNIC
App 2
App
OS
vNIC
Cisco Nexus 1000VE VSE
NIC
501975