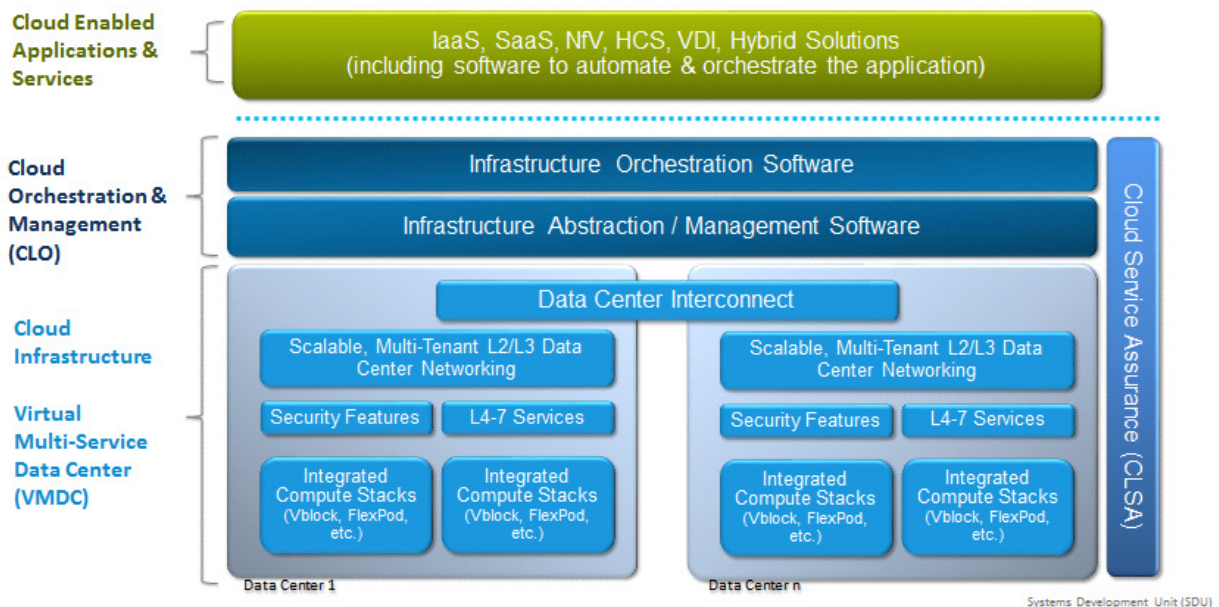# VMDC Architecture Overview

The VMDC solution provides design and implementation guidance for enterprises deploying private cloud services, and for service providers (SPs) building virtual private and public cloud services. The Cisco VMDC solution integrates various Cisco and third-party products that are part of the cloud computing ecosystem. Cisco's VMDC system defines an end-to-end architecture, which an organization may reference for the migration or build out of virtualized, multiservice data centers for new cloud-based service models such as Infrastructure as a Service (IaaS). Figure 1-1 shows the basic architectural framework for VMDC. The solution scope includes integrated compute, network, and storage components, a functional layered infrastructure, and service definitions for intra-DC, inter-DC, and automation and service assurance models.

Figure 1-1 *Basic VMDC Architecture Framework*

Refer to the Cisco Virtualized Multiservice Data Center site for additional details on VMDC.

Validated VMDC architectural systems include a range of traditional hierarchical classic Ethernet models and a variety of Clos FabricPath-based models. Although this document focuses on inserting Hyper-V into a specific FabricPath-based topology model called a "Typical Data Center" design (for FabricPath), deployment considerations described in this document generally apply to all validated VMDC architectures.

VMDC "Typical Data Center" Design for FabricPath

A "Typical Data Center" design is a 2-tier FabricPath design, as shown in Figure 1-2. All VMDC architectures are built around modular building blocks called pods. Each pod uses a localized services attachment model. In a pod, Virtual Port Channels (vPCs) handle Layer 2 (L2) switching between the Edge devices and the compute. This provides an active-active environment that does not depend on Spanning Tree Protocol (STP) and converges quickly after failures. Figure 1-2 shows a VMDC pod using FabricPath between the Edge and Aggregation/Spine devices. In previously VMDC releases, vPCs were also used here as well. FabricPath replaces these vPCs.

Figure 1-2   VMDC 3.0.1 Typical Data Center Design
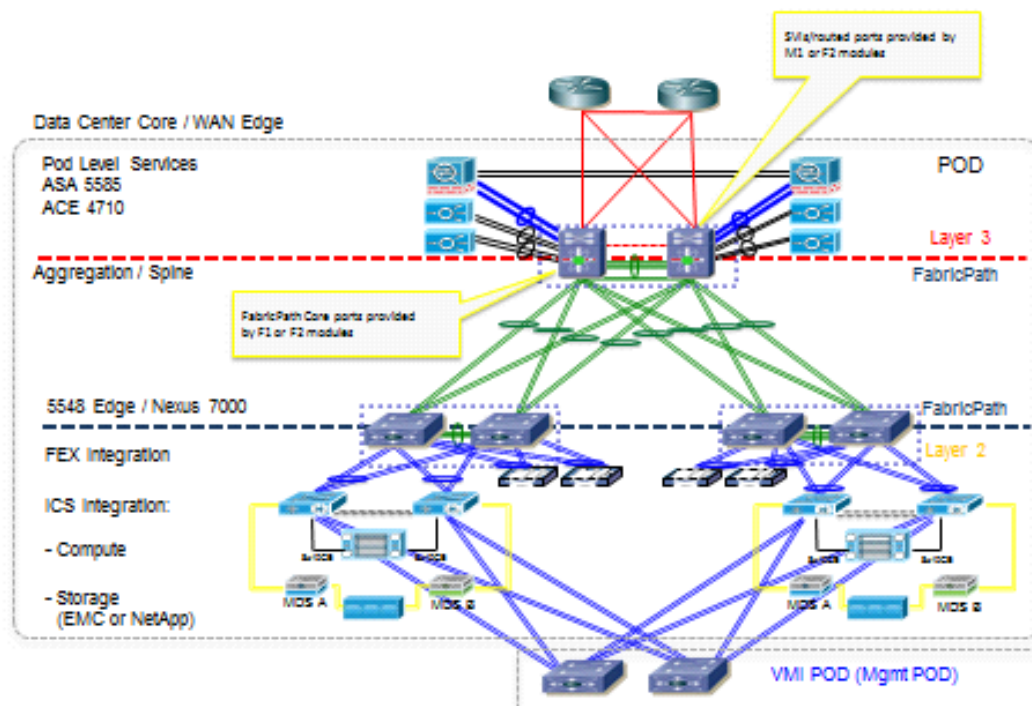
Hyper-V is used to implement hypervisor-based virtualization and enable the creation of VMs on physical servers. Hyper-V logically abstracts the server environment in terms of CPU, memory, and network touch points into multiple virtual software containers. In previous VMDC offerings, VMware's hypervisor was used.

The Cisco Nexus 1000V Switch for Microsoft Hyper-V L2 switch extends Cisco networking benefits to Microsoft Windows Server 2012 Hyper-V deployments. The Nexus 1000V Switch for Microsoft Hyper-V distributed virtual switching platform provides advanced features and is tightly integrated with the Hyper-V ecosystem.

Table 1-1 summarizes the capabilities and benefits of Cisco Nexus 1000V Switch for Microsoft Hyper-V switch when used in conjunction with Microsoft Hyper-V.

Table 1-1   Nexus 1000V Switch for Microsoft Hyper-V Benefits

Capabilities	Features	Operational Benefits
Advanced Switching	Private VLANs, Quality of Service (QoS), access control lists (ACLs), portsecurity, and Cisco vPath	Get granular control of virtual machine-to-virtual machine interaction.
Security	Dynamic Host Configuration Protocol (DHCP) Snooping, Dynamic Address Resolution Protocol Inspection, and IP Source Guard	Reduce common security threats in data center environments.
Monitoring	NetFlow, packet statistics, Switched Port Analyzer (SPAN), and Encapsulated Remote SPAN	Gain visibility into virtual machine-to-virtual machine traffic to reduce troubleshooting time.
Manageability	Simple Network Management Protocol, NetConf, syslog, and other troubleshooting command-line interfaces	Use existing network management tools to manage physical and virtual environments.
	Similar RBAC concept like physical switches – TACACS+, RADIUS	Centralize Access Control Management across physical and virtual switches

VMDC Tenancy Architecture

The Expanded Palladium tenancy model provides flexibility in server VLANs placement in different zones, public and private. This model was further refined in VMDC 3.0.1 for the private cloud use case. Public virtual routing and forwarding instances (VRFs) are combined into one common public zone. The model assumes there is an "infrastructure" demilitarized zone (DMZ) above the common public zone, so there is no need for a separate protected front-end zone (and VRF) to accommodate per-tenant DMZs. This is a norm in the Enterprise environment. The public zone is shared across multiple user organizations or "tenants" (infrastructure zone) and provides access to the public Internet and serves as a shared resource zone. Figure 1-3 shows a simplified, high-level version of this model.

Figure 1-3   Expanded Palladium Tenancy Model
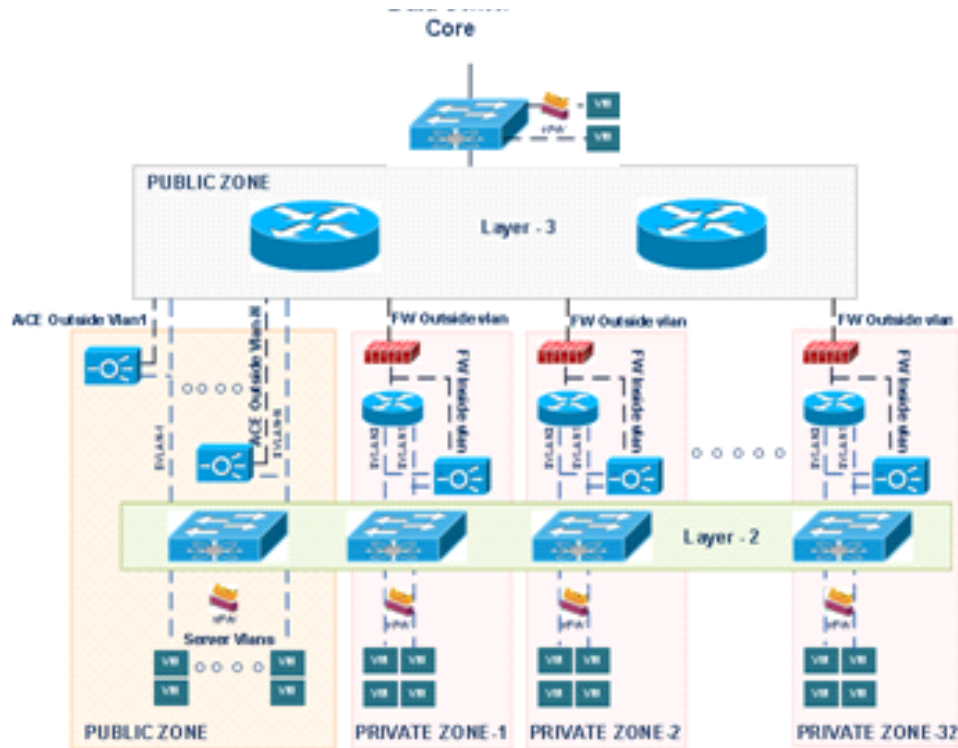
Microsoft Private Cloud Compared to VMware vSphere

Microsoft and VMware are both leading providers of cloud technologies. While their base technologies differ, their models exhibit the common functional components shown in Table 1-2.

Table 1-2   Microsoft vs. VMWare Cloud Technologies

Cloud Technology	Microsoft	VMware	Notes
Hypervisor	Hyper-V	ESXi	Both Type-1 Hypervisor
VM Management	SCVMM	vCenter Server	
Self-Service	App Controller	vCloud Director	
Monitoring	SCOM	vCenter Operations Management Suite	
Protection	Data Protection Manager	vSphere Data Protection	
Service Management	Service Manager	vCloud Automation Center	
Automation	Orchestrator	vCenter Orchestrator	

However, as might be expected, Microsoft and VMware terminology differs. Figure 1-4 highlights key terms in the Microsoft and VMware hypervisor ecosystems.

Figure 1-4   *Hypervisor Terminology Comparison*

VMware ESX	Microsoft Hyper-V
vMotion	Live Migration
Virtual Distr. Switch (VDS)	Logical Switch
Folder/DataCenter	Host Group
vmknic	Host VNIC
Port-group	Virtual PP + VM Networks
Distributed Resource Scheduling (DRS)	Dynamic Optimization
Distrib. Power Mgmt (DPM)	Power Management
vCenter, vCloud Director	SCVMM, Orchestrator
Site Recovery Manager	Hyper-V Replica
Update Manager (VUM)	Update Services (WSUS)
Virtual Machine Disk (VMDK)	Virtual Hard Disk (VHDX)
VXLAN	NVGRE

Microsoft and VMware also have different licensing practices, as summarized in Table 1-3.

Table 1-3   *Microsoft and VMware Licensing*

Cloud Technology	Microsoft	VMware	License Required?
Hypervisor	Free	Free	**Note**: The Hypervisors are free to install. However, each VM will require a per vCPU license
VM Management	Included with System Center	Sold Separately	Y
Self-Service	Included with System Center	Part of vCloud Suite	Y
Monitoring	Included with System Center	Included with vSphere	Y
Protection	Included with System Center	Included with vSphere	Y
Service Management	Included with System Center	Part of vCloud Suite	Y
Automation	Included with System Center	Packaged with vCenter Server	Y

vSphere Editions

There are three editions of VMware vSphere: Standard, Enterprise, and Enterprise Plus. To support VM management, each edition requires the purchase of a vCenter Server. For Nexus 1000V Switch for Microsoft Hyper-V support, an Enterprise Plus license is also required.

Refer to the VMware vSphere with Operations Management website for additional details.

Note   If Self-Service and Service Management are required, the user should consider purchasing the vCloud Suite, which includes a license for Enterprise Plus.

Microsoft Private Cloud Editions

Microsoft Private Cloud provides a Standard and a Datacenter Edition. The Standard Edition has a limitation on the number of vCPU and supported VMs, while the Datacenter Edition has unlimited support. The Nexus 1000V Switch for Microsoft Hyper-V is supported in both editions.

Refer to the Cisco Nexus 1000V Switch for Microsoft Hyper-V website for additional details on key benefits, features, and capabilities of Nexus 1000V with Microsoft Hyper-V.

Refer to the Microsoft Private Cloud website for additional details on key benefits, success stories, and how to evaluate or purchase Microsoft Hyper-V.

Refer to the Microsoft Private Cloud whitepaper for a comparative look at functionality, benefits, and economics.

Refer to VMware vSphere 5 vs. Microsoft Hyper-V 2012 for competitive performance results.

Interoperability

Both Microsoft and VMware can now manage multi-hypervisor environments.

Refer to the VMware vCenter Multi-Hypervisor Manager Documentation site to download the VMware vCenter Multi-Hypervisor Manager. Documentation for this plugin is also available on the webpage.

Microsoft System Center 2012 and SCVMM can manage multi-hypervisor environments. Refer to Managing VMware Infrastructure in VMM site for additional guidance.

VMDC Test Environment

Microsoft Hyper-V and Nexus 1000V Switch for Microsoft Hyper-V were tested in a VMDC 3.0.1 infrastructure. The system under test also leveraged the VMDC Virtual Management Infrastructure (VMI) for deploying the Nexus 1000V Switch for Microsoft Hyper-V Virtualized Switch Module (VSM).

Figure 1-5 shows how the Microsoft Hyper-V compute environment connects into the VMDC network infrastructure, VMI, and storage area network (SAN).
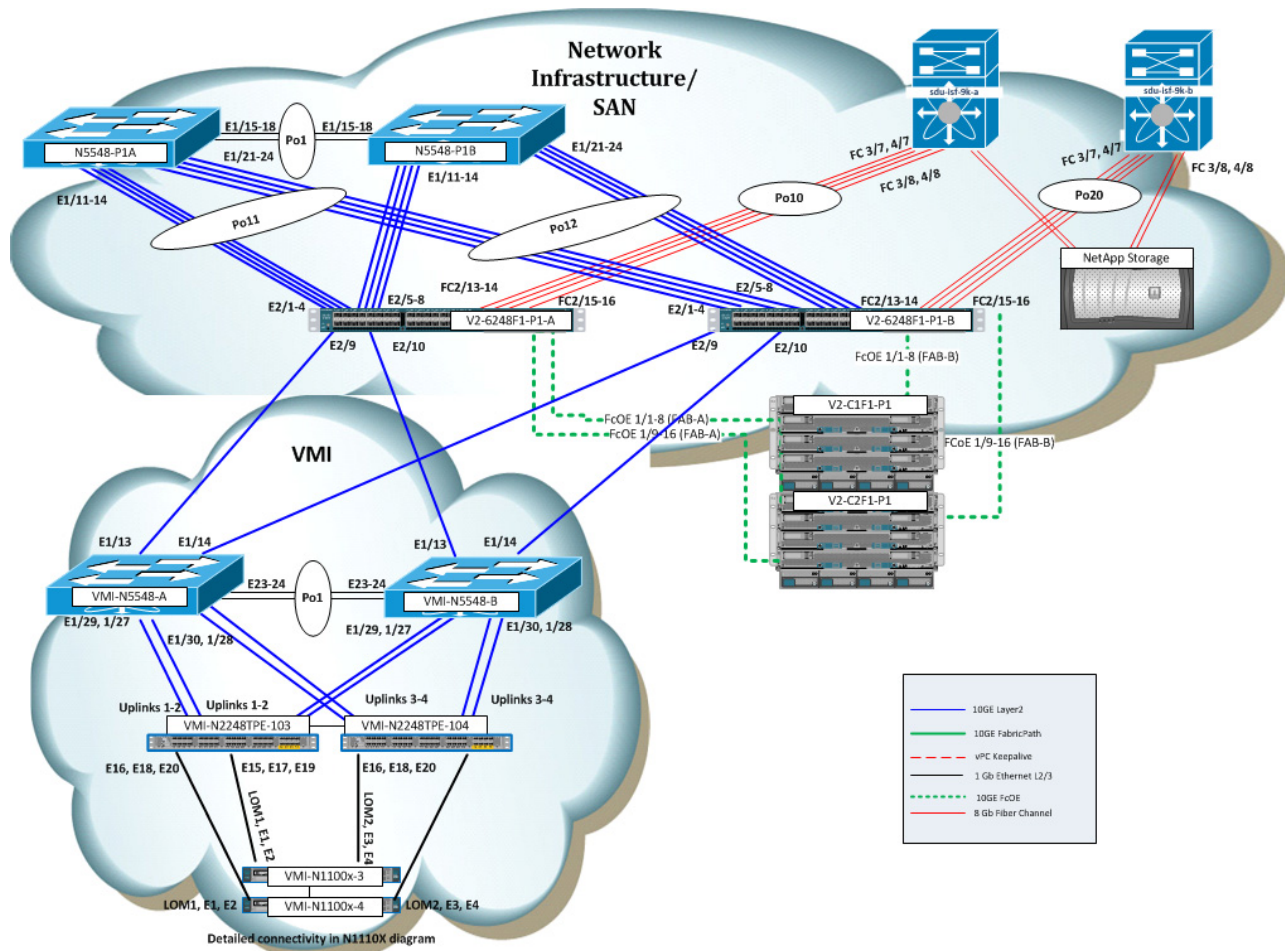
Figure 1-5   VMDC Test Environment

Table 1-4 lists the system hardware components and their associated software versions.

Table 1-4   Hardware Components and Associated Software Versions

Component	Typical VMDC Topology Software Version
Nexus 7000 (Aggregation-edge/Access-Edge/Core)	6.1.3
Nexus 5500 (Access-edge) w N2K-2232 and N2K-2248 FEX	5.2.1.N1.3
Catalyst 6500 (DSN and VSS)	12.2(33)SXJ3
ASA SM (In Extended Topology)	8.5(1)
ACE 30 (In Extended Topology)	A5.2.2
Unified Computing System	2.1.1(e)
Nexus 1000V Switch for Microsoft Hyper-V	5.2.1.SM1.5.1
1110 VSA	4.2(1)SP1(5.1a)
UCS Host OS	Windows Server 2012

Table 1-4   Hardware Components and Associated Software Versions (continued)

Component	Typical VMDC Topology Software Version
Virtual Machine Guest Operating System	CentOS 6.4
System Center Virtual Machine Manager	Windows Server 2012 UR2 Version 3.1.6020.0