Microsoft Hyper-V and Nexus 1000V Switch for Microsoft Hyper-V within a VMDC Architecture

August 23, 2013

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft Hyper-V and Nexus 1000V Switch for Microsoft Hyper-V within a VMDC Architecture
© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface iii

Document Goal iv

Audience iv

CHAPTER 1 **VMDC Architecture Overview** 1-1

VMDC "Typical Data Center" Design for FabricPath 1-2

VMDC Tenancy Architecture 1-3

Microsoft Private Cloud Compared to VMware vSphere 1-4

vSphere Editions 1-5

Microsoft Private Cloud Editions 1-6

Interoperability 1-6

VMDC Test Environment 1-6

CHAPTER 2 **Microsoft Private Cloud Implementation** 2-1

SAN Implementation 2-1

Boot from SAN Procedures 2-2

Deployment Guidelines 2-4

Microsoft Windows Server 2012 and Hyper-V Implementation 2-5

Microsoft Windows Server 2012 Installation 2-6

Microsoft Hyper-V Installation 2-10

SQL Server 2012 Installation 2-14

Deployment Guidelines 2-16

Microsoft System Center 2012 2-16

Deployment Guidelines 2-18

Virtual Switch Module Installation on Nexus 1110 2-19

Deployment Guidelines 2-19

CHAPTER 3 **Nexus 1000V Switch for Microsoft Hyper-V Configuration** 3-1

Network and Tenants Under Test 3-1

Nexus 1000V Switch for Microsoft Hyper-V VSM CLI Configuration 3-2

Nexus 1000V Part 2: SCVMM Configuration 3-7

Deployment Guidelines 3-39

Adding VMs to Nexus V Switch for Hyper-V Logical Switch 3-40

Deployment Guidelines 3-43

CHAPTER 4 **SCOM 2012 with UCS Management Pack 4-1**

Installation and Configuration 4-1

Deployment Guidelines 4-1

Cisco UCS Management Pack for SCOM 4-2

Monitors and Alerts 4-3

Summary 4-5

Preface

Compute consolidation through virtualization has been a consistent factor in data center trends over the last decade. Systems evolved from separate compute, network, and storage administrative silos to converged infrastructures and operational domains, and from traditional top-down network management and hierarchical infrastructure models, to newer models incorporating centralized controllers and increasingly virtualized, software-defined infrastructures.

Capex savings achieved by leveraging under utilized CPU and memory resources are a key driver of server virtualization. For many years, VMware has led the market for compute virtualization, but in recent years a more frequently encountered theme is that of hypervisor commoditization, as hypervisors from Microsoft, Citrix, and even open source projects have evolved to match, or in some cases exceed, VMware capabilities. As function and feature gaps narrow, some vendors have significantly lowered licensing costs to further hasten reevaluation of solution cost/benefit ratios, particularly for entry point use cases.

A key consideration for those virtualizing Windows environments is that there is no licensing for the Microsoft Hyper-V hypervisor. Microsoft offers Hyper-V in a free standalone version, or bundled into its Windows Server 2012 license. These advances are great news for customers, who now have more choices for virtualization solutions. Customers can select the virtualization environment which best meets their needs, in terms of cost, scale, performance, and application requirements.

The news for customers who adopt the Cisco Virtualized Multiservice Data Center (VMDC) reference model in their data centers is that a recent code release (Release 5.2(1)SM1(5.1)), enables the Nexus 1000V Switch for Microsoft Hyper-V to support advanced switching for Hyper-V virtual machines (VMs), along with Systems Center Virtual Machine Manager (SCVMM) integration. The networking benefits of the Nexus 1000V Switch for Microsoft Hyper-V were previously available only in vSphere environments (per-VM visibility, granular QoS, security policies, segmentation, and vPath service chaining for virtualized services such as Virtual Security Gateway), are now also available in the Windows Server 2012 environments.

This consistent operational model enables customers to leverage preferred management solutions. As noted, the Nexus 1000V Switch for Microsoft Hyper-V now offers SCVMM integration; for those who rely on Systems Center Operations Manager (SCOM), Cisco partnered with Jalasoft to develop an SCOM plug-in. Finally, for those who have Powershell expertise and prefer to use it for simple “CRUD” (create, update, delete) operations, the Nexus 1000V Switch for Microsoft Hyper-V offers RESTful APIs.

The Nexus 1000V Switch for Microsoft Hyper-V and Cisco VM Fabric Extender (VM-FEX) bring VM visibility and policy granularity to the virtualized compute environment as the “missing link” for service assurance in the architecture that VMDC addresses: highly consolidated, highly virtualized yet highly secure, multi-service public or private cloud data centers. This represents a significant step toward hypervisor-agnosticism and enhanced customer options, while maintaining key architectural advantages.

Document Goal

This document presents a “first look” at inserting SCVMM and Hyper-V-based compute resources into the compute tier of the VMDC reference architecture. We highlight differences from vSphere in terms of networking constructs, including policy profile implications and “tenancy.”

The following areas are addressed:

- **VMDC Architecture Overview**—VMDC architectural components and framework
- **Implementation Guidance**—on deploying Nexus 1000V Switch for Microsoft Hyper-V and Hyper-V in a VMDC environment
- **Management**—Management tools for monitoring (SCOM) Hyper-V

Audience

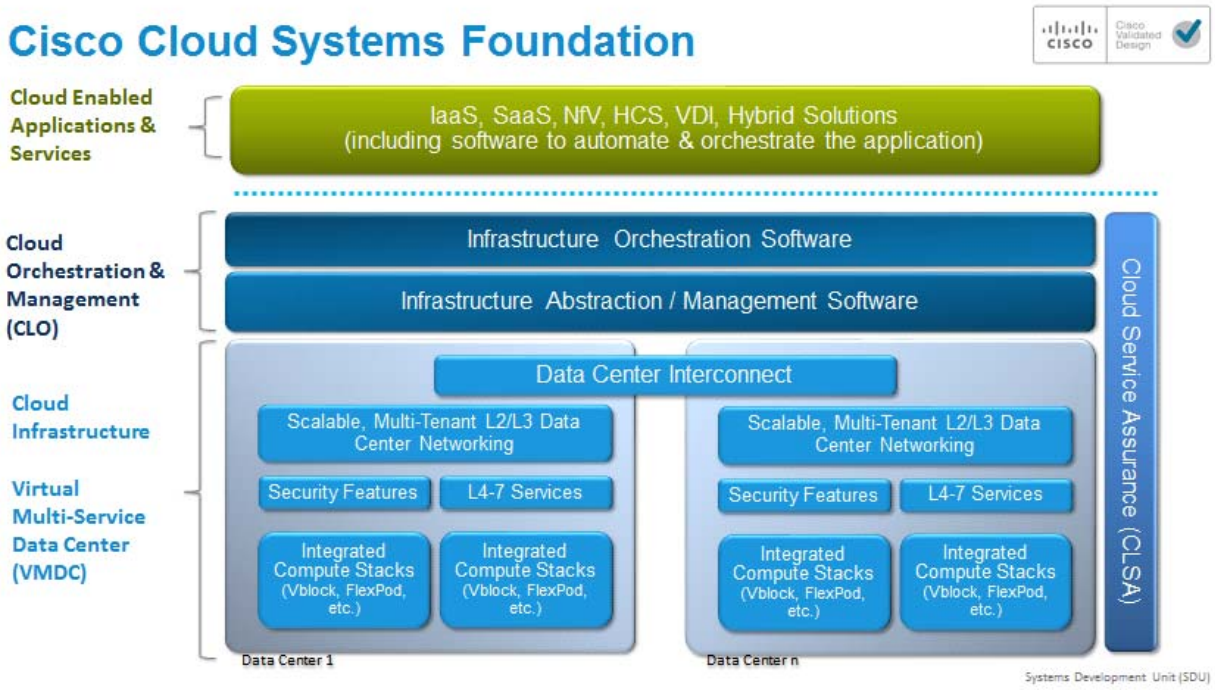
The target audience for this document includes sales engineers, field consultants, professional services, IT managers, Cisco channel partner engineering staff, and customers who have need cloud-ready data centers or have an existing VMDC implementation, and are considering Hyper-V based compute resources.

CHAPTER 1

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



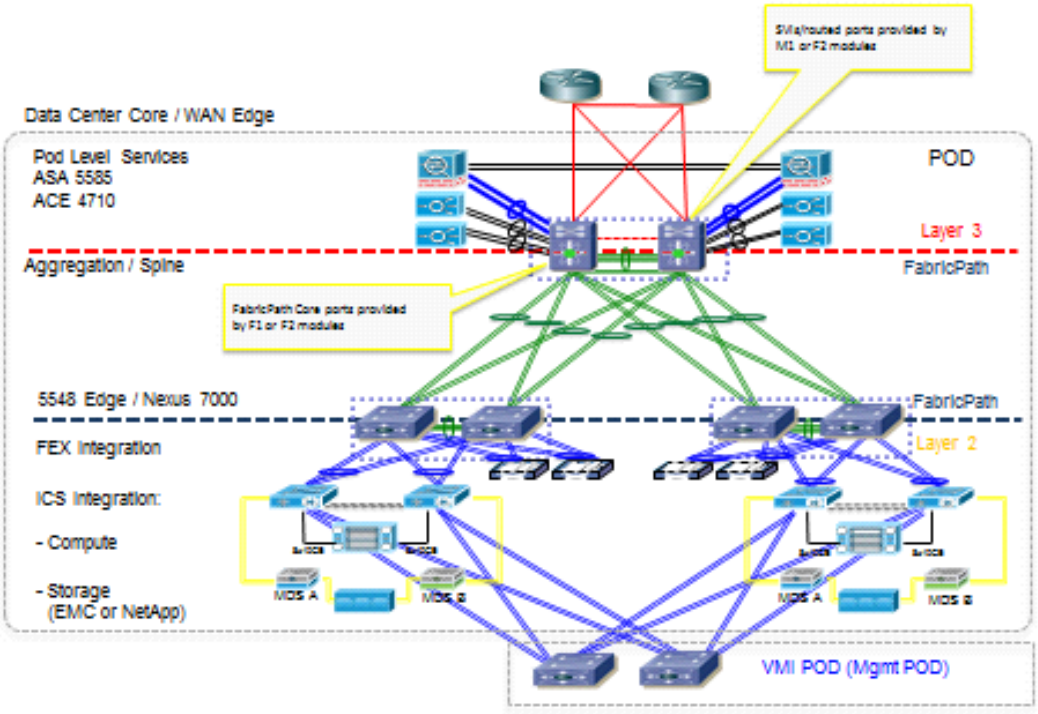
Refer to the Cisco Virtualized Multiservice Data Center site for additional details on VMDC.

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.

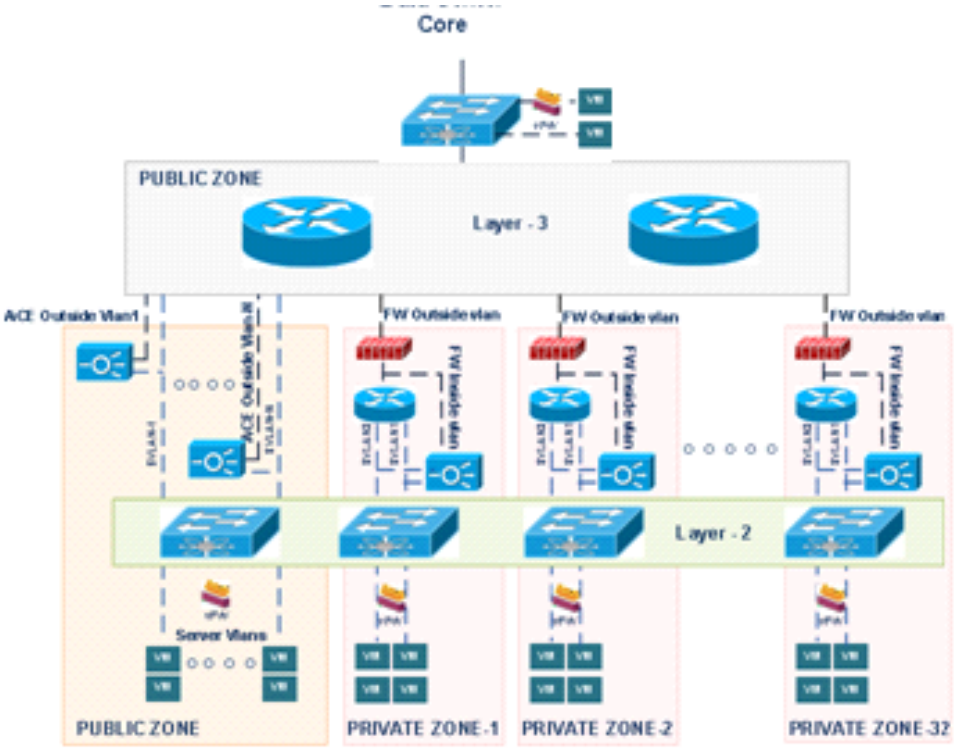
Table 1-1 Nexus 1000V Switch for Microsoft Hyper-V Benefits

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 Similar RBAC concept like physical switches – TACACS+, RADIUS	Use existing network management tools to manage physical and virtual environments. 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

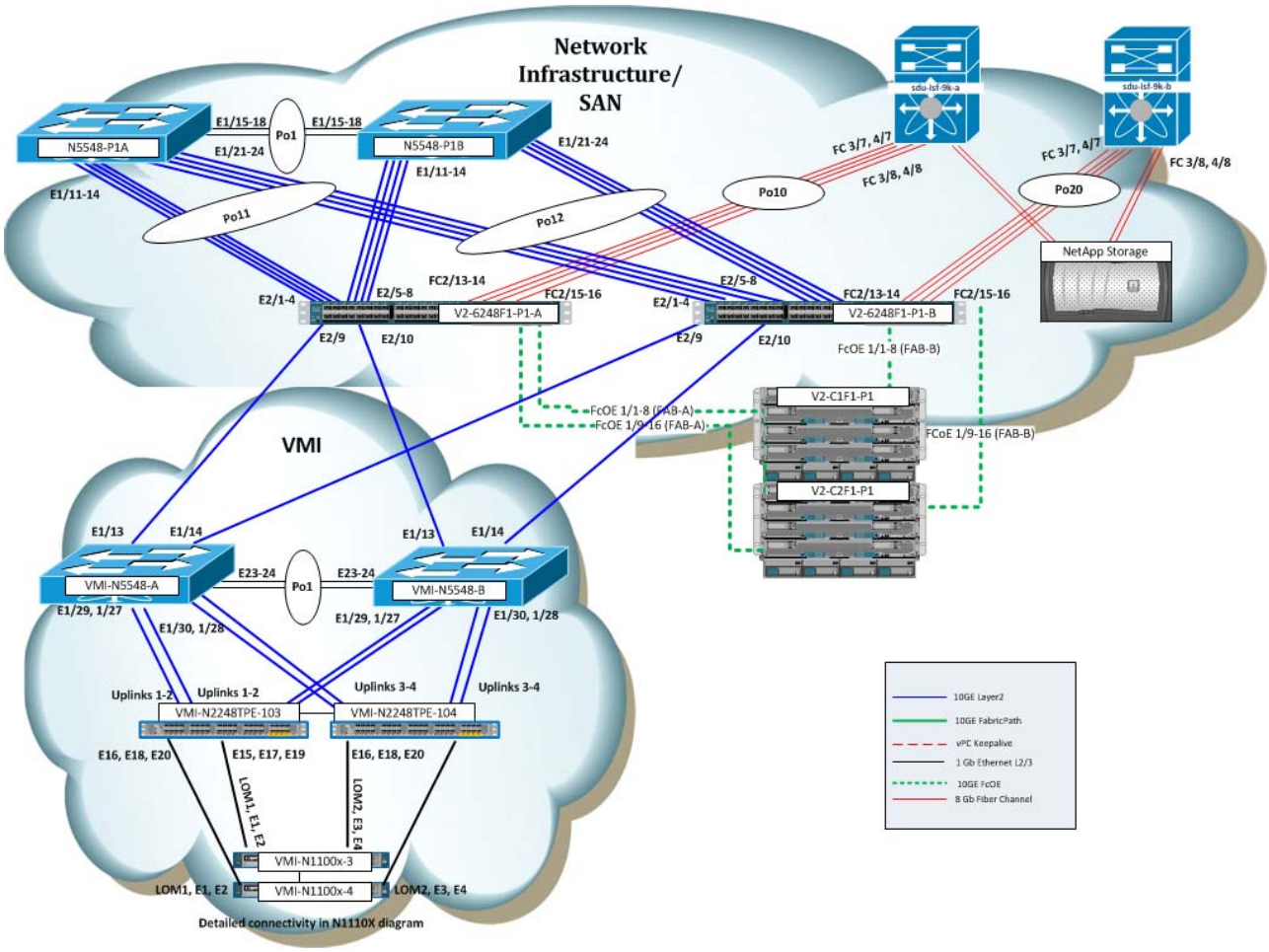


Table 1-4 lists the system hardware components and their associated software versions.

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

CHAPTER 2

Microsoft Private Cloud Implementation

In this section, we explore the implementation of a Microsoft Private Cloud solution through integrating the Microsoft Cloud OS into UCS. UCS is a computing systems comprising computing hardware, compute switching fabric, and virtualization and management software. These resources are integrated into a cohesive system that can be managed as an entity.

This provides unique benefits in the data center, such as:

- Hardware virtualization for streamlined deployment
- Ease of Cabling
- Single point of management for the compute resources (including blades, chassis and compute switching fabric)
- High Availability (including 1:N redundancy if desired)

Compute resources in the System Under Test included:

- 2 Cisco UCS 5108 Chassis
- 2 Cisco UCS 2208XP IOMs per chassis
- 2 Cisco UCS B200 M2 Blade Series Serves per chassis
- 2 Cisco UCS 6248UP Fabric Interconnects

The Cloud OS involves the simultaneous operation of several enterprise technologies including:

- UCS SAN Booting
- Windows Server 2012
- SQL Server 2012
- System Center 2012

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

Refer to the Microsoft Private Cloud-Making it Real white paper to learn more about Microsoft's strategic and technical differentiation.

SAN Implementation

The B200 M2 Series server blades in UCS are configured to boot from SAN. UCS has two Fibre Channel port channels that connect Fabric A and Fabric B to two MDS switches. The MDS switches connect to a NetApp storage device.

Details on the Service Profile creation for a server Hyper-V on UCS are found Figure 29 of the Deployment Guide.

Boot from SAN Procedures

Before starting, review the Common Errors during Windows SAN Boot Install on NetApp Storage Cisco internal document for lessons learned about the Windows SAN boot install.

Step 1 Shutdown all but one path to the boot logical unit number (LUN)

Microsoft supports only one path to the boot LUN when installing the OS. The Fibre Channel port channel (FC Po10) that connects to the MDS switches was disabled in UCS Manager (UCSM). All but one member of the second Fibre Channel port channel (FC Po20) was disabled.

Step 2 Map to fiber over Ethernet network interface card (fNIC) drivers and ISO image (Optional)

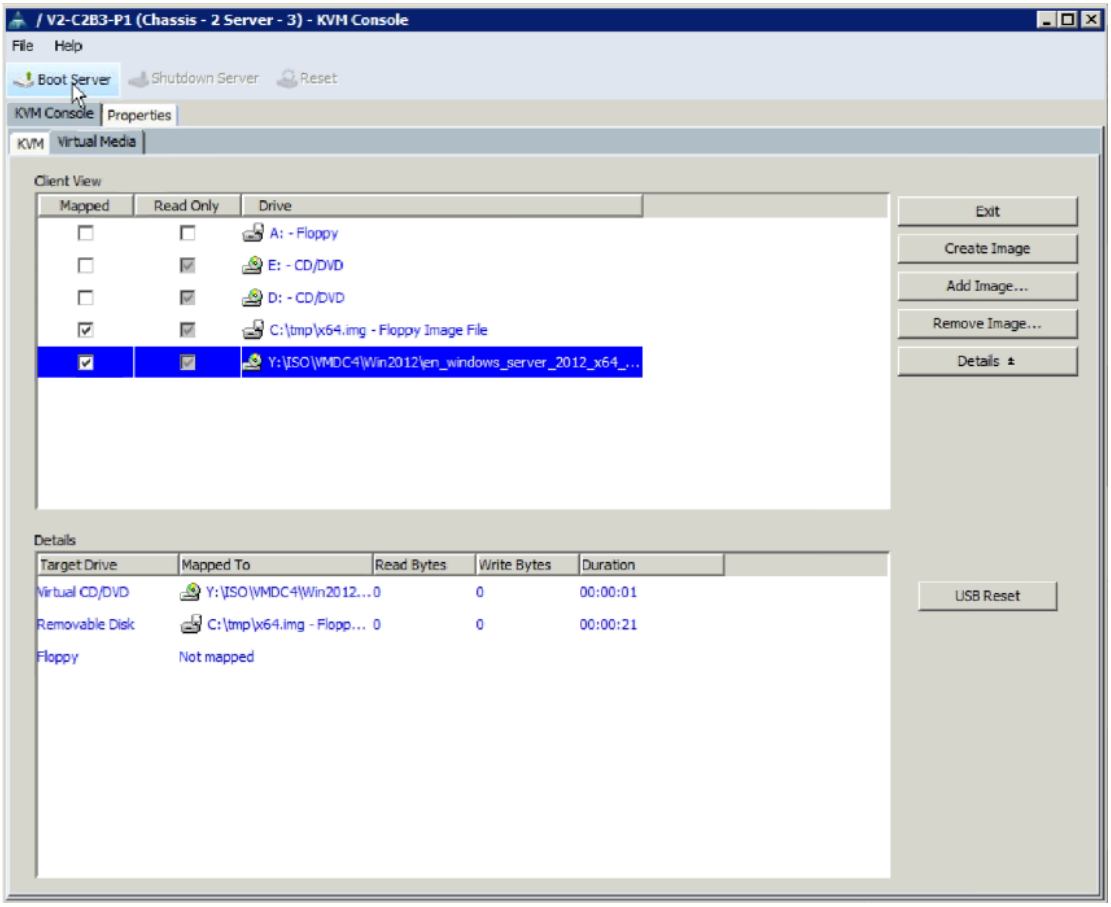
During OS installation, fNIC drivers must be installed in order to scan for the SAN boot LUN. To do this, map to the driver location using the UCS KVM console connection Virtual Media tab before starting the installation, and map to the ISO location of the OS to be installed.

As shown in Figure 2-1, in order to map to more than one image at a time, the FNIC drivers were copied locally (C:tmp in the Drive column). The ISO OS installation image was on a mapped drive to a network share.

Instead of mapping to both images at the same time, you could map and unmap as needed to go between the fNIC drivers and the OS during installation. However, mapping to multiple images supports not having to unmap and remap during installation.

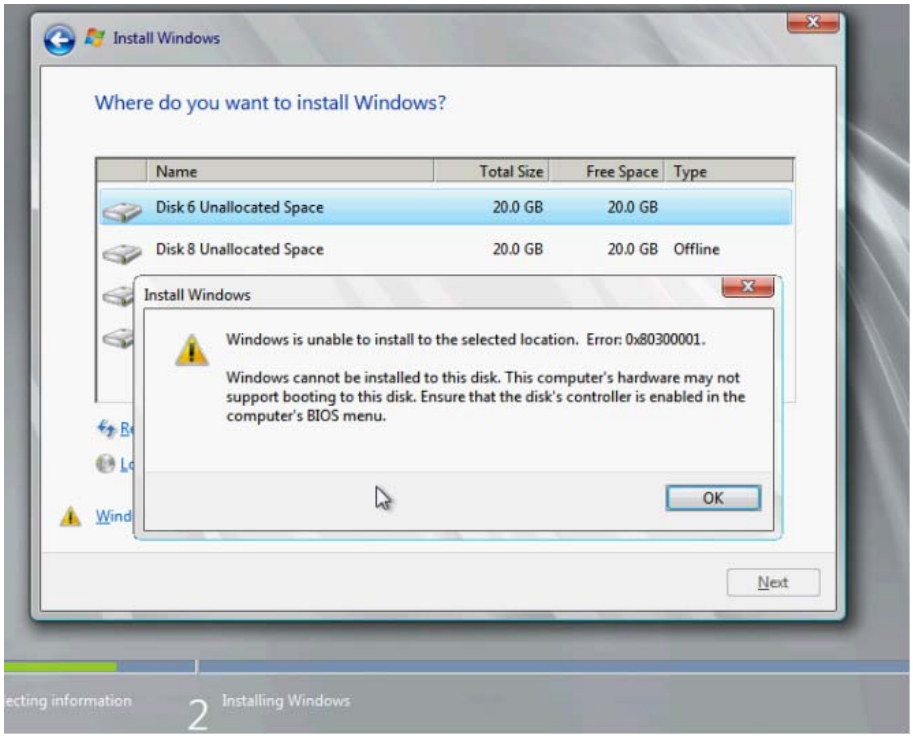
Figure 2-1 shows a display from the KVM Virtual Media tab for what was mapped.

Figure 2-1 Mapped KVM Virtual Media



If you forget to remap to an ISO image, the disk comes online but Windows fails to install and produces the following error:

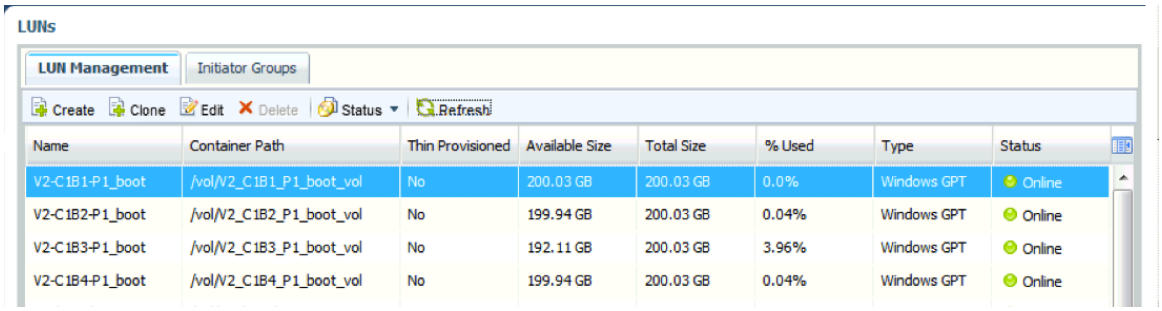
Figure 2-2 Forgot to re-map to ISO image



Note To proceed to the next step, you must remove the driver CD, insert the Windows CD, and refresh.

Step 3 Verify the NetApp LUNs are type **Windows GPT**. There are 2 Windows options for Type in the NetApp used during the testing, Windows and Windows GPT.

Figure 2-3 NetApp LUN configuration for B-Series Servers



Deployment Guidelines

1. Refer to Windows Boot from Fibre Channel SAN guide for an overview and the detailed instructions the administrator should follow.
2. Refer to Support for booting from a Storage Area Network (SAN) for information about booting a Windows server from a SAN.
3. Shutdown all but one path to Boot LUN.

Refer to Windows Setup in a boot from SAN configuration reports. Setup was unable to create a new system partition or locate an existing system partition.

4. Configure the NetApp Boot LUN as Windows GUID Partition Table (GPT).

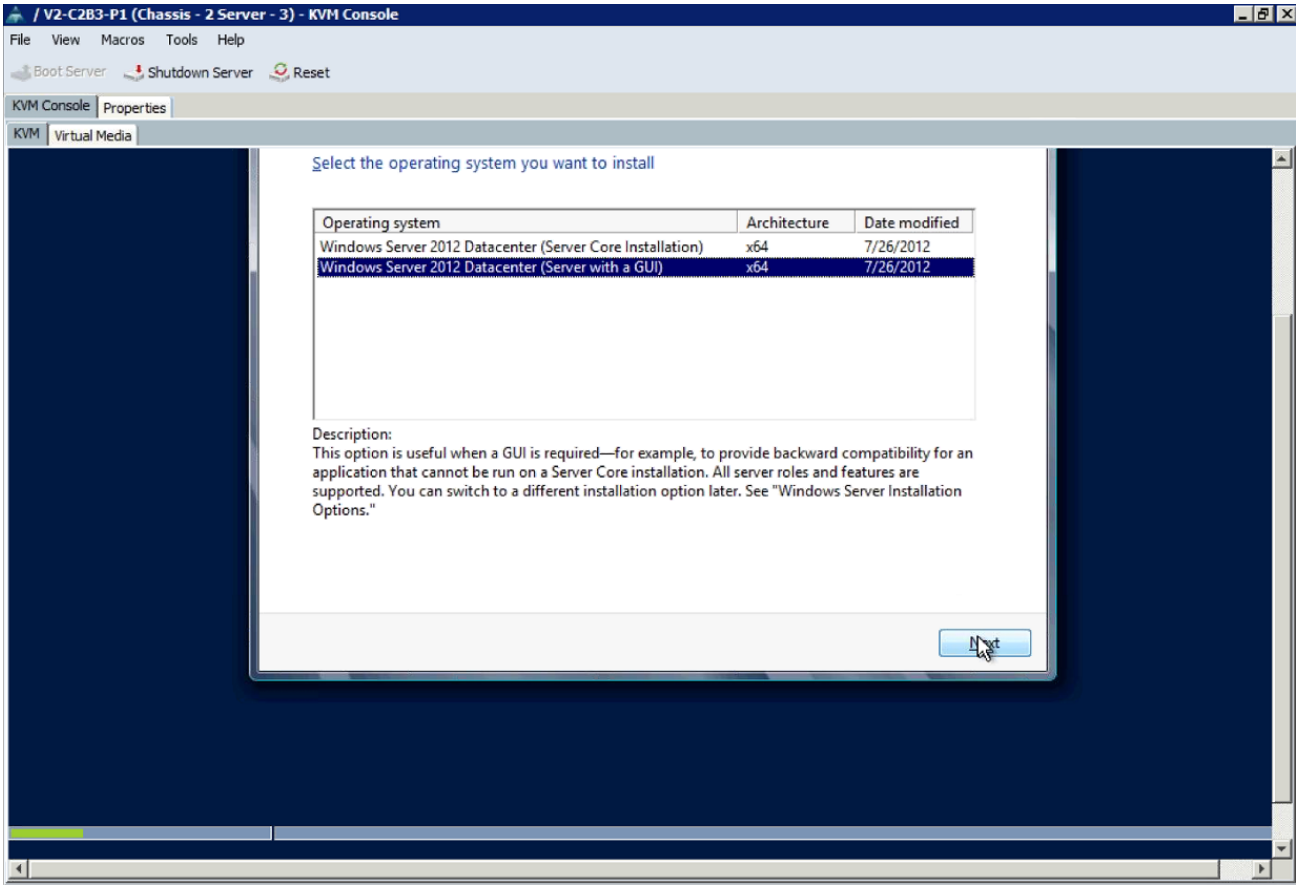
Microsoft Windows Server 2012 and Hyper-V Implementation

This section covers Microsoft Windows Server 2012 and Hyper-V implementation. A common misconception of Microsoft Hyper-V is that it is a Type-2 hypervisor because installation of Windows Server 2012 is required. However, Hyper-V is considered a Type-1 hypervisor because VMs can interface directly with the hypervisor layer, bypassing the operating system layer.

There are two versions of Hyper-V. The first is a standalone product called Microsoft Hyper-V Server 2012. This free product is available for download from Microsoft. The second version is the Hyper-V feature bundled with Microsoft Windows Server 2012.

For Microsoft Server 2008 R2, there were three editions: Standard, Enterprise, and Datacenter. For Windows Server 2012, the Enterprise edition was eliminated. The Standard and Datacenter editions support installing Hyper-V.

Figure 2-4 Data Center Edition



The choice between Standard and Datacenter Edition depends upon the number of active VMs required in the datacenter. Standard Edition supports a maximum of two VMs, but the Datacenter Edition does not limit active VMs.

Microsoft Windows Server 2012 Installation

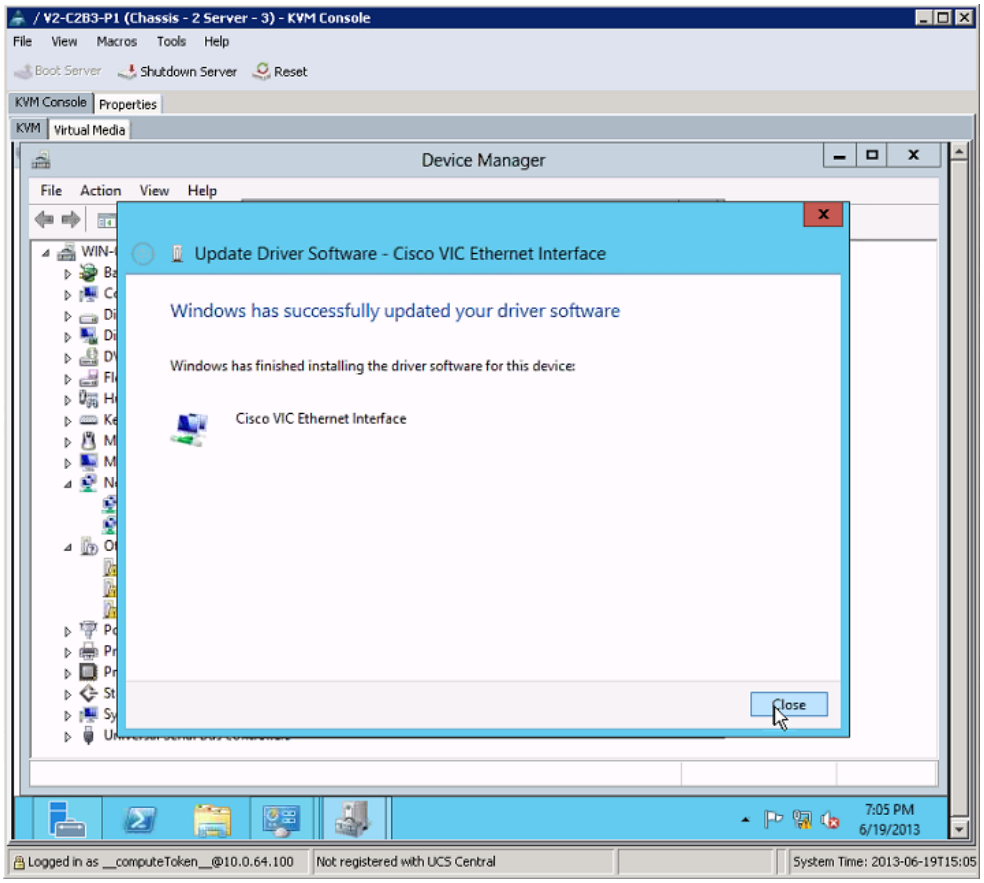
The Windows Server 2012 edition (Standard or Datacenter) to be installed depends upon the product key entered. To simplify installation, use the GUI to install Windows Server 2012 using the GUI. This is also the reason why it is better to install the full Windows Server 2012 instead of the standalone Hyper-V server.

Step 1 Install Windows Server 2012.

Refer to the Installing Windows Server 2012 site for detailed guidance.

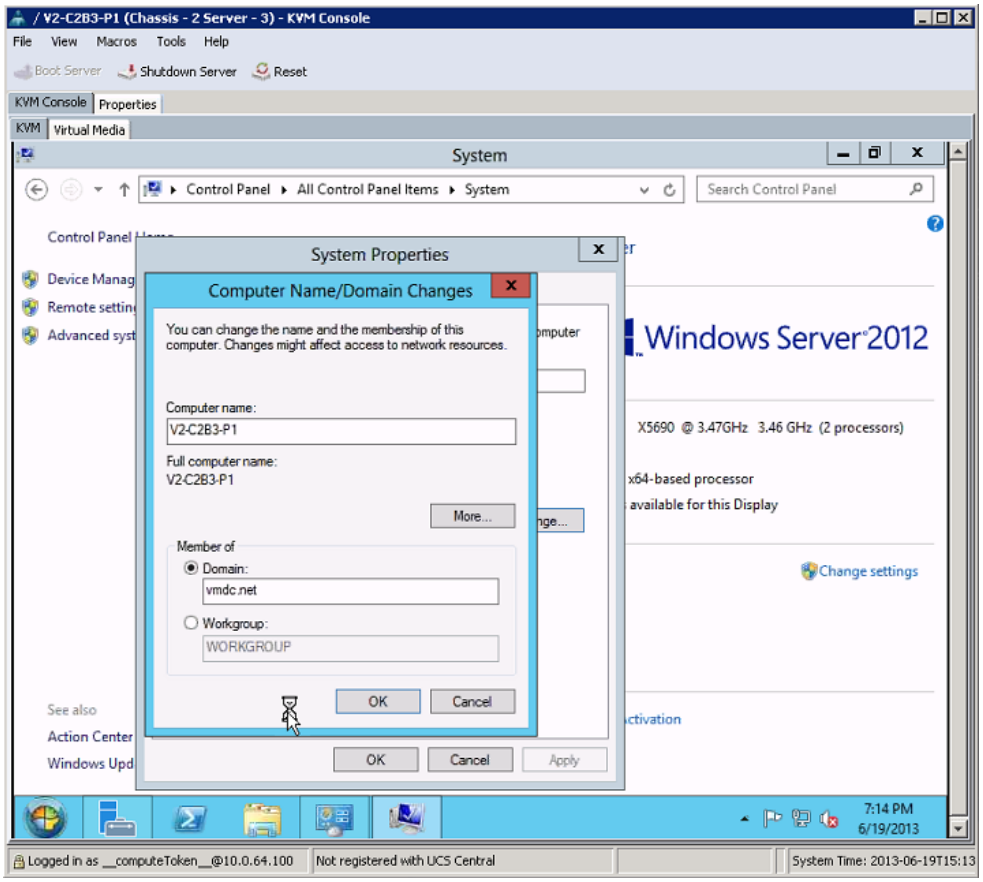
Step 2 After the installation completes, install the Cisco eNIC drivers to enable the network interface cards (NICs). The drivers are available on the Cisco software download site.

Figure 2-5 NIC Driver Installation



Step 3 After the NICs are enabled, verify that the server joins an Active Directory (AD) domain. This also satisfies the Network Time Protocol (NTP) requirement.

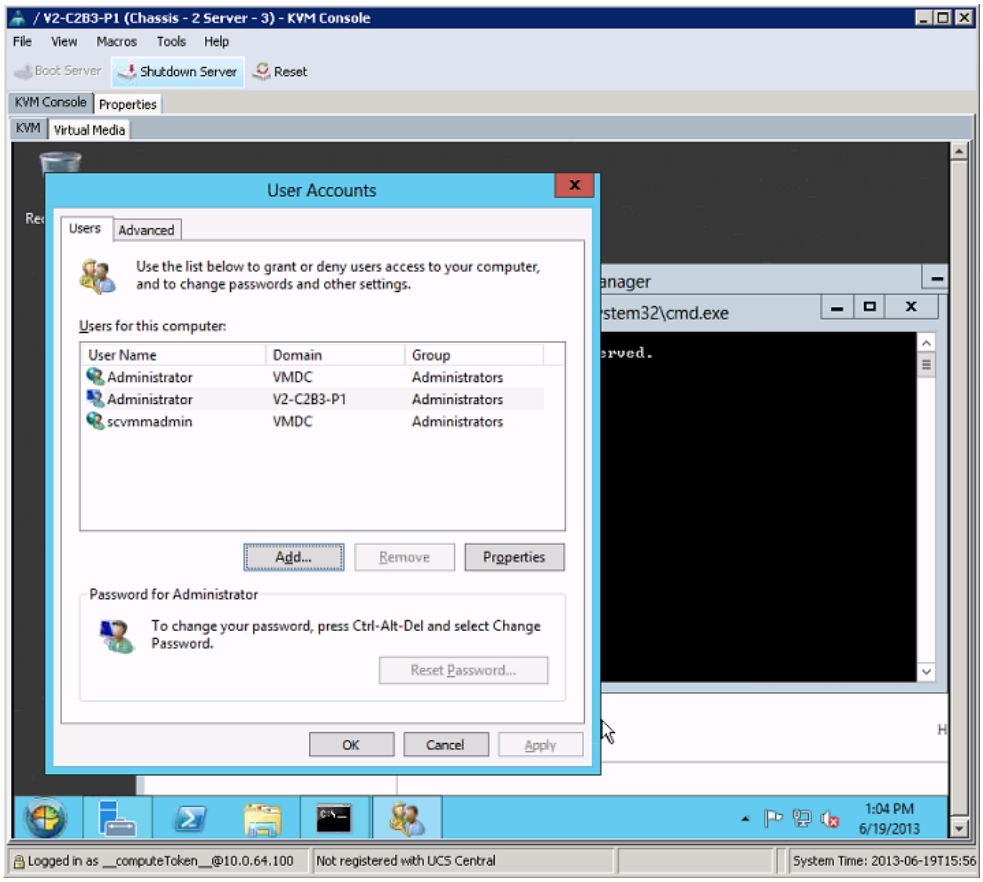
Figure 2-6 Joining an AD Domain



Step 4 On the AD server, verify that the **Administrator** account has Domain Administrator access. Add the **scvmmadmin** account and grant it the Domain Administrator access.

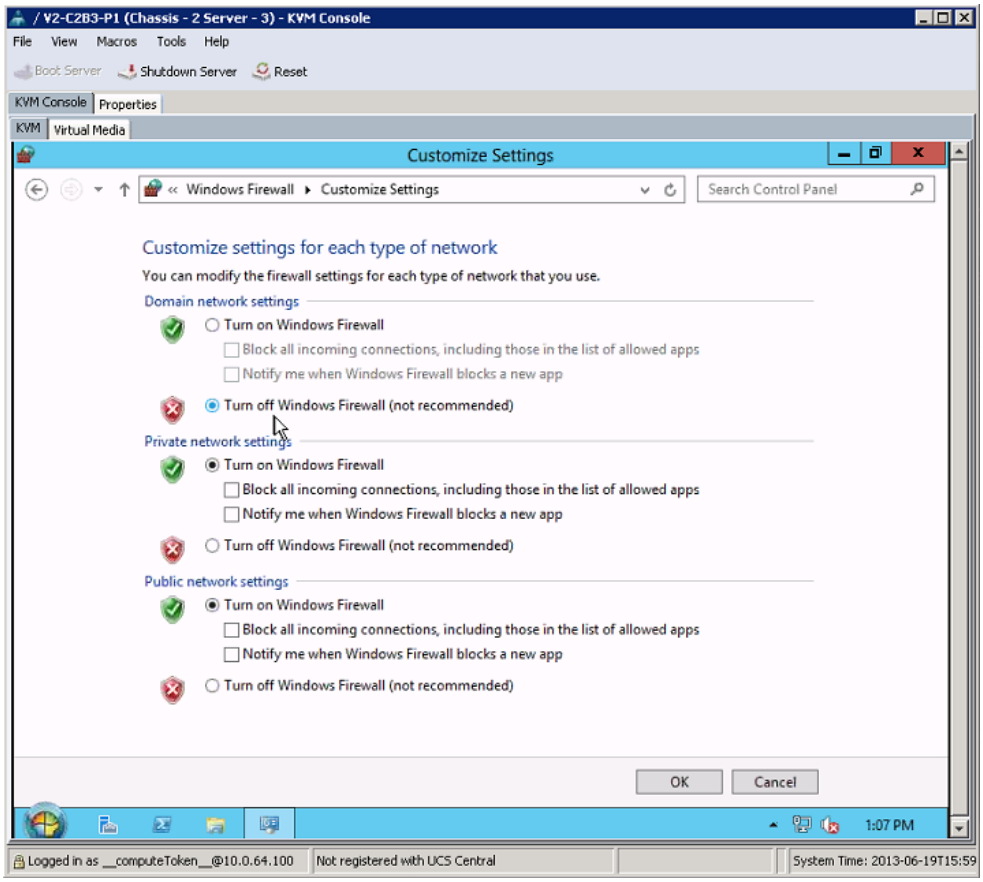
Step 5 On the Windows Server 2012 server, verify that the AD **Administrator** and **scvmmadmin** accounts are available and add them if they are not available. After AD **Administrator** and **scvmmadmin** accounts are available, log off and log on as the Domain Administrator.

Figure 2-7 Administrator and scvmmadmin Accounts



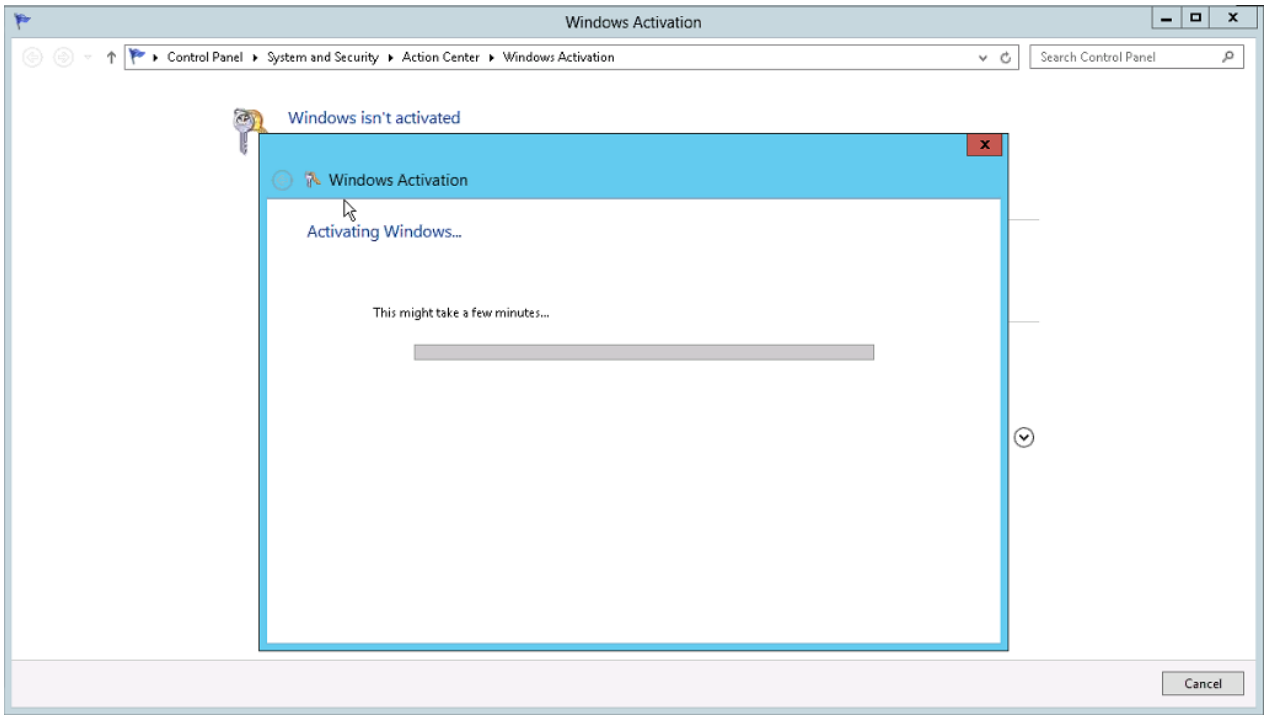
Step 6 After logging in, turn off the Windows Firewall in the Windows Firewall control panel.

Figure 2-8 Disabling Windows Firewall



Step 7 Verify that Windows Server 2012 can access the internet and activate Windows.

Figure 2-9 Windows Activation

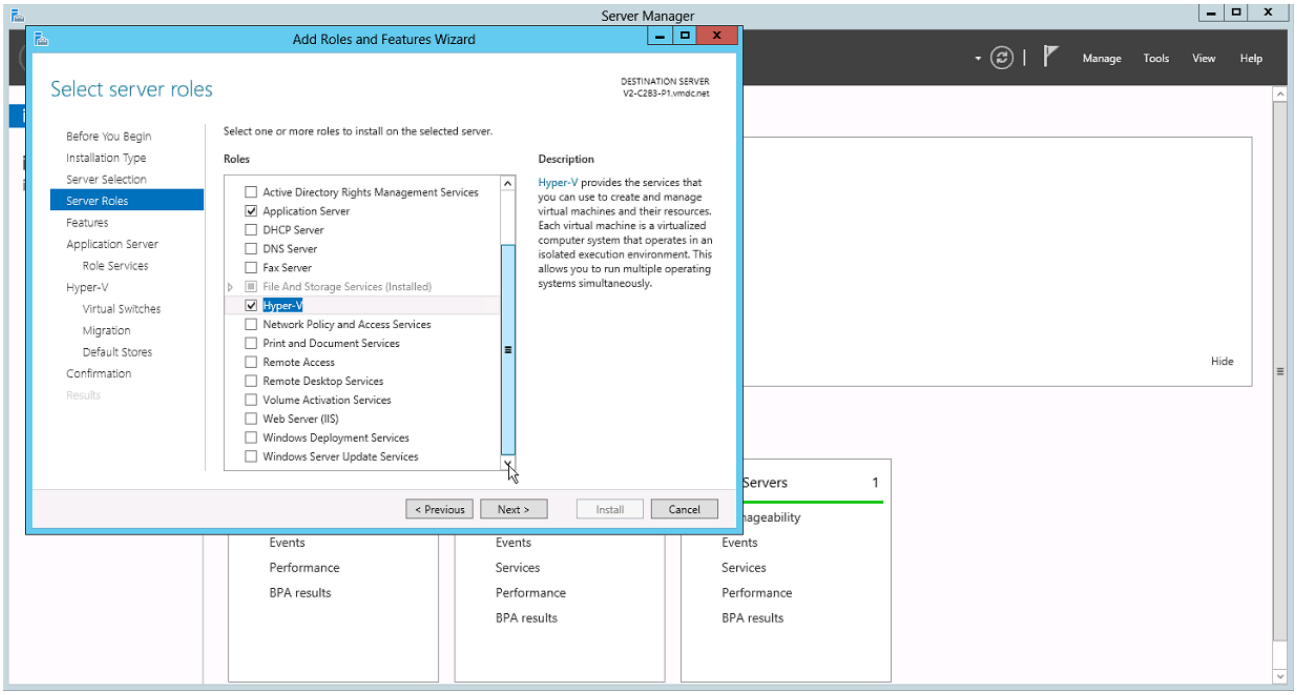


Microsoft Hyper-V Installation

Although Microsoft Hyper-V is included in Windows Server 2012, Hyper-V is not installed by default. After the initial Windows Server 2012 install finishes, the System Administrator must add the Hyper-V role manually. This section outlines the steps to install and configure Hyper-V.

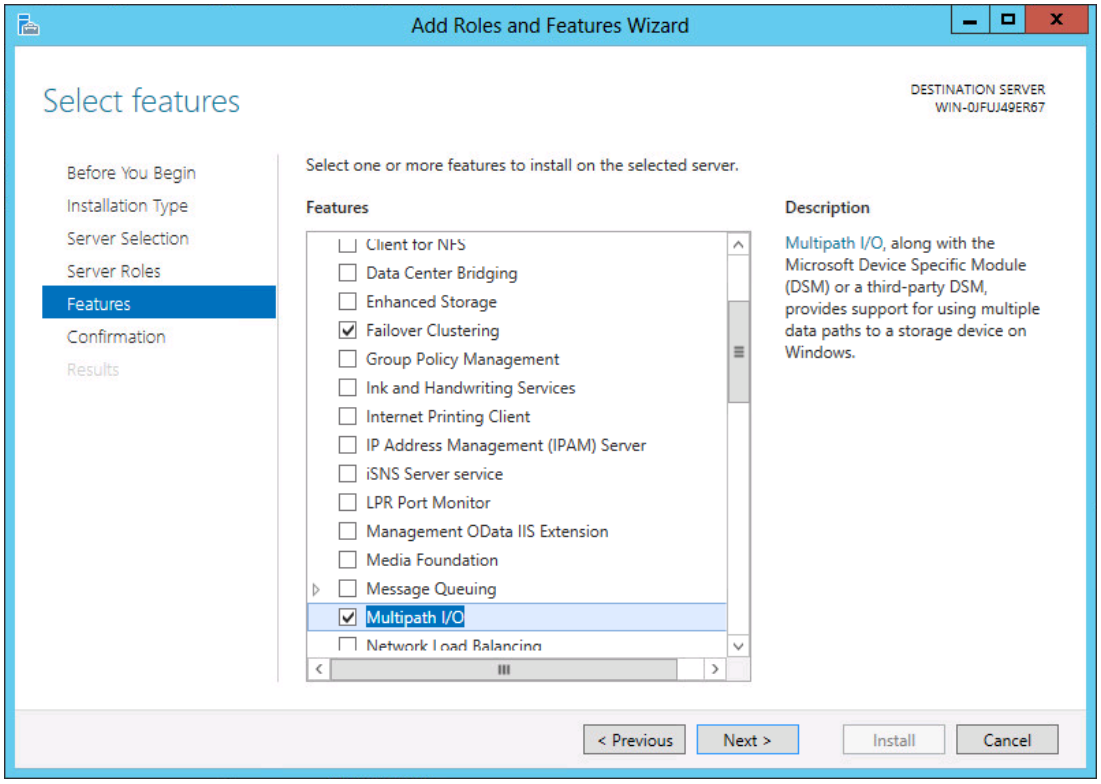
Step 1 In Server Manager, bring up **Add Roles and Features Wizard**.

Figure 2-10 Add Roles and Features Wizard



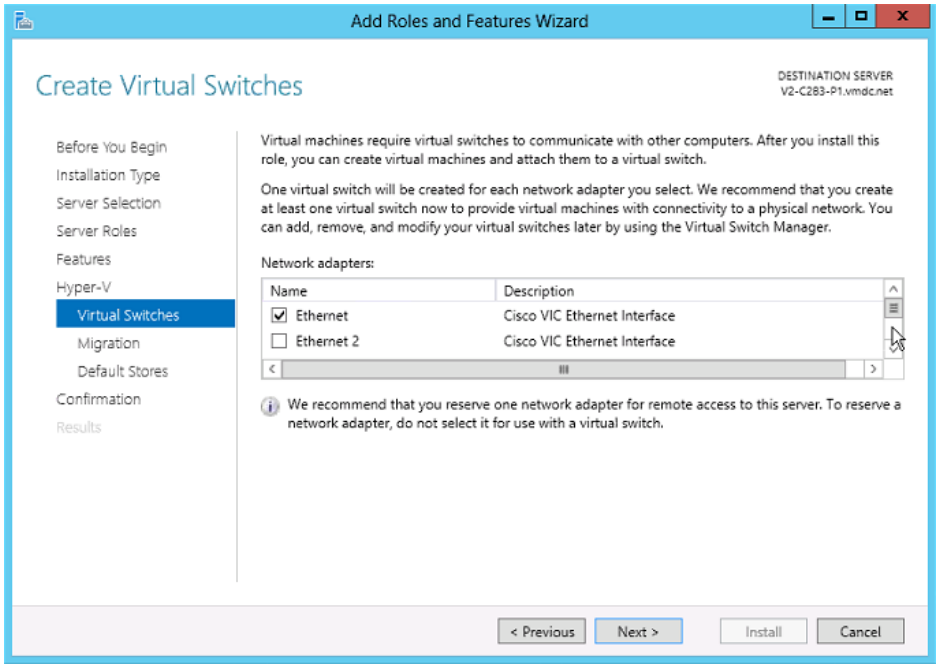
Step 2 In the Wizard, click **Next** until the "Server Roles" window appears. Verify that the **Hyper-V** role is selected and click **Next**. In the **Features** window, verify that **Failover Clustering** and **Multipath I/O** are selected.

Figure 2-11 Features Wizard



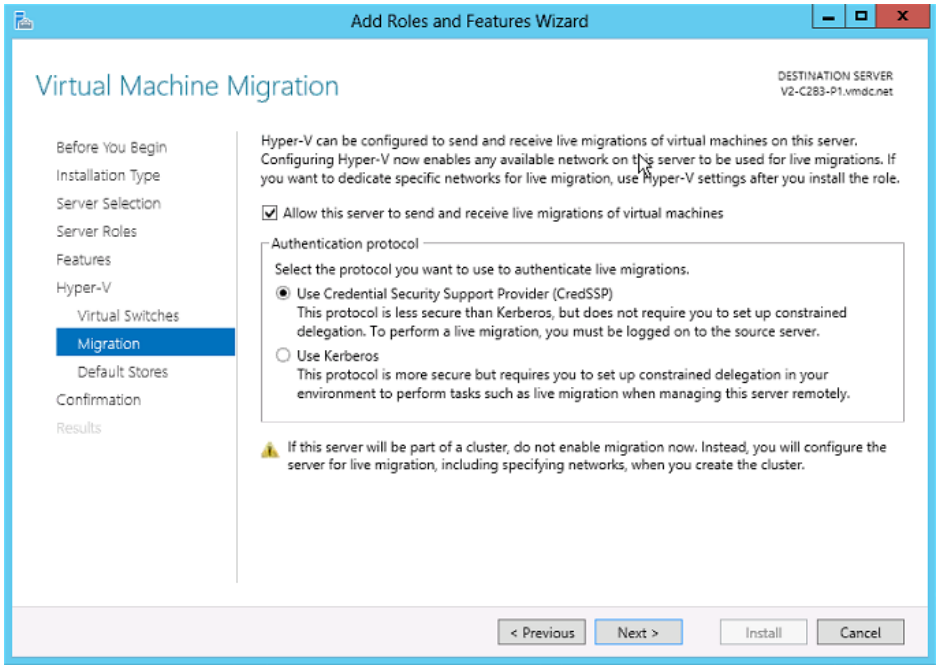
Step 3 With the Hyper-V role selected, the Wizard prompts for the creation of virtual switches. Depending on the number of available NICs, it is a good practice to create at least one switch for management. At the same time, reserve at least one NIC for the Nexus 1000V Switch for Microsoft Hyper-V.

Figure 2-12 Creating Virtual Switches



Step 4 Verify that Live Migrations are selected. This is a key advantages of Hyper-V.

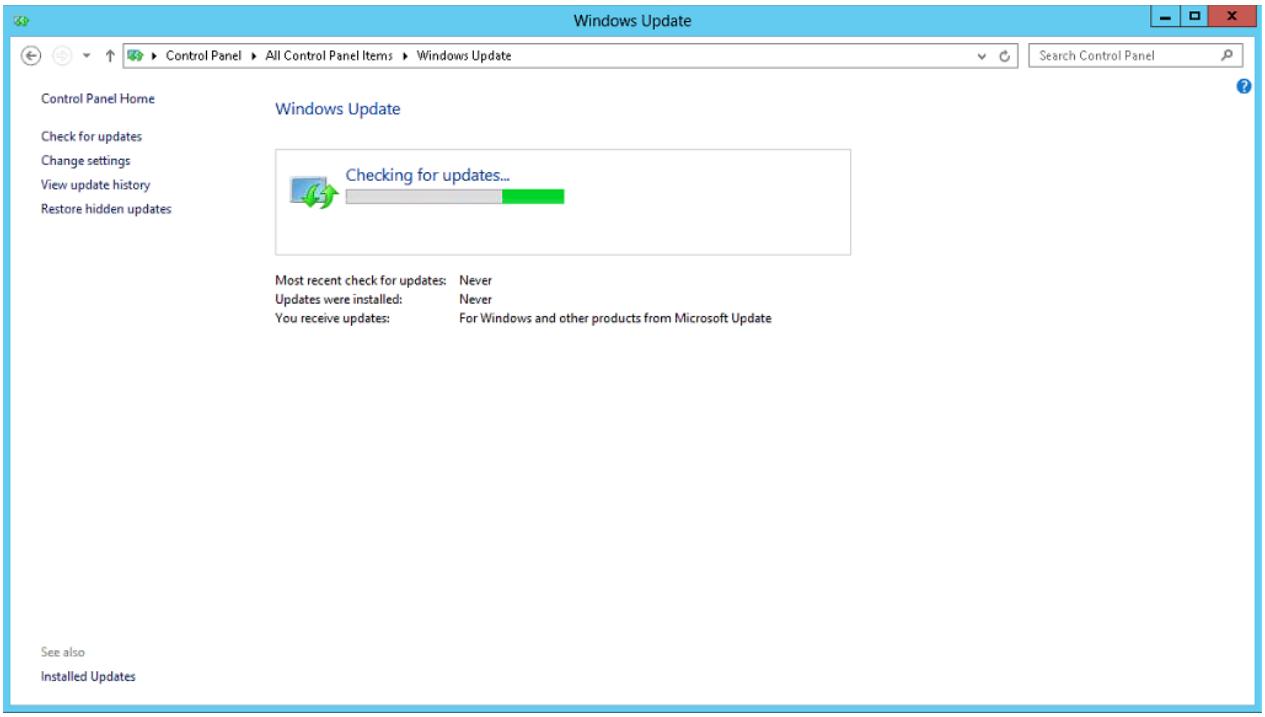
Figure 2-13 Live Migration Option



Step 5 Use the Defaults for the rest of the Wizard. Once the installation completes, reboot the server. The Windows Server 2012 server might reboot several times to install the added Roles and Features. This is normal. Simply wait until all the installation completes.

Note Run Windows Update to ensure that all installed components are running the latest versions.

Figure 2-14 Windows Update



Step 6 Repeat the above procedures for all Hyper-V hosts.

SQL Server 2012 Installation

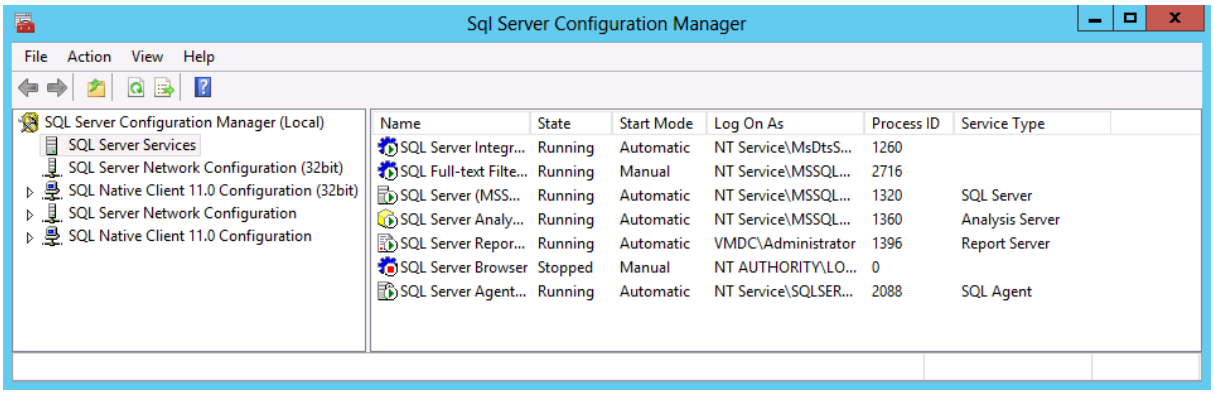
Before setting up Microsoft System Center 2012, we highly recommend that the System Administrator sets up a dedicated Microsoft SQL Server 2012 instance. Although System Center can install SQL Express, it is prudent to use the full version of SQL Server because it enables users to back up the database or set up MSCS clustering, which supports easy database recovery if a disaster occurs.

Step 1 Installing the SQL Server is straightforward. Unless MSCS clustering is required, no Windows Server 2012 customization is needed. Simply install Windows Server 2012 (either Standard or Enterprise) and then install SQL Server 2012 onto Windows Server 2012. After installation finishes, run Windows Update to obtain the latest patches and updates.

Refer to Install SQL Server 2012 from the Installation Wizard guide for information on installing SQL server.

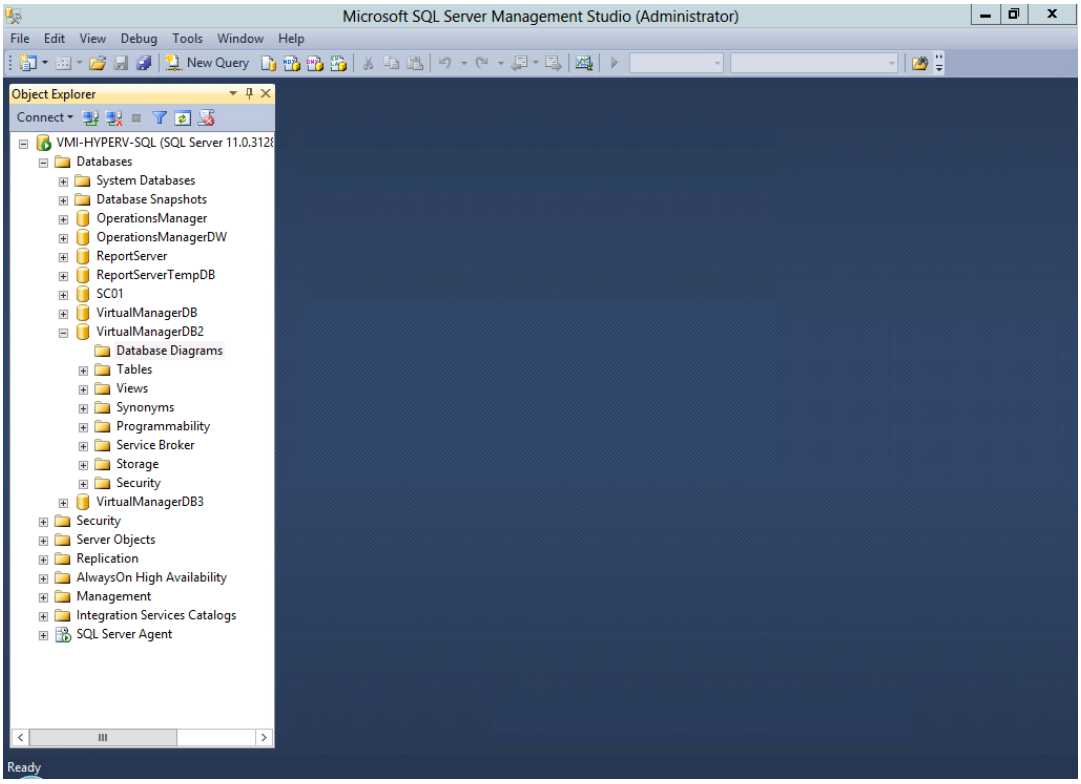
Step 2 Verify that all SQL Server services are running and bring up the SQL Server Configuration Manager.

Figure 2-15 SQL Server Configuration Manager



Step 3 Add, view, delete, or perform maintenance on any databases using SQL Server Management Studio.

Figure 2-16 SQL Server Management Studio



Note The necessary databases are automatically created when any System Center 2012 components are installed. No user intervention is necessary.

Deployment Guidelines

1. If a System Center 2012 component cannot communicate with SQL Server 2012, the problem might be caused by Windows Firewall. Disable Windows Firewall on all servers.
2. We highly recommend making periodic database backups to ensure effective disaster recovery. For more information about database backups, refer to Create a Full Database Backup (SQL Server).
3. Before installing System Center 2012, the System Administrator should create a test database and verify that all servers can connect to that test database.

Microsoft System Center 2012

This section describes Microsoft System Center 2012 (MSC) and System Center Virtual Machine Manager 2012 (SCVMM).

Refer to Installing System Center 2010 – Virtual Machine Manager for installation guidance.

SCVMM is part of MSC. Evaluation copies of MSC can be downloaded from the Microsoft System Center 2012 website.

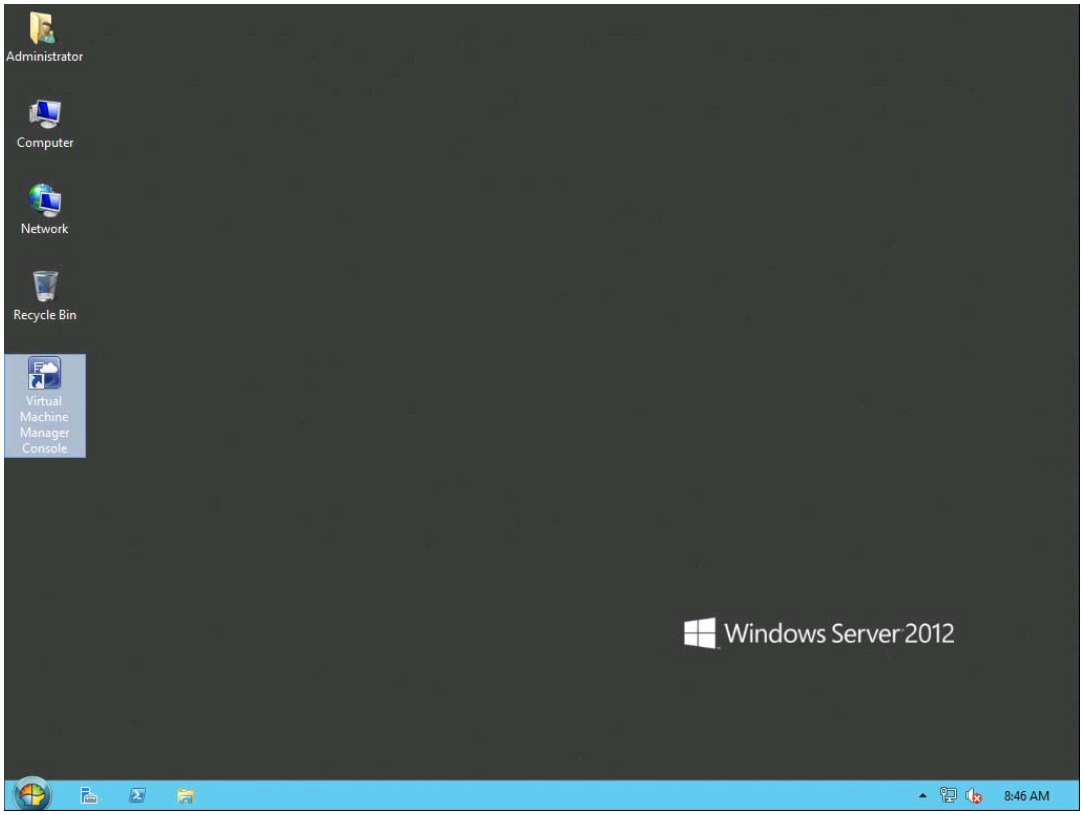
SCVMM can reside on a VM or a physical server. The Administrator can base the decision on preference and the availability of resources.

SCVMM requires a MS-SQL database server and an Active Directory server with the existing setup.

Step 1 Connect the Windows Server 2012 server to the AD domain where the Hyper-V servers resides on.

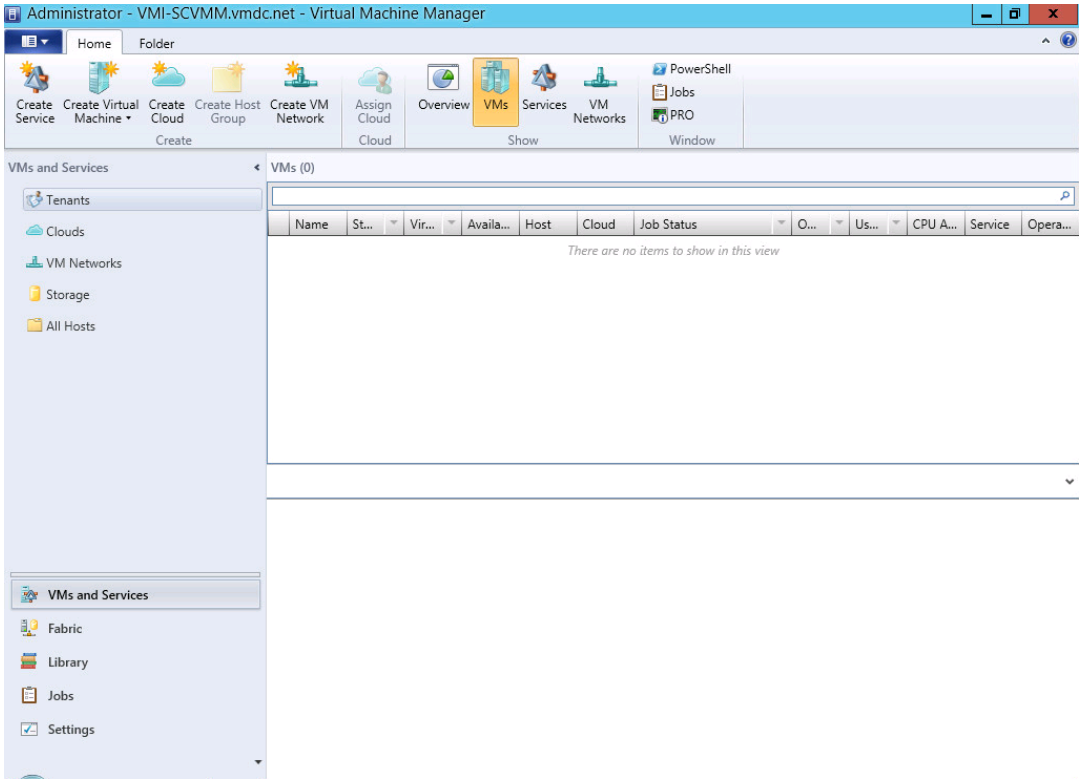
Step 2 The installation prompts for database information and automatically create a database instance on the server. If no database server is available, MS-SQL Express is automatically installed. After the installation finishes, the Virtual Machine Management (VMM) Console icon should appear on the Windows Server 2012 desktop.

Figure 2-17 Virtual Machine Management Console Icon



Step 3 Bring up the VMM Console. You can now add Hyper-V hosts and the Nexus 1000V Switch for Microsoft Hyper-V.

Figure 2-18 VMM Console



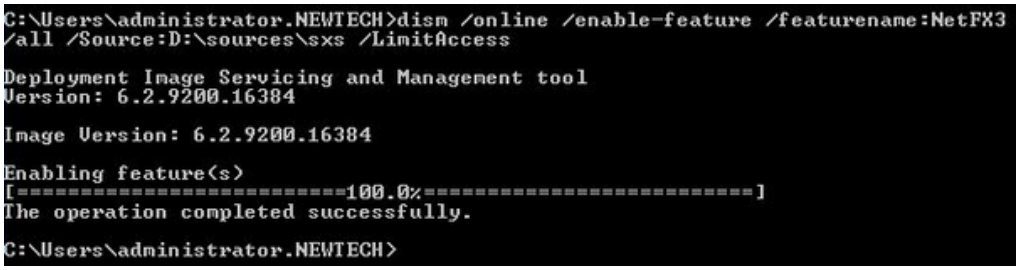
Deployment Guidelines

SCVMM requires .NET Framework 3.5 and .NET Framework 4.0 to be installed on the Windows Server 2012 server that SCVMM resides on. While .NET 4.0 can easily be added through the Roles and Features Wizard, installing .NET 3.5 through the same wizard will only result in an error. This is a known Microsoft issue. The only workaround to this issue is to use the following method.

1. Verify that the Windows Server 2012 server can connect to the internet.
2. Bring up the KVM console using UCSM.
3. Mount the Windows Server 2012 installation media onto the CD/DVD drive (D:).
4. Enter the following command on a DOS prompt:

```
dism /online /enable-feature /featurename:NetFX3 /all /Source:d:\sources\sxs
/LimitAccess
```

Figure 2-19 dism Output



5. Repeat the same command and procedure for “asp.net”.

```
dism /online /enable-feature /featurename:iis-aspnet /all /Source:d:\sources\sxs
/LimitAccess
```

This should satisfy all the prerequisites for SCVMM.

Virtual Switch Module Installation on Nexus 1110

The Cisco Nexus 1000V Switch for Microsoft Hyper-V Distributed Virtual Switch requires a Virtual Supervisor Module (VSM) for control and management. The VSM controls multiple Virtual Ethernet Modules (VEMs) as one logical modular switch. However, while a physical switch uses linecards for Ethernet connectivity, VEMs are logical entities running in software inside physical servers.

In this test setup, VSMs were deployed in a Nexus 1110 Virtual Service Appliance (VSA), instead of in a Windows Server 2012 blade with Hyper-V enabled. From an architectural perspective, the idea is that the VSA resides in the management pod (called “VMI”), colocated with other management servers, rather than with production resources.

The deployment procedure for the Nexus 1000V Switch for Microsoft Hyper-V VSMs (VSBs) for Hyper-V is the same as for VMware deployments.

Refer to Installing VSM on Cisco Cloud Service Platform for additional guidance.

Refer to Cisco Nexus Virtual Services Appliance Release Notes, Release 4.2(1)SP1(5.1a) for more information about new features and caveats.

Deployment Guidelines

1. Use the correct ISO image for Hyper-V.

   When creating the VSB, use the correct ISO for Hyper-V, as described in Step 4 of *Configuring Virtual Service Blades* in the Configuration guide.

2. Use a unique Domain ID in the VSM.

   The Domain ID configured in the VSBs must be different than the domain ID used for the Nexus 1110 VSA. If domain IDs are not unique, the secondary VSA continuously reboots and message similar to this is seen:

```
2013 Jun  1 10:07:53 vsm-1 %KERN-1-SYSTEM_MSG: Dropping received frames from
duplicate VSM saddr (0x1010000) - kernel
```

Note See CSCtq75997 more information.

CHAPTER 3

Nexus 1000V Switch for Microsoft Hyper-V Configuration

This section describes how to configure the Nexus 1000V Switch for Microsoft Hyper-V in a VMDC solution.

- VSM CLI Configuration
- SCVMM Configuration

Figure 3-1 compares the SCVMM and Nexus 1000V Switch for Microsoft Hyper-V terminology that will be referenced in each section.

The reader should be familiar with these terms to better understand the role of each object as it pertains to the entire configuration and how each relates to SCVMM and the Nexus 1000V Switch for Microsoft Hyper-V.

Figure 3-1 SCVMM and Nexus 1000V Switch for Microsoft Hyper-V Terminology

SCVMM Terminology	Cisco Nexus 1000V Terminology
Logical Networks	Logical Networks
Network Sites	Network Segment Pools
VM Network Definitions	Network Segments
IP-Pools	IP-Pools & IP-Pool Templates
Port-Classifications	Port-profiles

Network and Tenants Under Test

Three private tenants and one public tenant **logical networks** were created.

Six **network segment pools** were created, three public (T1, T2, T3) and three private (PT1, PT2, PT3). The three public network segment pools were configured as members of the public tenant logical network; the three private network segment pools were each configured as an individual member of a the three private tenant logical networks.

Only one **network segment** per public network segment pool was created. Two network segments per private network segment pool were created.

The **IP pool templates** and **port-profiles** are described in the IP Pool templates and Port-profiles sections later in the doc.

The configuration looks like this:

```
logical network  PublicTenants
    network segment pool T1
       network segment T1-NetworkSegment101
    network segment pool T2
       network segment T2-NetworkSegment102
    network segment pool T3
       network segment T3-NetworkSegment103

logical network  PrivateTenant1
    network segment pool PT1
       network segment PT1-NetworkSegment2013
       network segment PT1-NetworkSegment2014

logical network  PrivateTenant3
    network segment pool PT2
       network segment PT2-NetworkSegment2023
       network segment PT2-NetworkSegment2024

logical network  PrivateTenant3
    network segment pool PT3
       network segment PT3-NetworkSegment2033
       network segment PT3-NetworkSegment2034
```

Refer to Cisco Nexus 1000V for Microsoft Hyper-V Network Segmentation Manager Configuration Guide for more information about Microsoft networking concepts, command details, and implementation.

Refer to Cisco Nexus 1000V for Microsoft Hyper-V Release Notes, Release 5.2(1)SM1(5.1) for new features and caveats.

Nexus 1000V Switch for Microsoft Hyper-V VSM CLI Configuration

This section describes how to configure the Nexus 1000V with Hyper-V using the Network Segmentation Manager (NSM) CLI on the VSM.

Step 1 Create Logical Networks.

A logical network (for example, internet, intranet, DMZ) is a connectivity abstraction that models separate networks managed by an enterprise. Logical network abstraction hides VLANs and IP subnets from users (VM network administrators, the tenant administrators, and the server administrators), except for the fabric administrator managing the physical fabric.

In other words, a logical network is composed of one or more network segment pools and each network segment pool is a group of VLANS, IP subnets, or VLAN/IP subnet pairs.

The following logical networks configuration shows three private tenants and one public tenant.

```
nsm logical network PublicTenants
nsm logical network PrivateTentant1
nsm logical network PrivateTentant2
```

```
nsm logical network PrivateTentant3
```

Step 2 Create Network Segments Pools.

A network segment is associated with a unique broadcast domain and facilitates the availability of the network resources to a VM. SCVMM uses the VM networks and the VM subnets to provide the isolated virtual machine networks.

When a Nexus 1000V manages the virtual network, the VMM administrator creates the VM networks that use external isolation. To create external isolation, the network administrator creates network segments on the Nexus 1000V and provisions the isolated networks using VLANs and private VLANs.

Note In Nexus 1000V for Microsoft Hyper-V, a VLAN is not created to define a bridge domain. Instead, a network segment is created on the VSM. Creating a network segment triggers VLAN auto-creation.

The following configuration shows network segment pools.

```
nsm network segment pool T1
nsm network segment pool T2
nsm network segment pool T3
nsm network segment pool PT1
nsm network segment pool PT2
nsm network segment pool PT3
```

Step 3 Add each Network Segment Pool to the Logical Network.

The T1, T2, and T3 segment pools are members of the same public tenant logical network. The PT1, PT2, and PT3 segment pools are members of unique logical networks.

The following configuration shows mapping for network segment pools into logical networks.

```
nsm network segment pool T1
  member-of logical network PublicTenants
nsm network segment pool T2
  member-of logical network PublicTenants
nsm network segment pool T3
  member-of logical network PublicTenants
nsm network segment pool PT1
  member-of logical network PrivateTentant1
nsm network segment pool PT2
  member-of logical network PrivateTentant2
nsm network segment pool PT3
  member-of logical network PrivateTentant3
```

Step 4 Create IP Pool Templates.

Server administrators can manage IP addresses for the virtual environment using IP pool templates. You can use the IP pool templates to assign a range of IP addresses to hosts and VMs in the Microsoft SCVMM-managed environment. When creating an IP pool template for a VM network, you can define a range of IP addresses for VMs managed by SCVMM.

The following configurations shows IP pool templates that were created.

```
nsm ip pool template PT1-VL2013-IP-Pool
  ip address 200.1.3.2 200.1.3.250
  network 200.1.3.0 255.255.255.0
  default-router 200.1.3.253
nsm ip pool template PT1-VL2014-IP-Pool
  ip address 200.1.4.2 200.1.4.250
  network 200.1.4.0 255.255.255.0
  default-router 200.1.4.253
nsm ip pool template PT2-VL2023-IP-Pool
```

```
  ip address 200.2.3.2 200.2.3.250
  network 200.2.3.0 255.255.255.0
  default-router 200.2.3.253
nsm ip pool template PT2-VL2024-IP-Pool
  ip address 200.2.4.2 200.2.4.250
  network 200.2.4.0 255.255.255.0
  default-router 200.2.4.253
nsm ip pool template PT3-VL2033-IP-Pool
  ip address 200.3.3.2 200.3.3.250
  network 200.3.3.0 255.255.255.0
  default-router 200.3.3.253
nsm ip pool template PT3-VL2034-IP-Pool
  ip address 200.3.4.2 200.3.4.250
  network 200.3.4.0 255.255.255.0
  default-router 200.3.4.253

nsm ip pool template T1-VL101-IP-Pool
  ip address 10.101.1.2 10.101.1.250
  network 10.101.1.0 255.255.255.0
  default-router 10.101.1.253
nsm ip pool template T2-VL102-IP-Pool
  ip address 10.102.1.2 10.102.1.250
  network 10.102.1.0 255.255.255.0
  default-router 10.102.1.253
nsm ip pool template T3-VL103-IP-Pool
  ip address 10.103.1.2 10.103.1.250
  network 10.103.1.0 255.255.255.0
  default-router 10.103.1.253
```

Step 5 Create Network Segments.

Configure each network segment to be a member of the previously configured network segment pools. Configure each network segment as an access port with an access VLAN. Import the previously configured IP pool for each network segment. Publish each network segment.

The Step 9VM Network Creation., page 3-36 commands are added automatically and appear later in this section when configuring VM networks in SCVMM.

VM networks enable the SCVMM administrator to create an isolated virtual Layer 3 (L3) network. Each VM network can have multiple VM subnets (virtual L2 domain). Microsoft SCVMM 2012 supports VLAN-backed and network virtualization (NVGRE)-backed VM networks. The Nexus 1000V supports VLAN-backed VM networks only.

The following configuration shows network segments that were created.

```
nsm network segment T1-NetworkSegment101
  member-of network segment pool T1
  switchport access vlan 101
  ip pool import template T1-VL101-IP-Pool
  publish network segment
  switchport mode access

nsm network segment T2-NetworkSegment102
  member-of network segment pool T2
  switchport access vlan 102
  ip pool import template T2-VL102-IP-Pool
  publish network segment
  switchport mode access

nsm network segment T3-NetworkSegment103
  member-of network segment pool T3
  switchport access vlan 103
  ip pool import template T3-VL103-IP-Pool
  publish network segment
```

```
  switchport mode access

nsm network segment PT1-NetworkSegment2013
  member-of vmnetwork PT1-NetworkSegment2013
  member-of network segment pool PT1
  switchport access vlan 2013
  ip pool import template PT1-VL2013-IP-Pool
  publish network segment
  switchport mode access

nsm network segment PT1-NetworkSegment2014
  member-of network segment pool PT1
  switchport access vlan 2014
  ip pool import template PT1-VL2014-IP-Pool
  publish network segment
  switchport mode access

nsm network segment PT2-NetworkSegment2023
  member-of network segment pool PT2
  switchport access vlan 2023
  ip pool import template PT2-VL2023-IP-Pool
  publish network segment
  switchport mode access

nsm network segment PT2-NetworkSegment2024
  member-of network segment pool PT2
  switchport access vlan 2024
  ip pool import template PT2-VL2024-IP-Pool
  publish network segment
  switchport mode access

nsm network segment PT3-NetworkSegment2033
  member-of network segment pool PT3
  switchport access vlan 2033
  ip pool import template PT3-VL2033-IP-Pool
  publish network segment
  switchport mode access

nsm network segment PT3-NetworkSegment2034
  member-of network segment pool PT3
  switchport access vlan 2034
  ip pool import template PT3-VL2034-IP-Pool
  publish network segment
  switchport mode access
```

Step 6 Create Port profiles.

Unlike the Nexus 1000V for ESX, in which a port profile identifies both network policy and network isolation (VLAN), SCVMM networking decouples this information into a VM network and the port classification. When the Nexus 1000V is used with Hyper-V, the network administrator creates network segments to isolate networks. The SCVMM server administrator uses network segments in the resulting VM networks. The network administrator defines creates port profiles to define port policy. The server administrator uses port profiles to create a port classification.

To deploy a VM to the virtual access layer, choose the port classification, VM network, and the VM subnet. When a VM is deployed, a port profile is dynamically created on the Nexus 1000V for each unique combination of port classification, VM network, and VM subnet. All other VMs deployed with the same policy to this network reuse the dynamic port profile, which is a combination of network isolation and network policy.

Note The generated profile should be neither modified nor inherited in other port profiles.

When a port-attach notification is received, the port profile globally unique identifier (GUID) and network segment GUID are generated. A GUID provides a unique reference for the port profile and the network segment.

When a GUID is generated, a new port profile, combining the port profile and the VLAN, is created on the VSM. This auto-created port-profile is inherited on the interface. If more than one port uses the same combination of port profile and network segment, the port profile is shared. Port profiles are dynamically created during the interface attach process.

The following configuration shows port-profiles that were created.

```
port-profile type vethernet T1-PortProfile
  no shutdown
  state enabled
  publish port-profile
port-profile type vethernet T2-PortProfile
  no shutdown
  state enabled
  publish port-profile
port-profile type vethernet T3-PortProfile
  no shutdown
  state enabled
  publish port-profile
port-profile type vethernet PT1-PortProfile
  no shutdown
  state enabled
  publish port-profile
port-profile type vethernet PT2-PortProfile
  no shutdown
  state enabled
  publish port-profile
port-profile type vethernet PT3-PortProfile
  no shutdown
  state enabled
  publish port-profile
```

Step 7 Create Uplink Port Profile and Network Uplink.

An uplink port profile is essentially a template that defines a list of network segment pools to be associated with any (physical) network adapters to which the uplink port profile is applied. An uplink port profile enables you to specify protocols and port policy for the uplink adapter, using an Ethernet port profile to be specified.

The following configuration shows uplink port-profiles.

```
port-profile type ethernet UplinkPortProfile
  channel-group auto mode on mac-pinning
  no shutdown
  max-ports 512
  state enabled
nsm network uplink UCS-Uplink
  import port-profile UplinkPortProfile
  allow network segment pool T1
  allow network segment pool T2
  allow network segment pool T3
  allow network segment pool PT1
  allow network segment pool PT2
  allow network segment pool PT3
  publish network uplink
```

Note When a new segment is created and tied to an existing network segment pool in the list under the network uplink, VLANs are inherited in the NSM created profile as shown.

The following configuration shows an Ethernet UCS-Uplink port-profile.

```
port-profile type ethernet UCS-Uplink
  inherit port-profile UplinkPortProfile
  switchport mode trunk
  switchport trunk allowed vlan 101-103,2013-2014,2023-2024,2033-2034
  no shutdown
  max-ports 512
  description NSM created profile. Do not delete.
  state enabled
```

Note The **Switchport allow vlan add** command is not needed.

Nexus 1000V Part 2: SCVMM Configuration

This section provides guidance on how to create the N1000V logical switch (VSM and VEMs) in Hyper-V through SCVMM.

Step 1 Download Cisco Nexus 1000V Package.

The Nexus 1000V for Hyper-V package (zip file) is available at the download URL location provided with the software. Complete the following steps to download the package.

Download the Cisco Nexus 1000V for Microsoft Hyper-V package for Microsoft System Center Virtual Machine Manager (SCVMM) 2012. The package contains the following files:

- Virtual Supervisor Module (VSM) ISO (n1000vh-dk9.5.2.1.SM1.5.1.iso)
- Virtual Ethernet Module (VEM) MSI package (Nexus1000V-VEM-5.2.1.SM1.5.1.msi)
- Cisco VSEM Provider MSI package (Nexus1000V-VSEMProvider-5.2.1.SM1.5.1.msi)
- Cisco SCVMM VM Template (Cisco Nexus1000V VSM Template)
- Cisco Installer App (Cisco.Nexus1000VInstaller.UI.exe)

Step 2 Install the Virtual Switch Extension Manager Provider.

To establish communication between SCVMM and the Nexus 1000V VSM, the Virtual Switch Extension Manager (VSEM) provider must be installed on the SCVMM server.

a. Run the Cisco VSEM Provider MSI package (Nexus1000V-VSEMProvider-5.2.1.SM1.5.1.msi) that comes with the Nexus 1000V Package.

   Follow the link to where the MSI was downloaded and double-click **MSI** to run it.

b. Follow the prompts as shown in Figure 3-2, Figure 3-3, and Figure 3-4 until the install is complete.

Figure 3-2 Run the MSI Installer

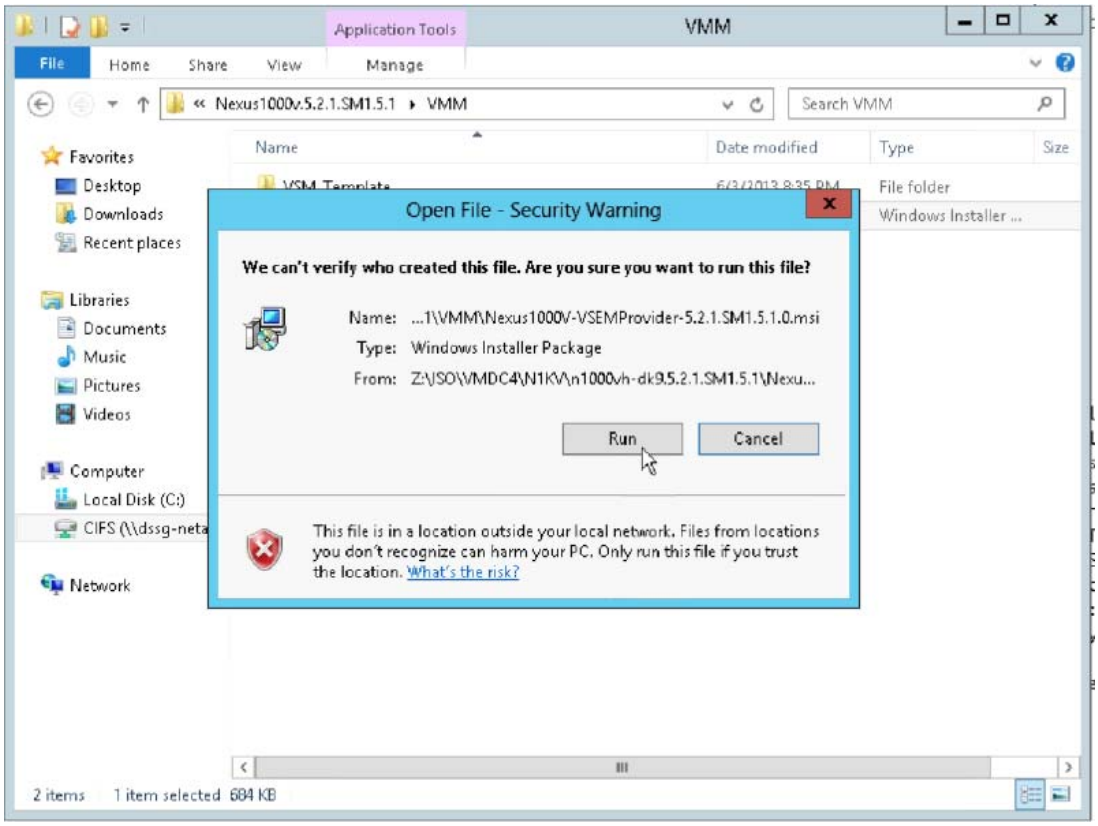


Figure 3-3 Read and Accept the License Agreement

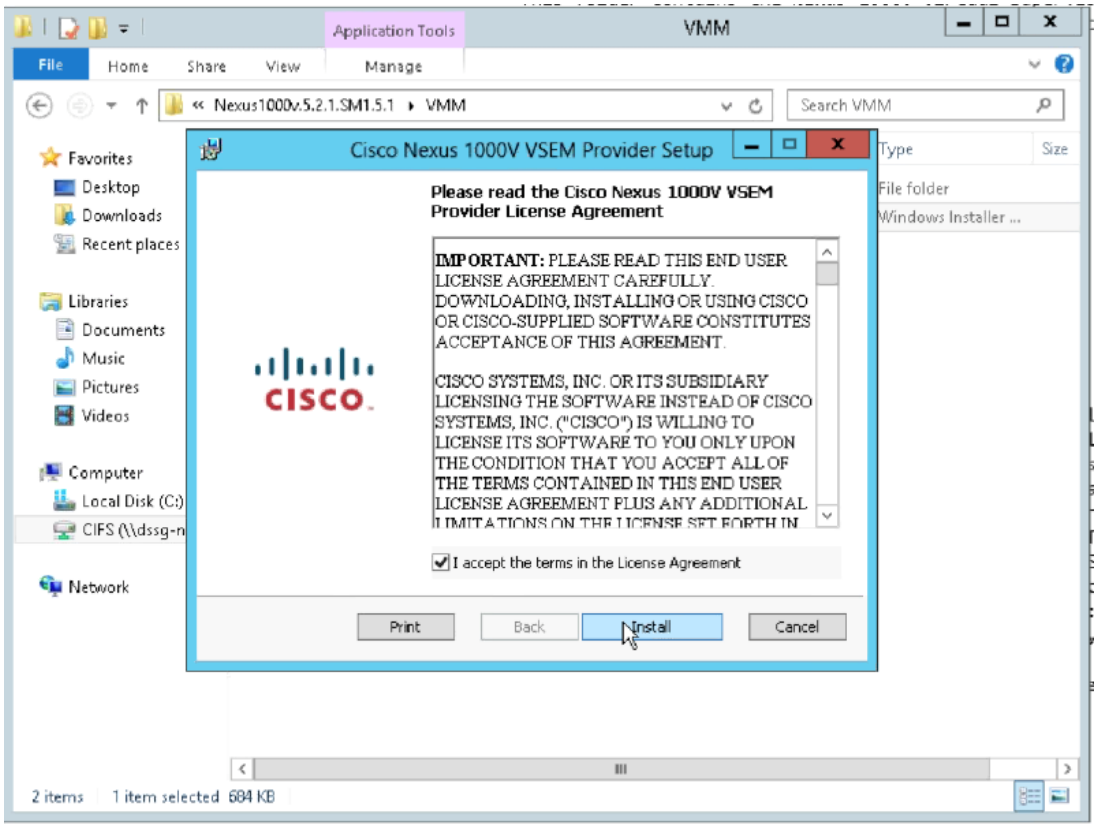
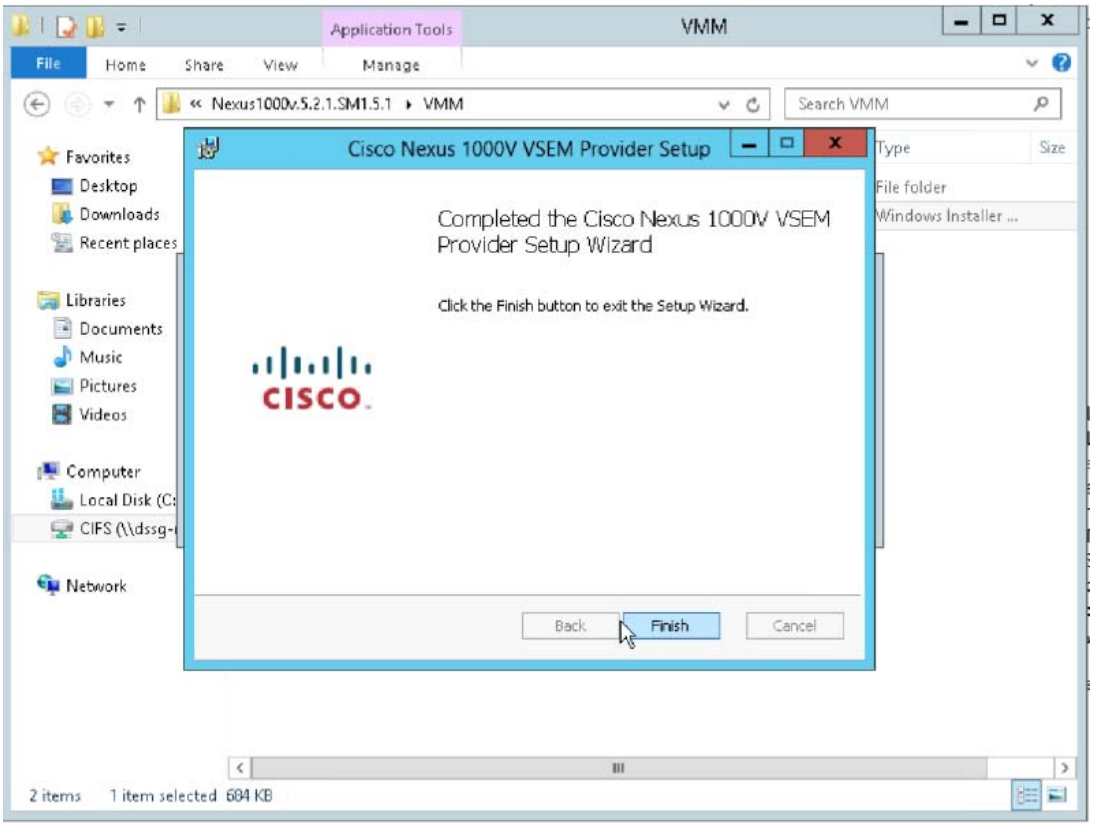


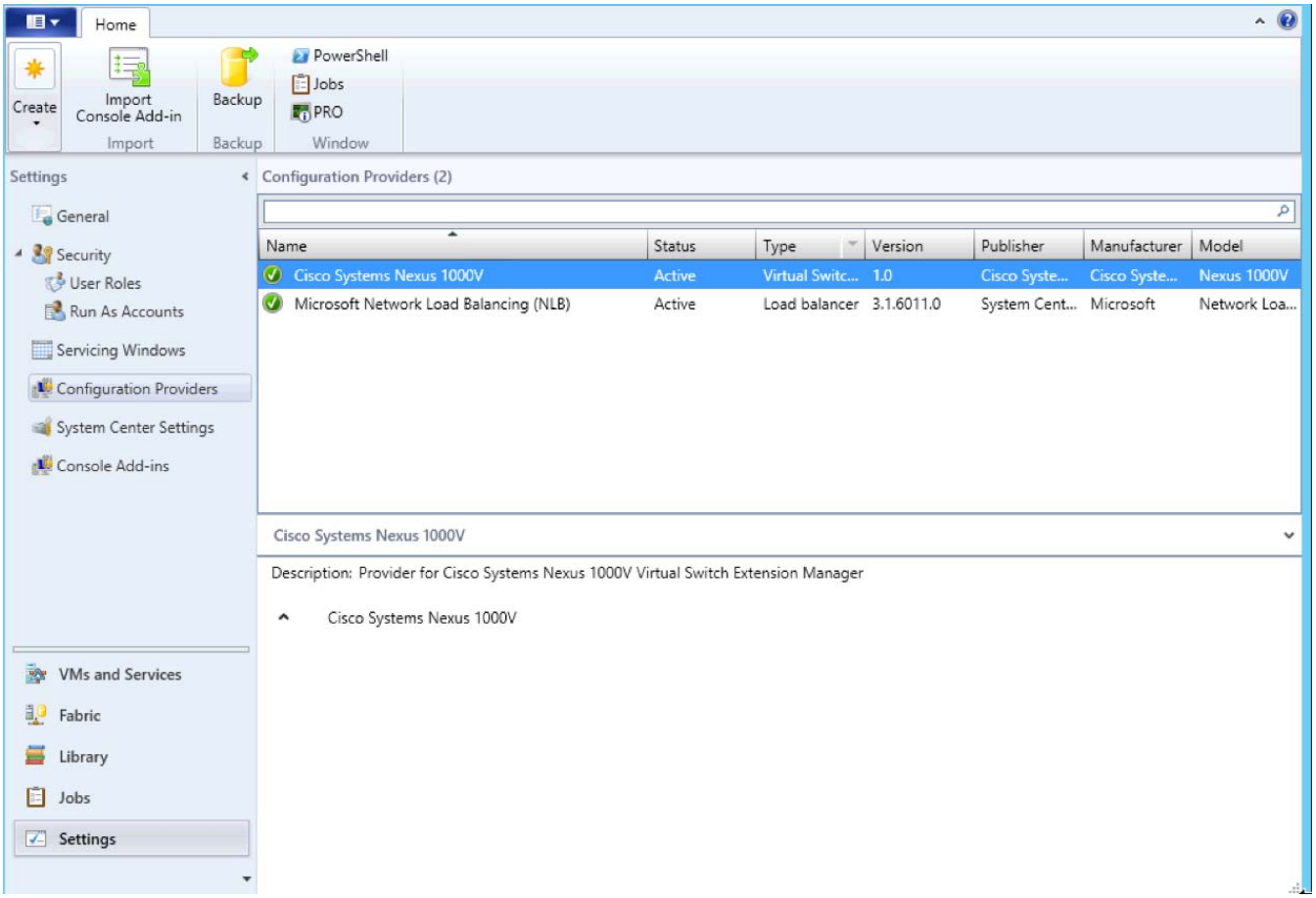
Figure 3-4 Select Finish when the Installer completes



Step 3 Verify that VSEM Provider is installed properly.

Go to **Settings > Configuration Providers**. Confirm that **Cisco Systems Nexus 1000V** is listed as a **Configuration Provider**.

Figure 3-5 Cisco VSEM Provider installed



Step 4 Copy VEM MSI to SCVMM repository.

The VEM is an MSI file that must be placed in the following location on the SCVMM server: **ALLUSERSPROFILE%\Switch Extension Drivers**, for example, **C:\ProgramData\Switch Extension Drivers**. SCVMM uses the MSI file during the Add host operation to install VEM code on the host.

Note Do not install VEM code on the SCVMM server; only copy the file to the specified location.

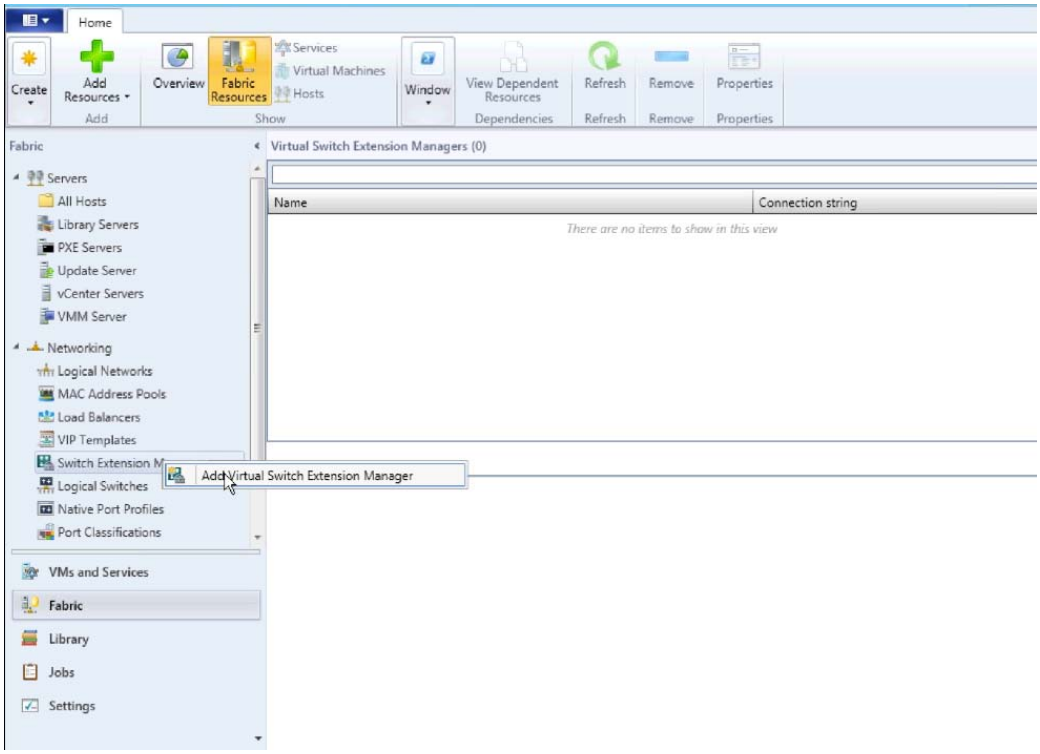
Step 5 Add VSEM (Connect SCVMM to VSM).

The following procedures add the VSEM that was just installed. This step is required to connect SCVMM to the VSM in Hyper-V.

In these steps, the login account and the MGMT IP address configured in the VSM are needed to establish the communication between SCVMM and the VSM. Once the VSEM is added, the configuration that was created in the CLI of the VSM can be pulled in the SCVMM.

a. Right-click **Switch Extension Manager** and select **Virtual Switch Extension Manager**..

Figure 3-6 Add VSEM

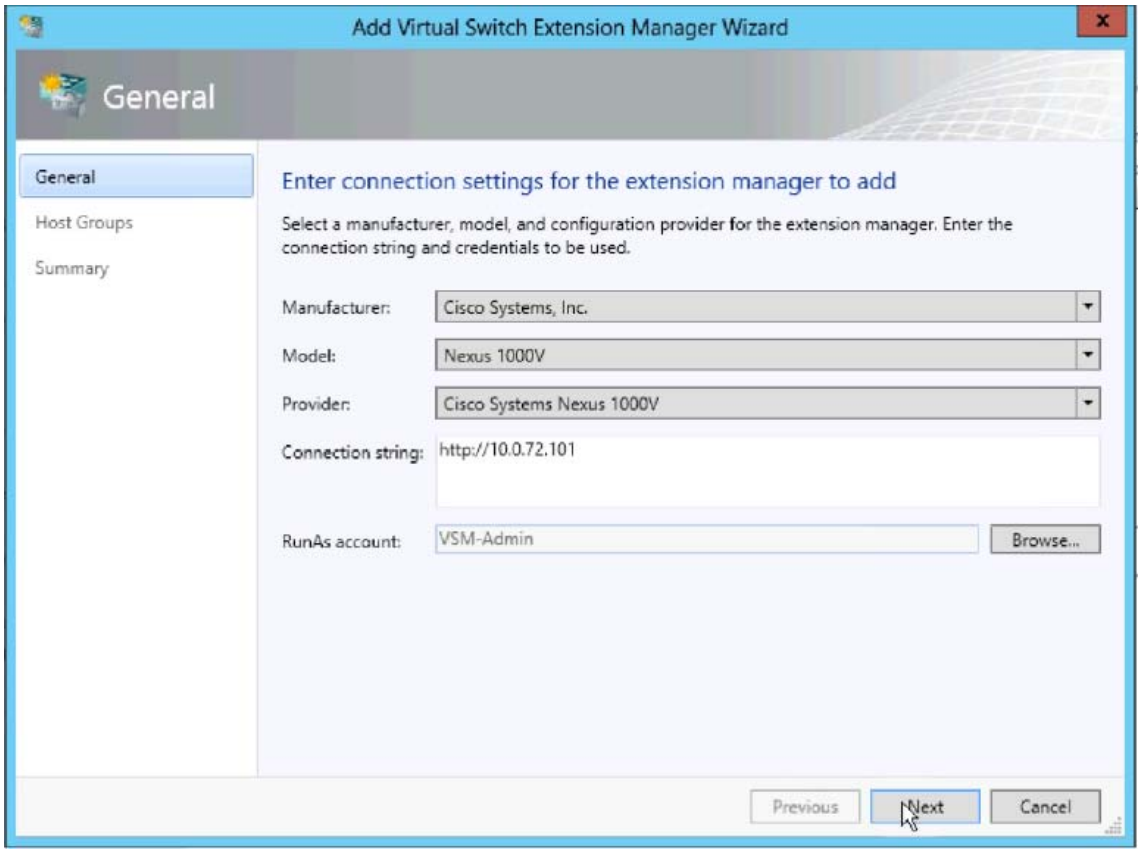


b. Add the Connection string and select **Run As Account.**

10.0.72.101 is the IP address of the VSM created on the Nexus 1110x.

The created account uses the login credentials required to log in to VSM.

Figure 3-7 Add VSEM Wizard



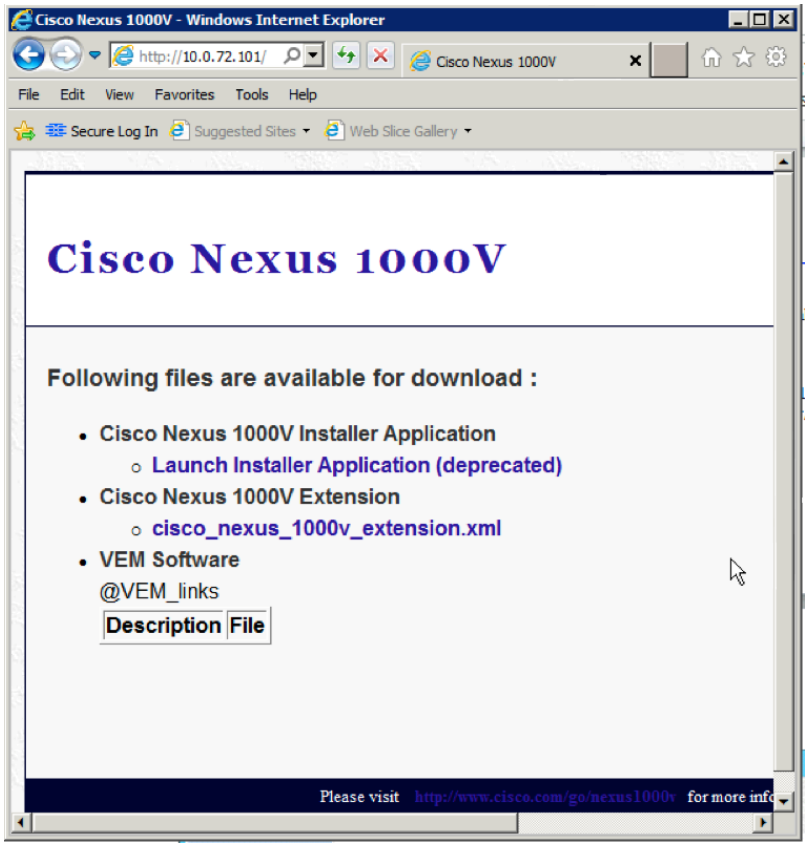
Refer to Installing Cisco Nexus 1000v for Microsoft Hyper-V for more information about creating a **Run As Account**.

c. Verify that no additional configuration, such as proxy, is required.

Open a browser and test the connection to the VSM. Browse to http://<VSM IP Address>.

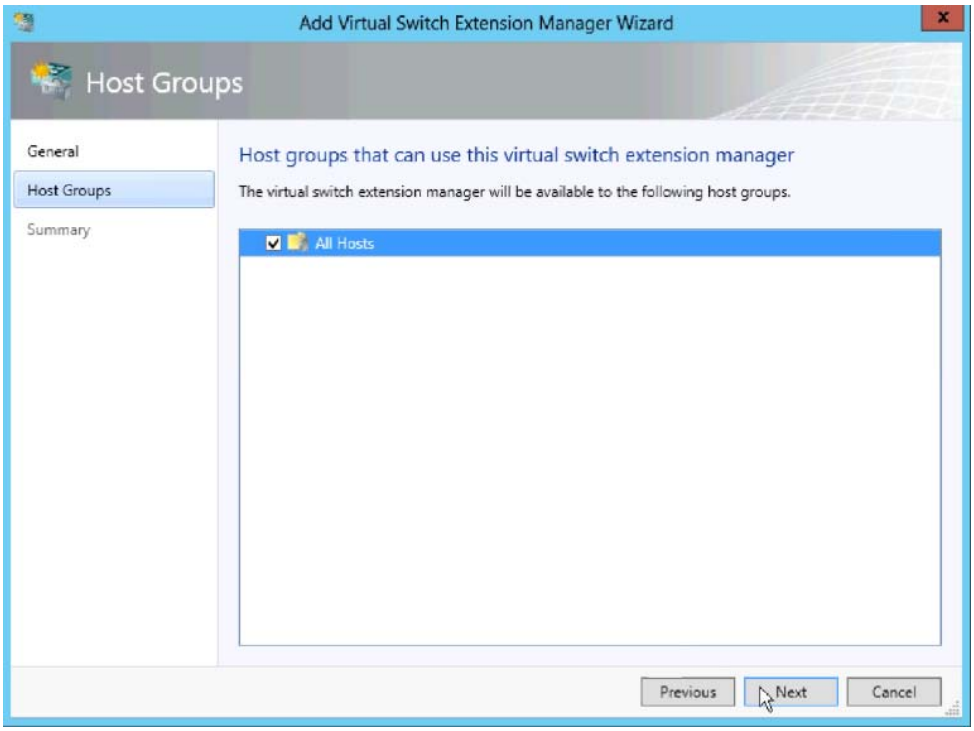
Output similar to Figure 3-5 should be seen:

Figure 3-8 Browse to VSM



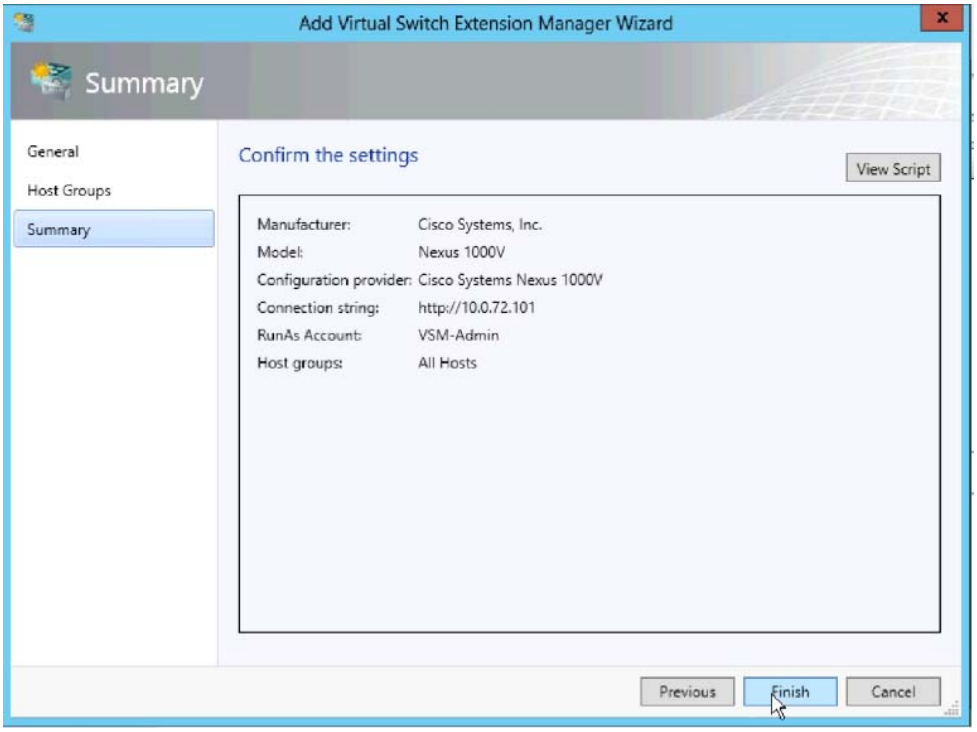
d. Select the host group to which the VSEM is available.

Figure 3-9 Add VSEM Wizard All Hosts



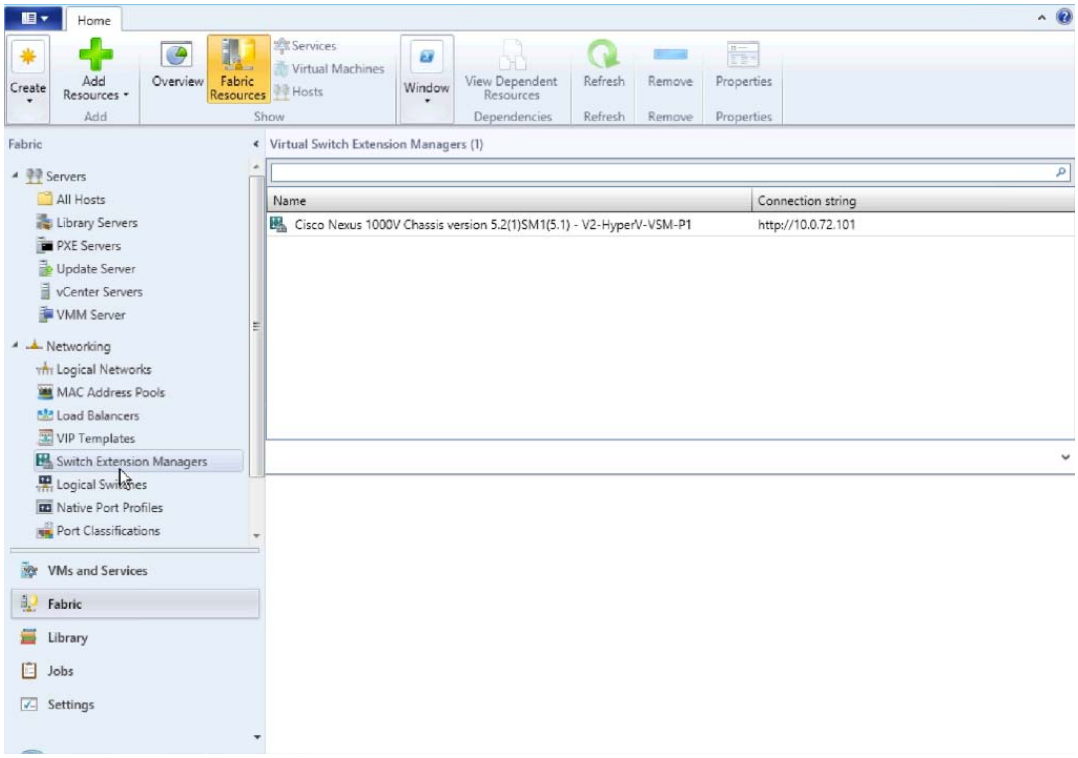
e. Confirm the VSEM settings and click **Finish.**

Figure 3-10 Add VSEM Wizard Confirm Settings



f. Verify that Virtual Switch Extension Manager is installed.

Figure 3-11 Verify VSEM is installed

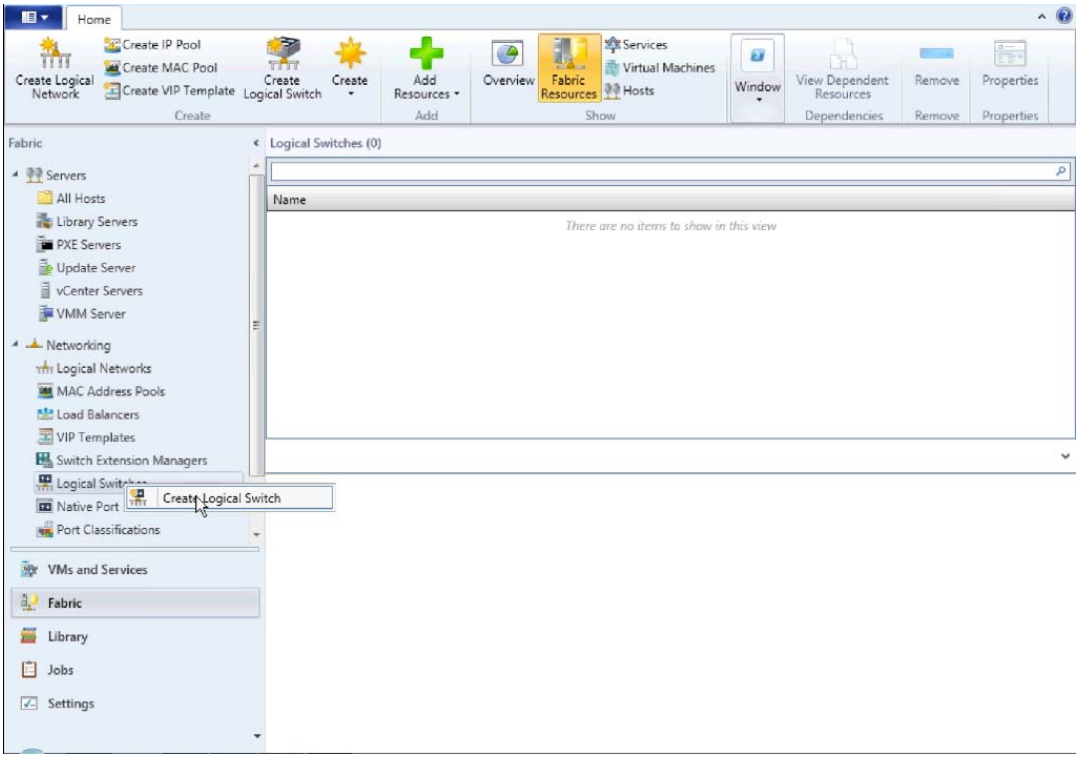


Step 6 Create Logical Switch in SCVMM.

After VSEM is added (Step 5), do the following:

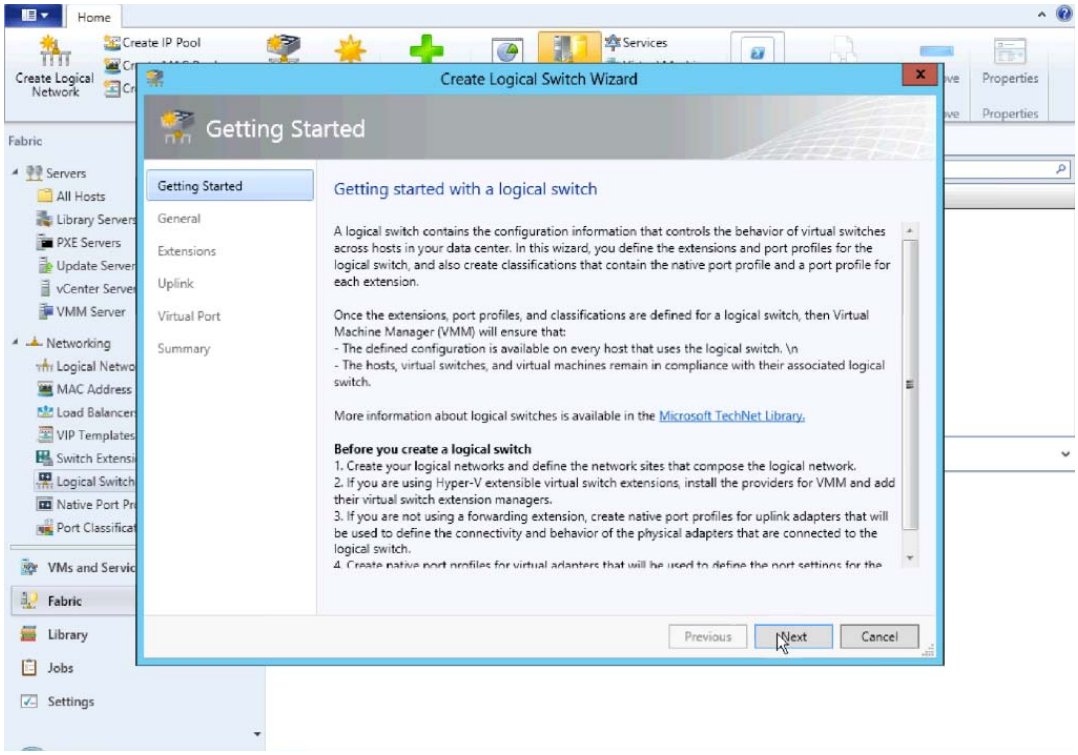
1. Create a logical switch on VMM using VSEM.
2. Define extensions and port profiles for the logical switch.
3. Create classifications containing the native port profile and a port profile for each extension.
   a. Right-click **Logical Switch** and select **Create Logical Switch**.

Figure 3-12 Create Logical Switch



b. Read the text and click **Next**.

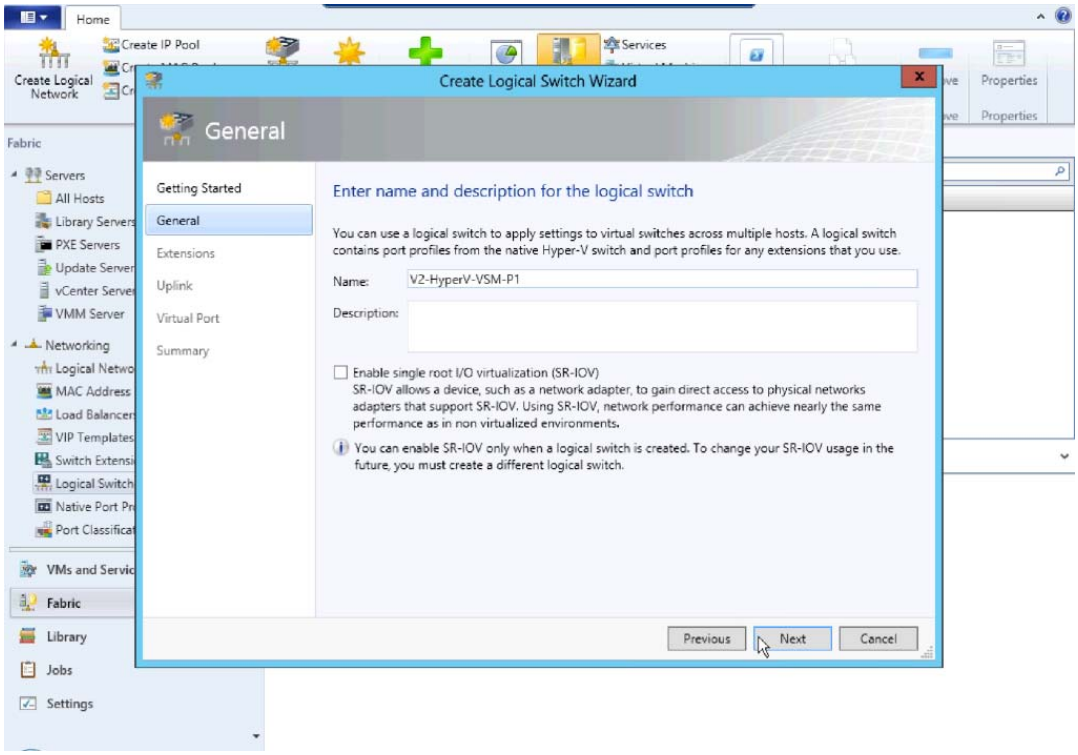
Figure 3-13 Create Logical Switch Getting Started



c. Name the logical switch.

In this case, the hostname of the VSM was used. Use defaults for SR-IOV.

Figure 3-14 Create Logical Switch Name



d. Check the previously configured VSEM (V2-HyperV-VSM-P1) and click **Next**.

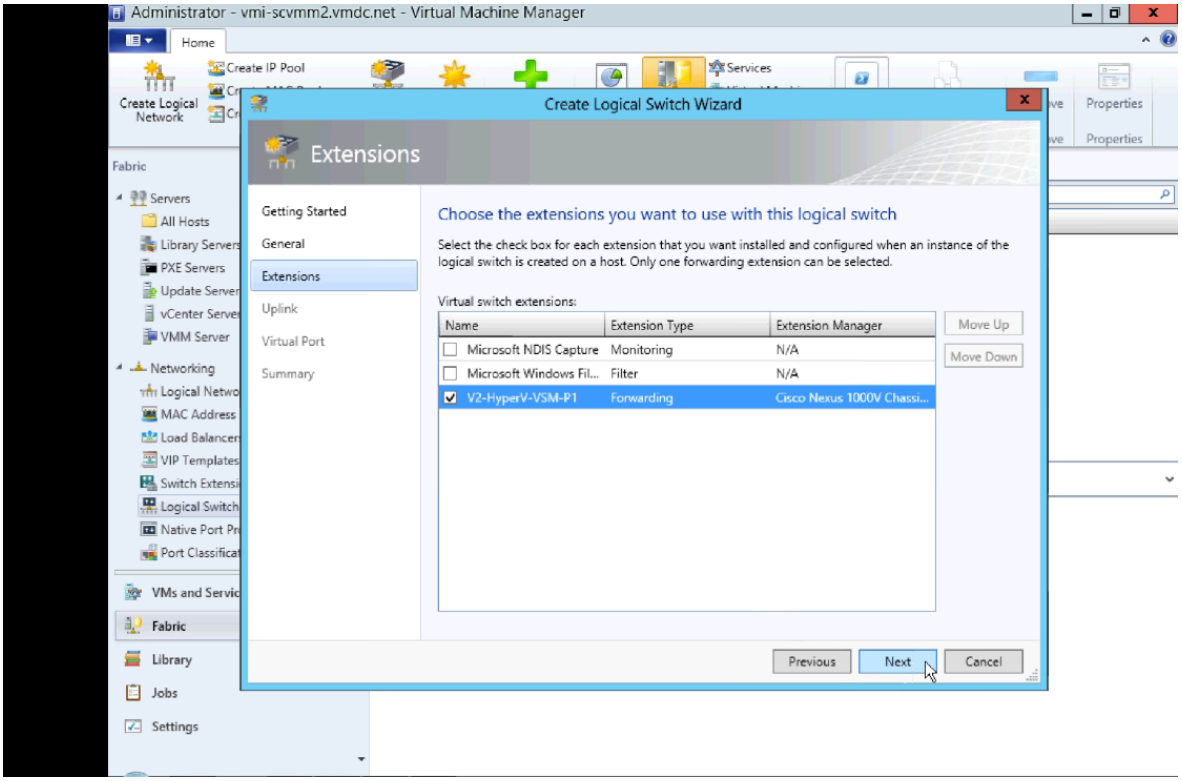
The VSEM has the following attributes:

Extension type: Forwarding

Extension Manager: Cisco Nexus 1000V Chassis

Only one virtual switch extension can be selected.

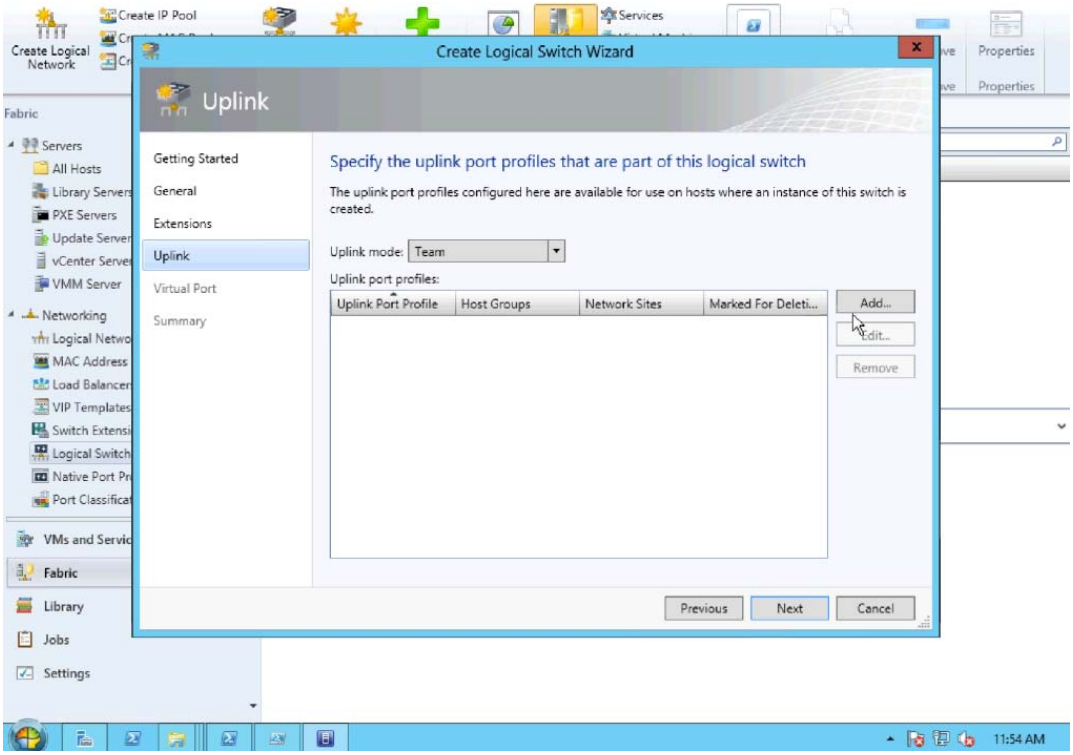
Figure 3-15 Create Logical Switch Select VSEM



e. Select **Team** in the uplink mode field and click **Add** to add the uplink port profile**.**

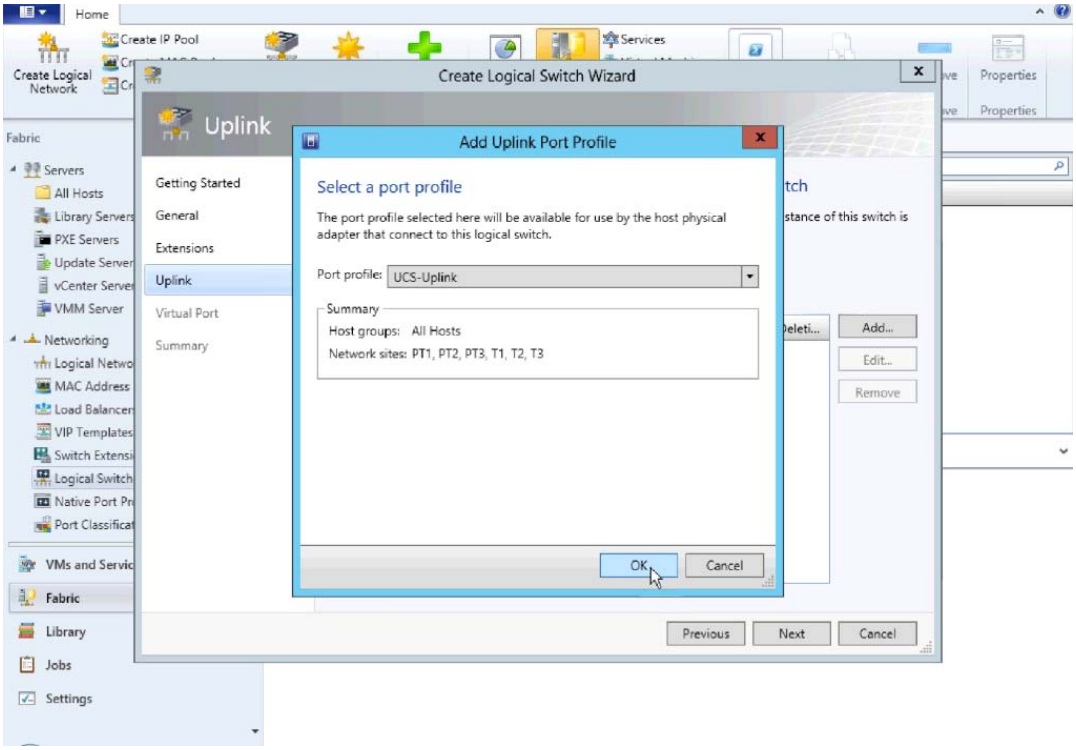
Note The mode should always be **Team**, whether using a single uplink or multiple uplinks.

Figure 3-16 Create Logical Switch Select Add Uplink



f. Select the uplink port profile and click **OK**.

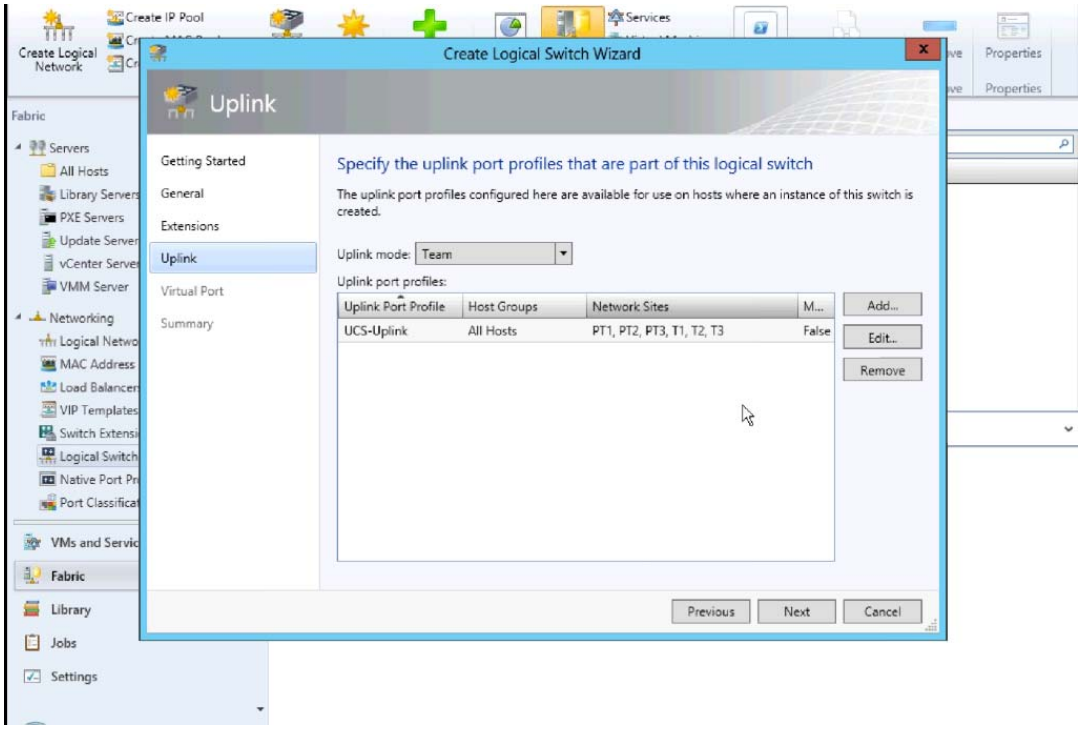
Figure 3-17 Add Uplink Port Profile



g. Confirm the uplink port profile settings and click **Next**.

By default, the host group **All Hosts** is created in Hyper-V. The network sites PT1, PT2, PT3, T1, T2 and T3 were created during Nexus 1000V CLI configuration.

Figure 3-18 Create Logical Switch Note Host Groups and the Network site

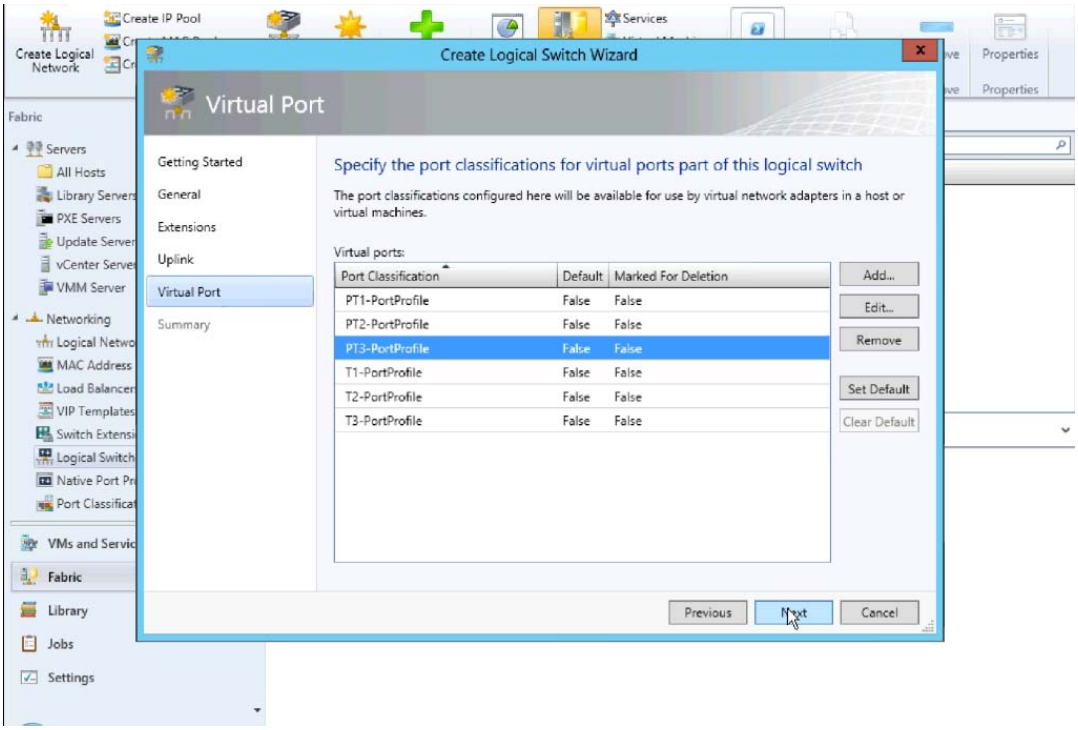


h. Specify the Port Classifications and click **Next**.

Port Classifications must be created in SCVMM and linked to port-profiles created in the VSM. The port-profiles were created previously in the "Nexus 1000V Switch for Microsoft Hyper-V VSM CLI Configuration" section on page 3-2; one port classification per port profile was created. When adding VMs to the logical switch, the port classification and VM network are selected when configuring network adapters (see VM Deployment).

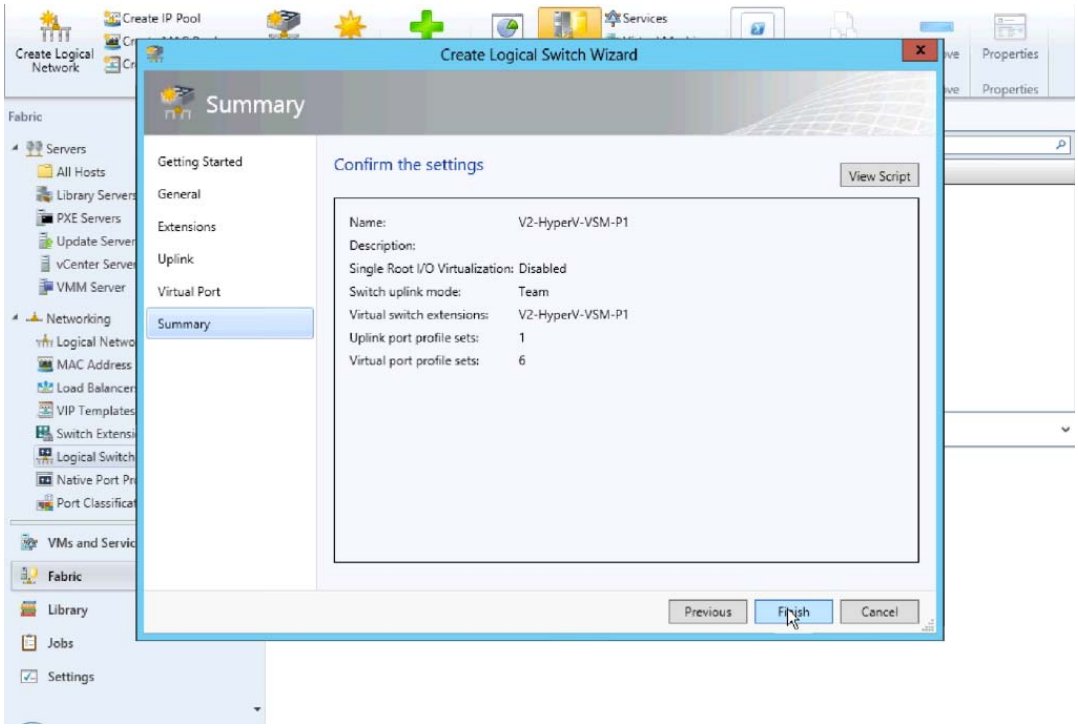
Refer to **Creating Logical Switch in SCVMM** in Installing Cisco Nexus 1000V for Microsoft Hyper-V for additional guidance for creating port classifications.

Figure 3-19 Create Logical Switch Specify the Port Classifications



i. In the **Summary** panel, confirm the settings and click **Finish** to create the logical switch.

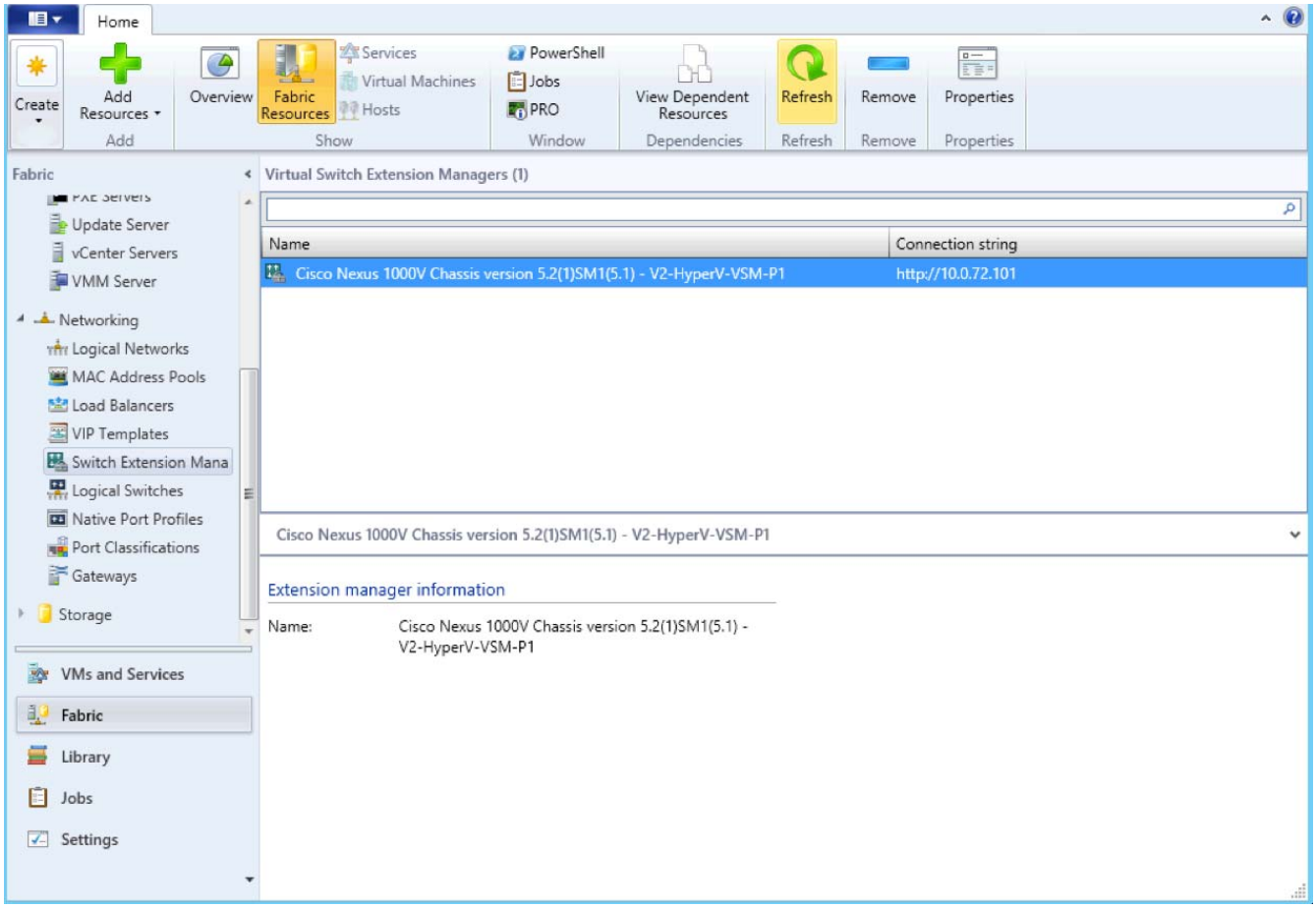
Figure 3-20 Create Logical Switch Specify Confirm Settings



j. Manually refresh the VSEM.

After the Nexus 1000V logical switch is created, manually refresh VSEM to force the updates to appear in SCVMM.

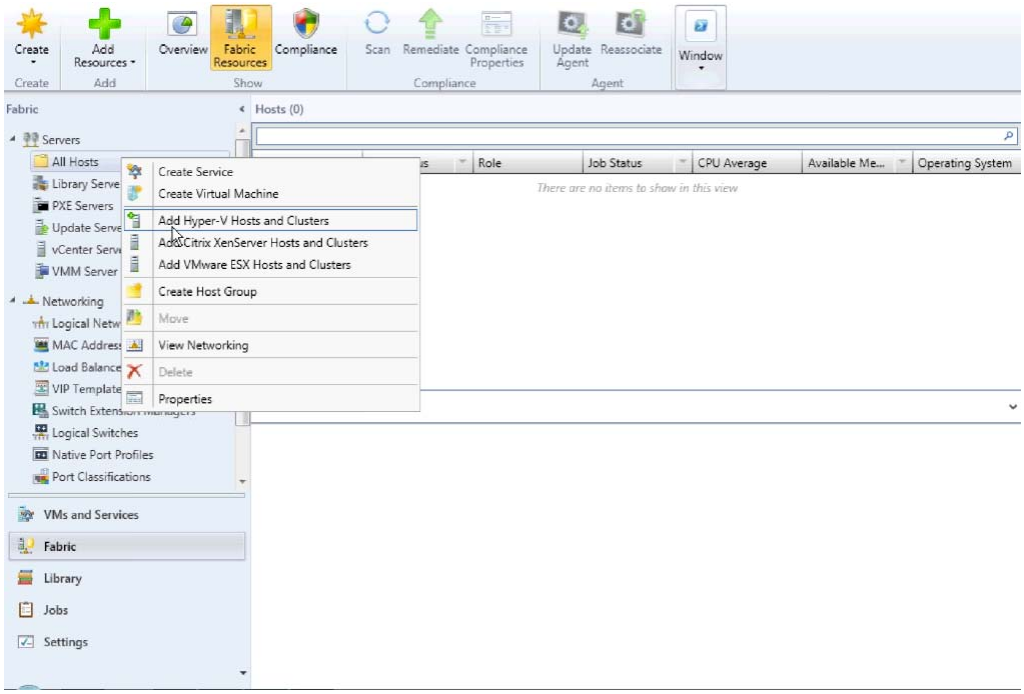
Figure 3-21 Manual Refresh of the VSEM



Step 7 Add VEMs (Hosts) to the Nexus 1000V.

a. Right-click **All Hosts** and select **Add Hyper-V Hosts and Clusters**..

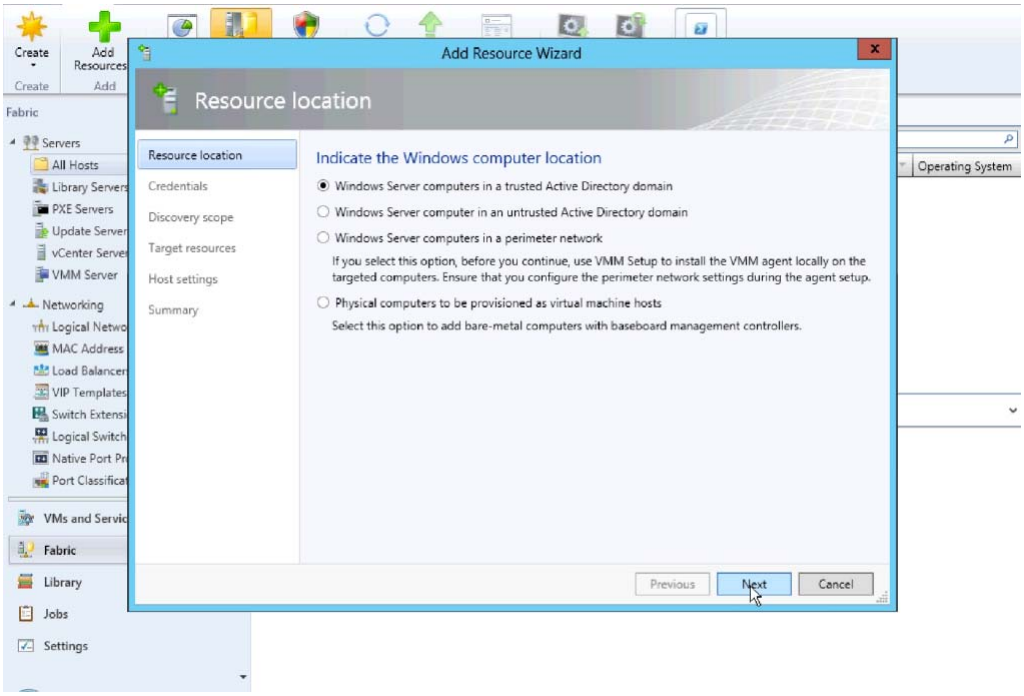
Figure 3-22 Add Hyper-V Hosts



b. Select the appropriate computer location and click **Next**.

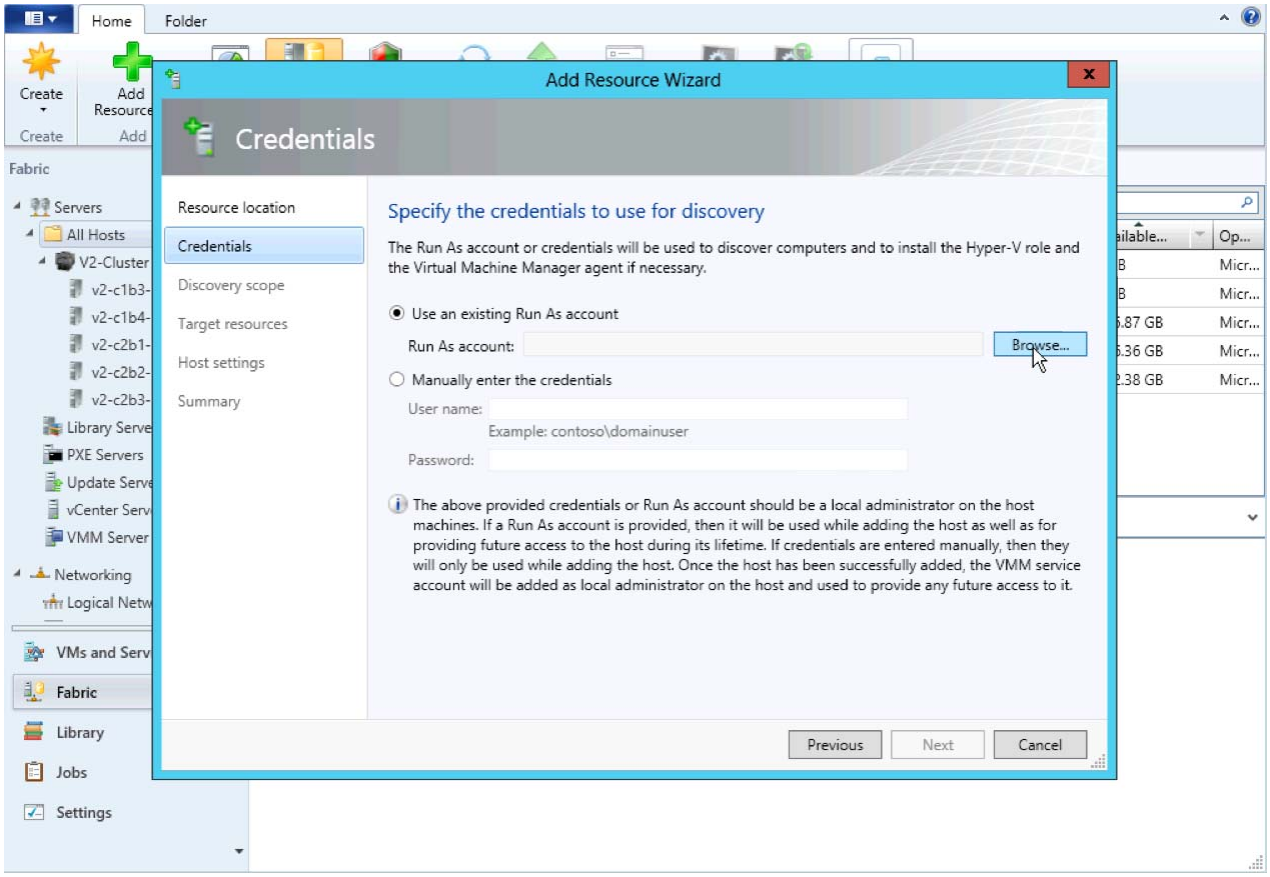
All hosts in the test bed were in a trusted Active Directory domain.

Figure 3-23 Add Hyper-V Hosts Windows Computer Location



c. Click **Browse** to see a list of **Run As Accounts**.

Figure 3-24 Add Hyper-V Hosts Specify Credentials

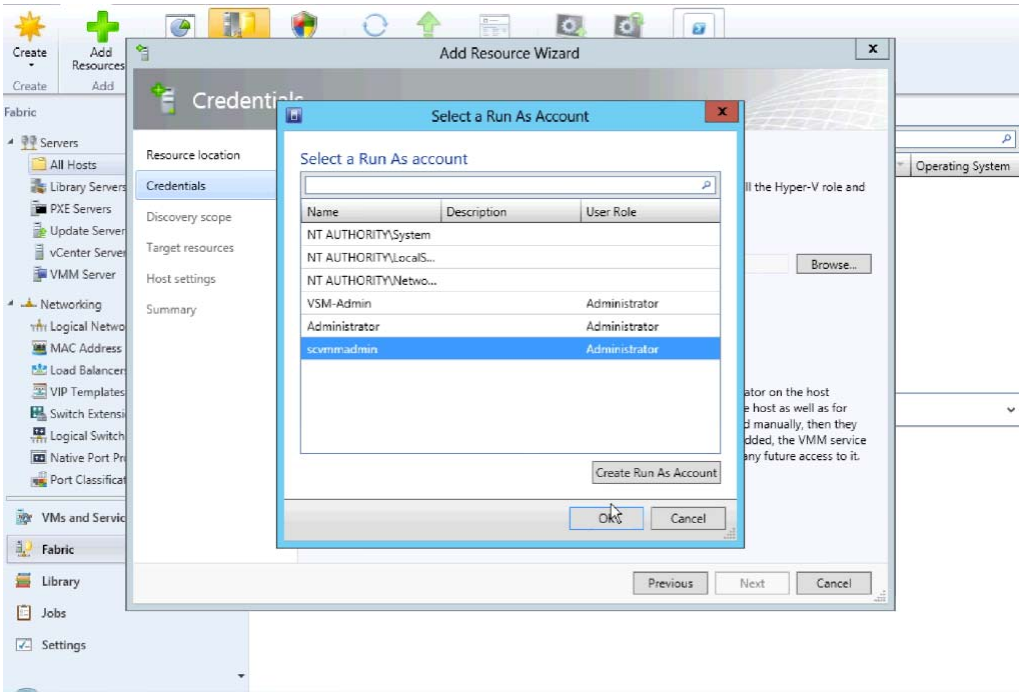


d. Select the **Run As account** created during the Hyper-V install.

The account is different than the **Run As account** used to install VSEM. The scvmmadmin account was created in Active Directory and is a domain administrator account for the local domain.

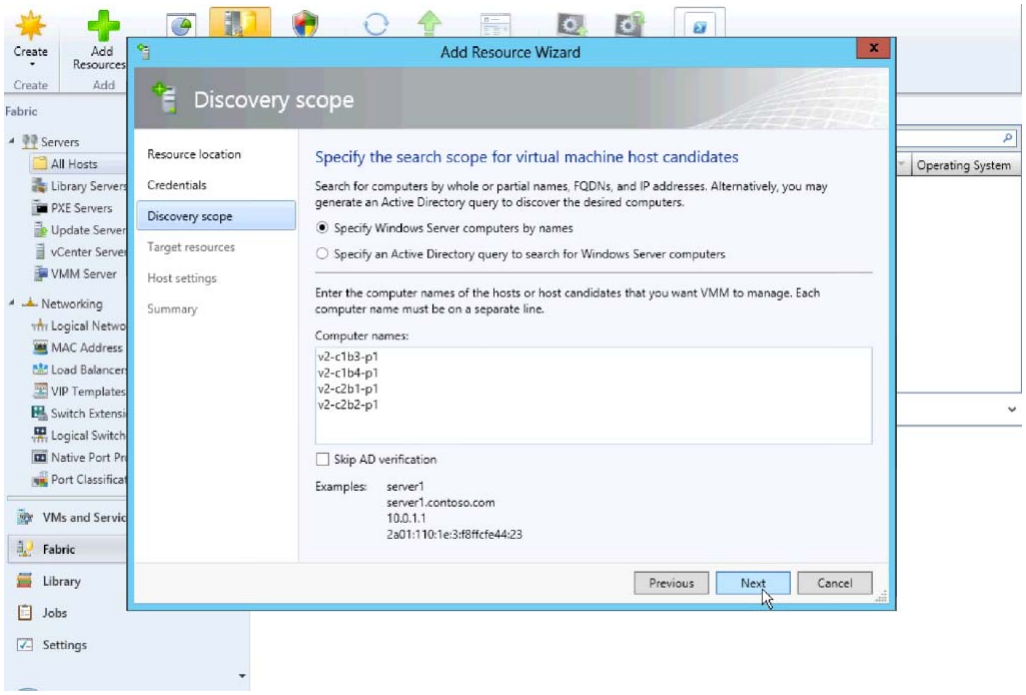
See the "Microsoft Windows Server 2012 Installation" section on page 2-6 for more information about the scvmmadmin account.

Figure 3-25 Add Hyper-V Hosts Select Run As Account



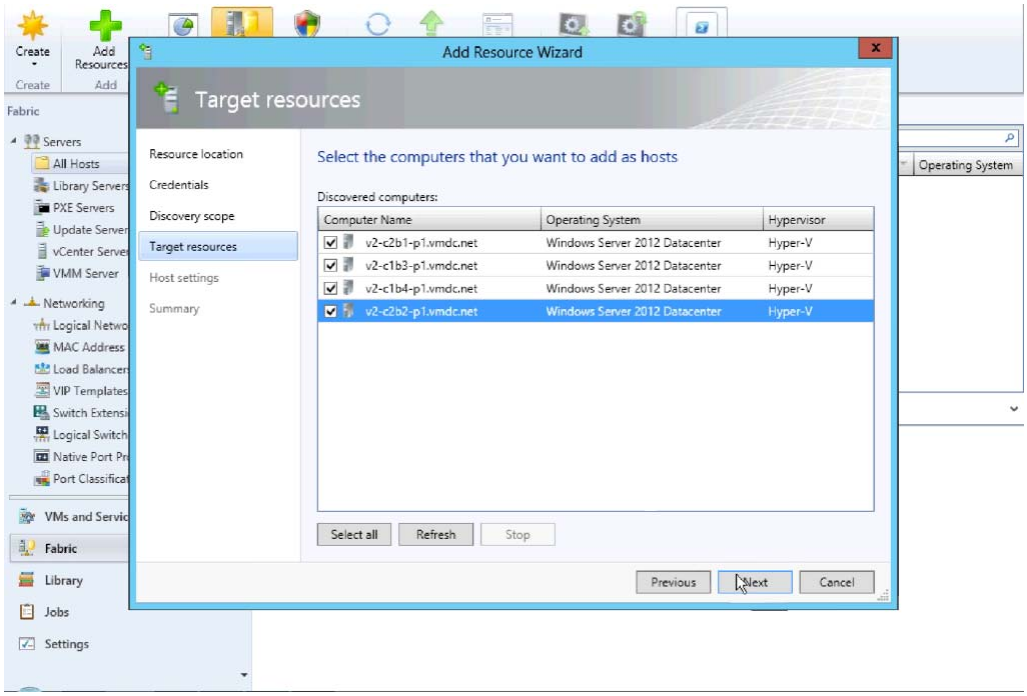
e. Enter the hostname of each host to add as a VEM and click **Next**.

Figure 3-26 Add Hyper-V Hosts Enter Hostnames



f. After hosts are discovered, select each host to add and click **Next**.

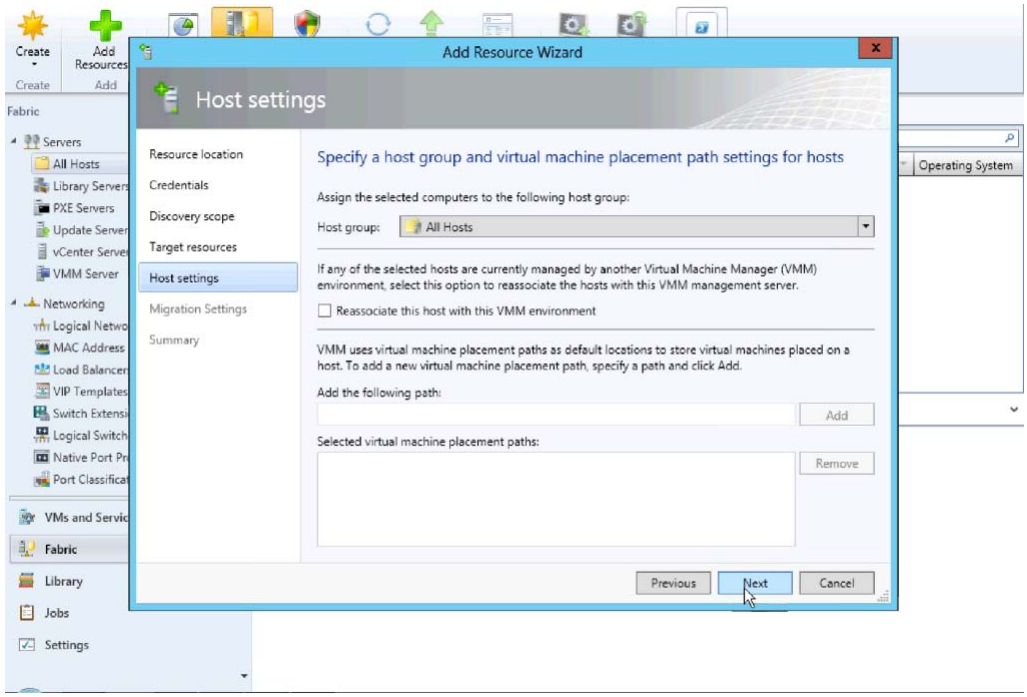
Figure 3-27 Add Hyper-V Hosts Select the Hosts



g. Assign hosts to a host groups.

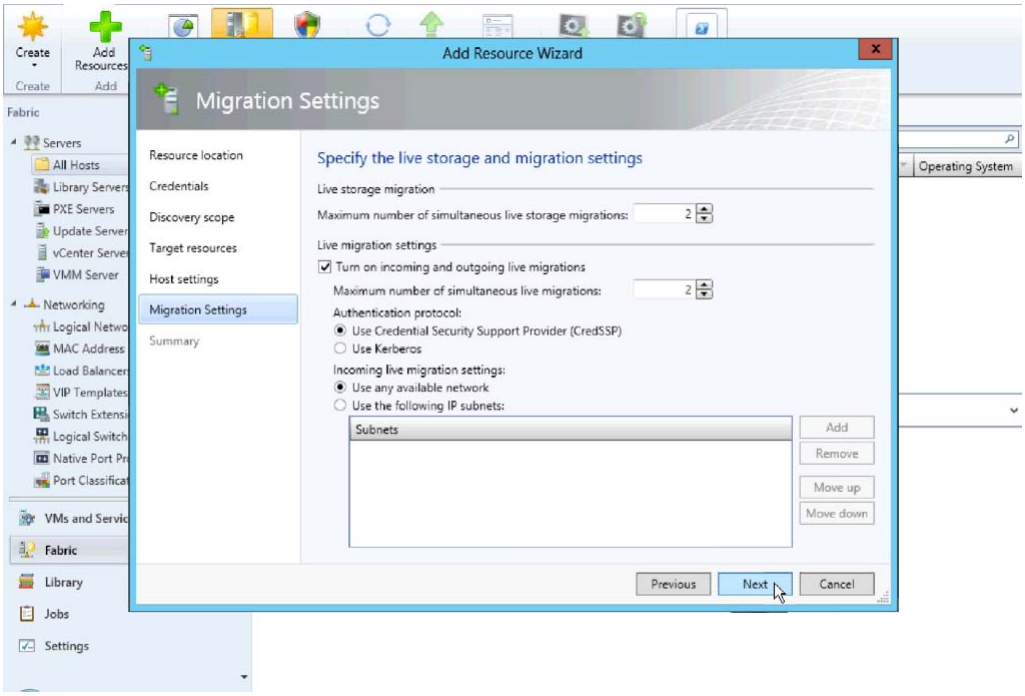
Leave **Reassociate this host with the VMM environment** unchecked and click **Next**.

Figure 3-28 Add Hyper-V Hosts Assign the Host Group



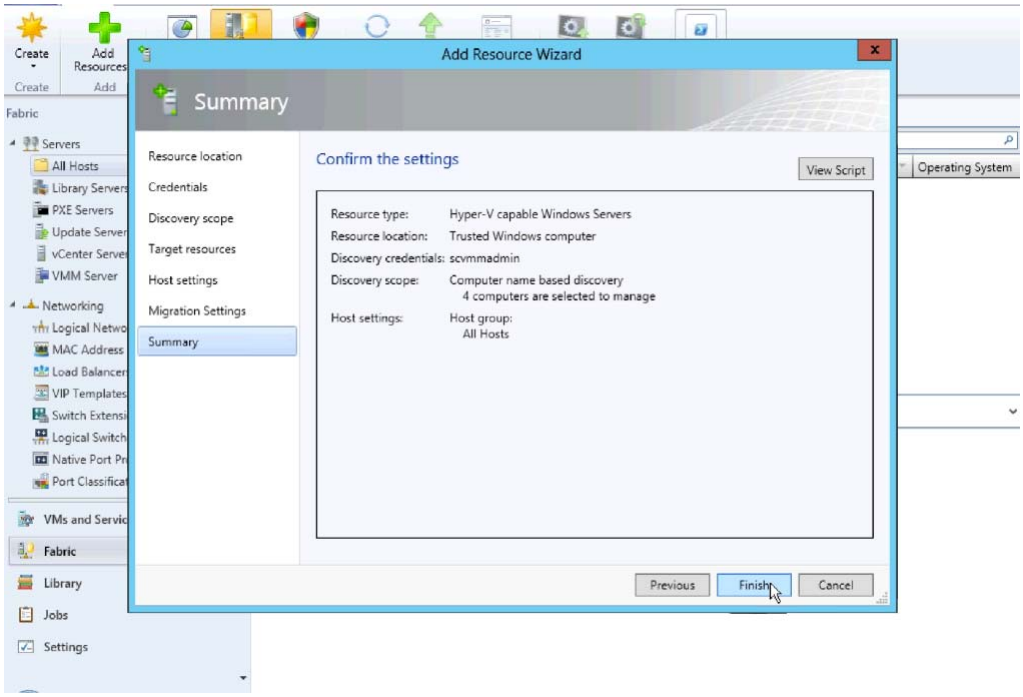
h. Enable Live Migration and click **Next**.

Figure 3-29 Add Hyper-V Hosts Enable Live Migration



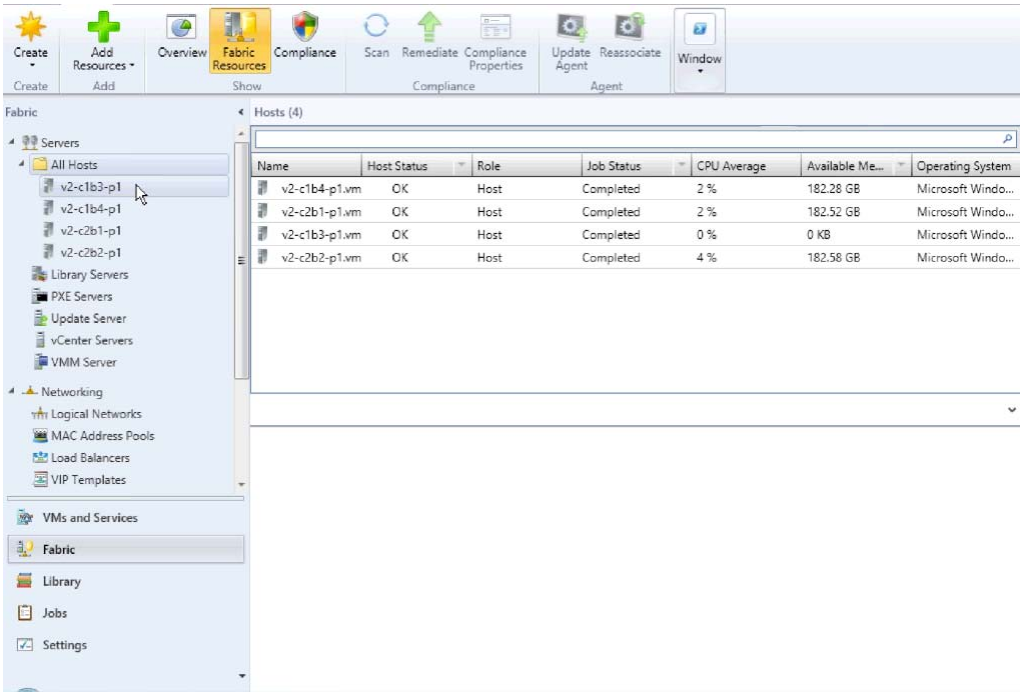
i. Confirm the Settings and click **Finish**.

Figure 3-30 Add Hyper-V Hosts Confirm Settings



j. Verify All Hosts are seen in the **All Hosts** group.

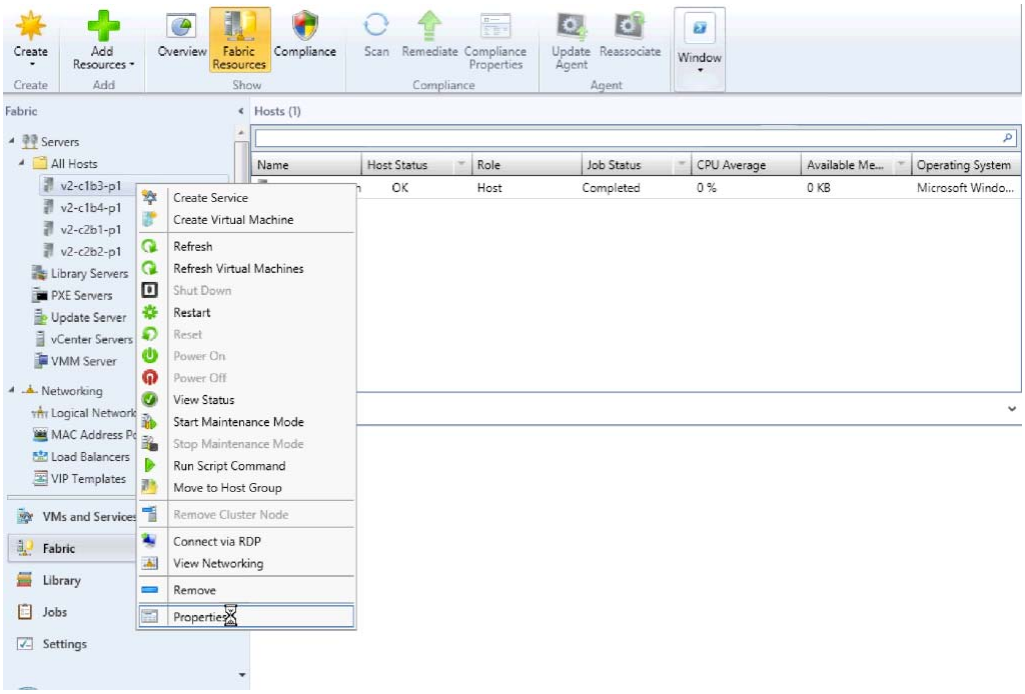
Figure 3-31 Add Hyper-V Hosts Verify All Hosts



Step 8 Add Each Host to Logical switch.

a. Right-click the host to be added and select **Properties**.

Figure 3-32 Host Properties

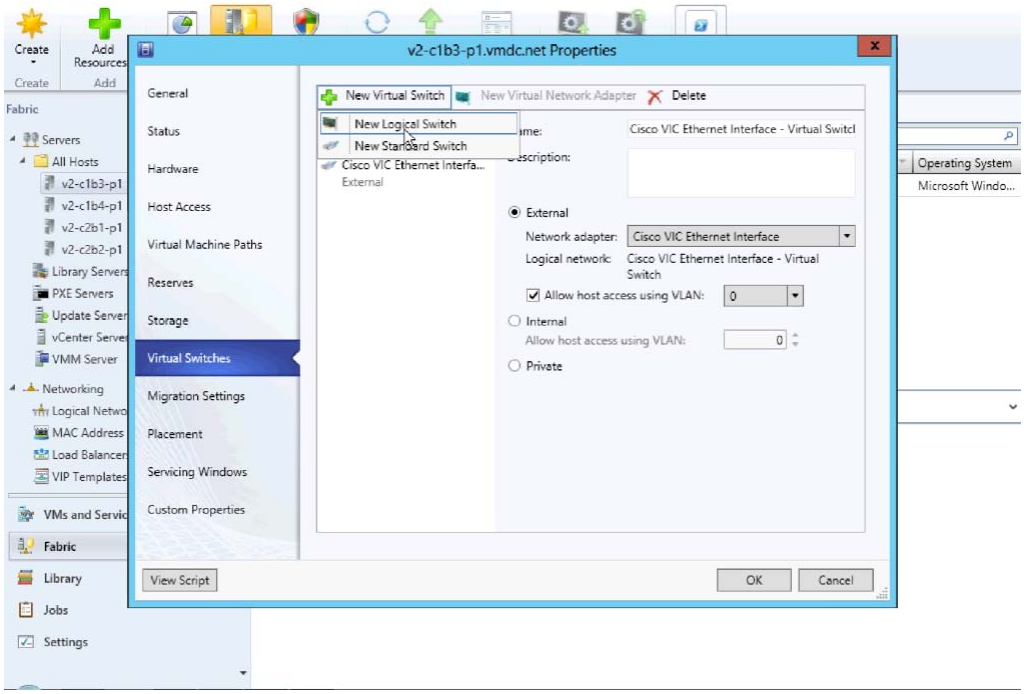


b. Add New Logical Switch.

In the **Host Properties > Virtual Switches** window, select **New Virtual Switch** and **New Logical Switch** to add the host to the Nexus 1000V.

As seen in Figure 3-33, a standard External switch was already created for management. In Hyper-V, multiple switches can exist on the host.

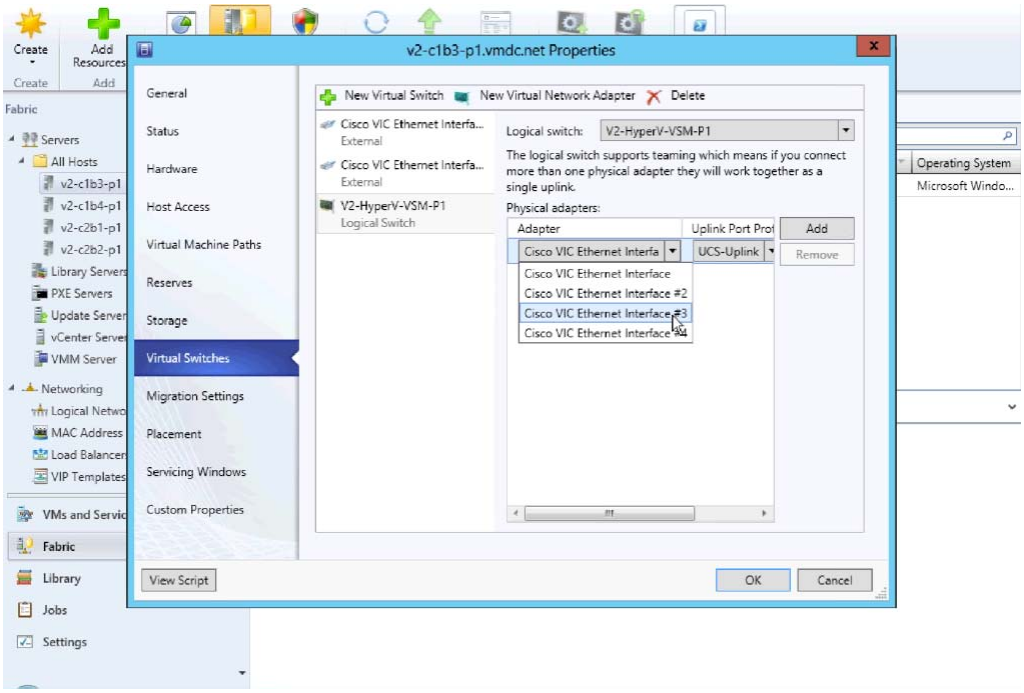
Figure 3-33 Host Properties New Logical Switch



c. Add physical adapters to the logical switch team.

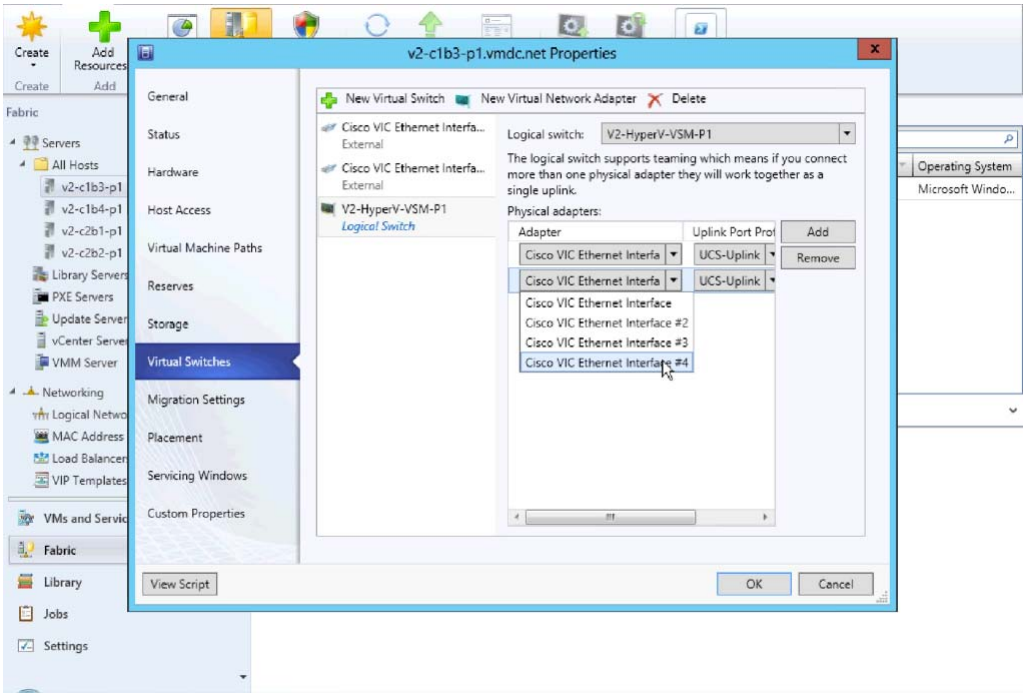
There are two adapters, VIC Ethernet interface 3 and VIC Ethernet interface 4 that will be used on each host. Add these to the logical switch.

Figure 3-34 Host Properties Add Physical Adapter 1



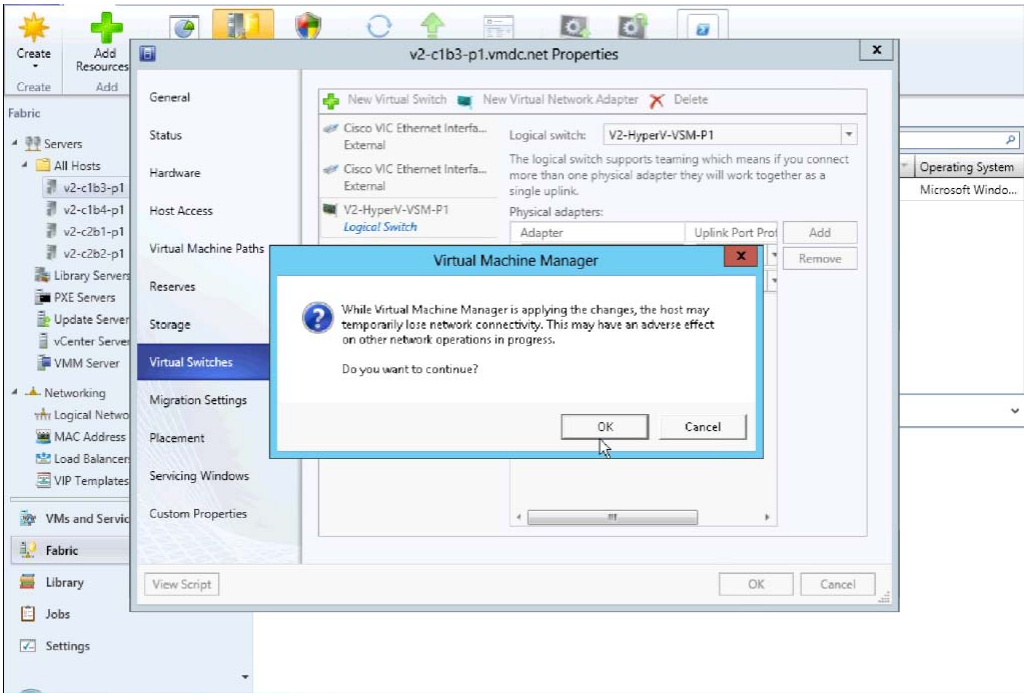
Add the second physical adapter 2 and hit OK.

Figure 3-35 Host Properties Add Physical Adapter 2



d. Click **OK** to continue to add host to the logical switch.

Figure 3-36 Host Properties Continue to Add Host to Logical Switch



e. Verify that the VEM is installed on the VSM.

Figure 3-37 shows the output seen on the VSM when the VEM is added to the Logical switch.

Figure 3-37 Host added as a VEM

```
V2-HyperV-VSM-P1(config-net-seg)# sho mod
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------  -----------------  ----------
1    0      Virtual Supervisor Module        Nexus1000V         active *
2    0      Virtual Supervisor Module        Nexus1000V         ha-standby
4    288    Virtual Ethernet Module          NA                 ok
5    288    Virtual Ethernet Module          NA                 ok
6    288    Virtual Ethernet Module          NA                 ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    5.2(1)SM1(5.1)    0.0
2    5.2(1)SM1(5.1)    0.0
4    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)
5    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)
6    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA
5    02-00-0c-00-05-00 to 02-00-0c-00-05-80  NA
6    02-00-0c-00-06-00 to 02-00-0c-00-06-80  NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.0.72.101      NA                                   NA
2    10.0.72.101      NA                                   NA
4    10.0.65.4        627C87AB-FABE-E211-0025-B59102200004  V2-C1B4-P1
5    10.0.65.1        627C87AB-FABE-E211-0025-B59102200001  V2-C2B1-P1
6    10.0.65.2        627C87AB-FABE-E211-0025-B59102200002  V2-C2B2-P1

* this terminal session
V2-HyperV-VSM-P1(config-net-seg)#
V2-HyperV-VSM-P1(config-net-seg)#
V2-HyperV-VSM-P1(config-net-seg)# 2013 Jun 10 16:00:33 V2-HyperV-VSM-P1 %VEM_MGR-2-VEM_MGR_DETECTED: Host V2-C1B3-P1 detected as module 3
2013 Jun 10 16:00:33 V2-HyperV-VSM-P1 %VEM_MGR-2-MOD_ONLINE: Module 3 is online

V2-HyperV-VSM-P1(config-net-seg)#
V2-HyperV-VSM-P1(config-net-seg)#
```

f. After all hosts were added to the logical switch, they are seen as VEMs in the VSM. Execute **show module** on the VSM to verify these hosts are seen as VEMs.

Figure 3-38 All Host Added as a VEM

```
V2-HyperV-VSM-P1(config-net-seg)#
V2-HyperV-VSM-P1(config-net-seg)# sho mod
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------  -----------------  ------------
1    0      Virtual Supervisor Module        Nexus1000V         active *
2    0      Virtual Supervisor Module        Nexus1000V         ha-standby
3    288    Virtual Ethernet Module          NA                 ok
4    288    Virtual Ethernet Module          NA                 ok
5    288    Virtual Ethernet Module          NA                 ok
6    288    Virtual Ethernet Module          NA                 ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    5.2(1)SM1(5.1)    0.0
2    5.2(1)SM1(5.1)    0.0
3    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)
4    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)
5    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)
6    5.2(1)SM1(5.1)    Windows Server 2012 - Datacenter (6.2.9200. 6.30)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA
5    02-00-0c-00-05-00 to 02-00-0c-00-05-80  NA
6    02-00-0c-00-06-00 to 02-00-0c-00-06-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.0.72.101      NA                                    NA
2    10.0.72.101      NA                                    NA
3    10.0.65.3        627C87AB-FABE-E211-0025-B59102200003  V2-C1B3-P1
4    10.0.65.4        627C87AB-FABE-E211-0025-B59102200004  V2-C1B4-P1
5    10.0.65.1        627C87AB-FABE-E211-0025-B59102200001  V2-C2B1-P1
6    10.0.65.2        627C87AB-FABE-E211-0025-B59102200002  V2-C2B2-P1

* this terminal session
V2-HyperV-VSM-P1(config-net-seg)# sho mod
```

g. Verify interfaces are added to Logical Switch.

Because each host has two Cisco VIC Ethernet interfaces, two Ethernet interfaces per host are seen, along the port-channel interfaces.

These are:

```
Eth3/1
Eth3/2
Eth4/1
Eth4/2
Eth5/1
Eth5/2
Eth6/1
Eth6/2

Po1
Po2
Po3
Po4
```

These interfaces and port-channels can get verified by executing **show interface brief** on the VSM**:**

Figure 3-39 Show Interface Brief

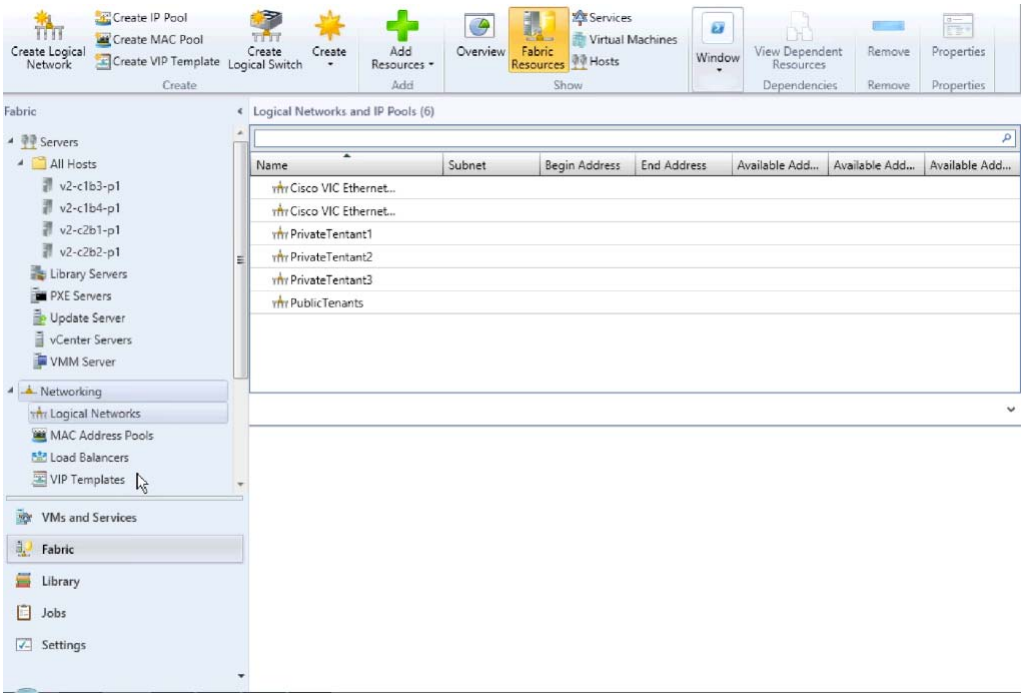
```
4    10.0.65.4        627C87AB-FABE-E211-0025-B59102200004  V2-C1B4-P1
5    10.0.65.1        627C87AB-FABE-E211-0025-B59102200001  V2-C2B1-P1
6    10.0.65.2        627C87AB-FABE-E211-0025-B59102200002  V2-C2B2-P1

* this terminal session
V2-HyperV-VSM-P1(config-net-seg)# sho int br

--------------------------------------------------------------------------------
Port      VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0     --           up     10.0.72.101                             1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/1        1       eth  trunk  up      none                     10G       1
Eth3/2        1       eth  trunk  up      none                     10G       1
Eth4/1        1       eth  trunk  up      none                     10G       2
Eth4/2        1       eth  trunk  up      none                     10G       2
Eth5/1        1       eth  trunk  up      none                     10G       3
Eth5/2        1       eth  trunk  up      none                     10G       3
Eth6/1        1       eth  trunk  up      none                     10G       4
Eth6/2        1       eth  trunk  up      none                     10G       4

--------------------------------------------------------------------------------
Port-channel VLAN    Type Mode   Status  Reason                   Speed     Protocol
Interface
--------------------------------------------------------------------------------
Po1           1       eth  trunk  up      none                      a-10G(D)  none
Po2           1       eth  trunk  up      none                      a-10G(D)  none
Po3           1       eth  trunk  up      none                      a-10G(D)  none
Po4           1       eth  trunk  up      none                      a-10G(D)  none

--------------------------------------------------------------------------------
Port      VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
control0  --           up     --                                      1000     1500
V2-HyperV-VSM-P1(config-net-seg)#
V2-HyperV-VSM-P1(config-net-seg)#
V2-HyperV-VSM-P1(config-net-seg)#
```

Step 9 VM Network Creation.

After the Nexus 1000V Switch for Microsoft Hyper-V Logical switch has been installed, the VM Networks can get created.

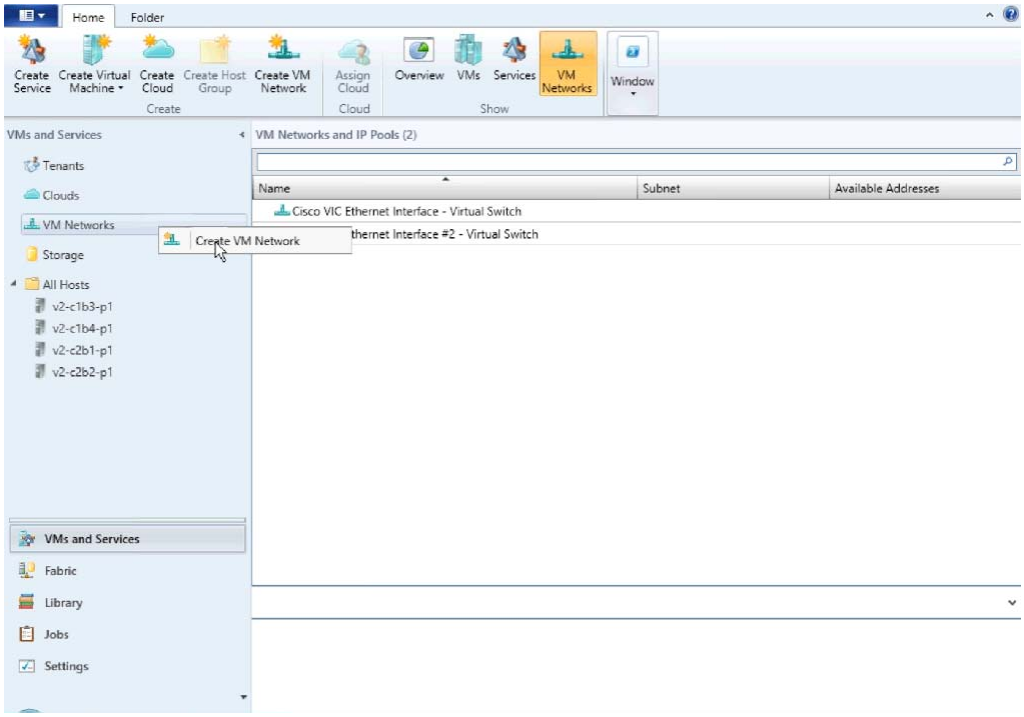
a. Verify the Logical Networks created on the N1000V are seen in Hyper-V.

Figure 3-40 Logical Networks



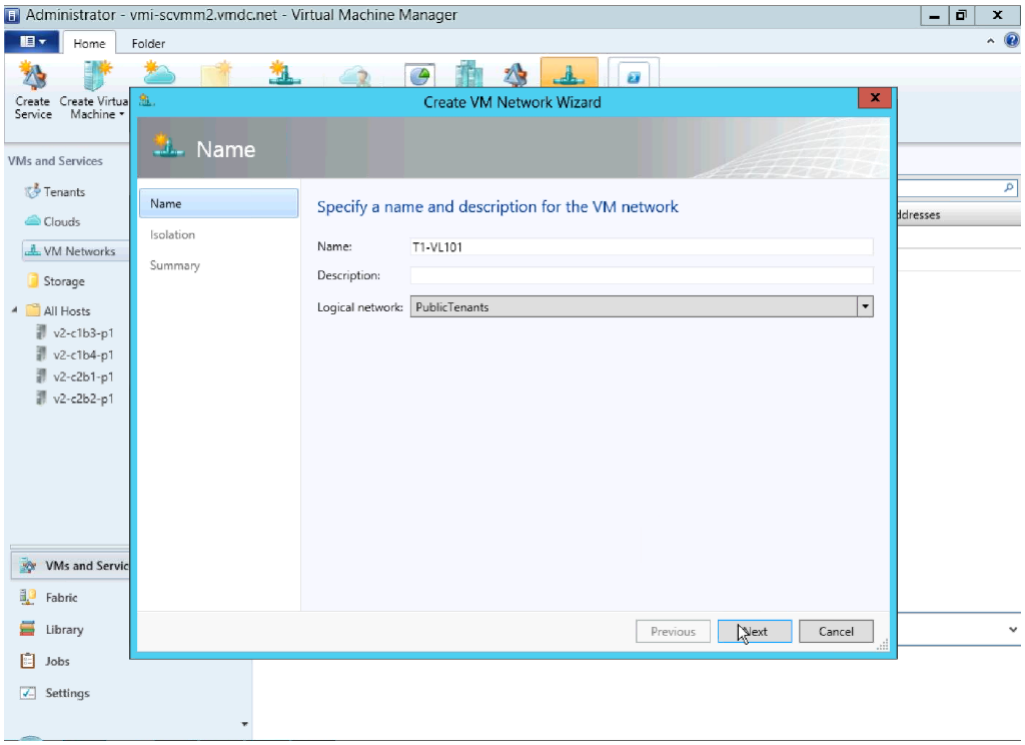
b. Right-click **VM Network** and select **Create VM Network**.

Figure 3-41 Create VM Network



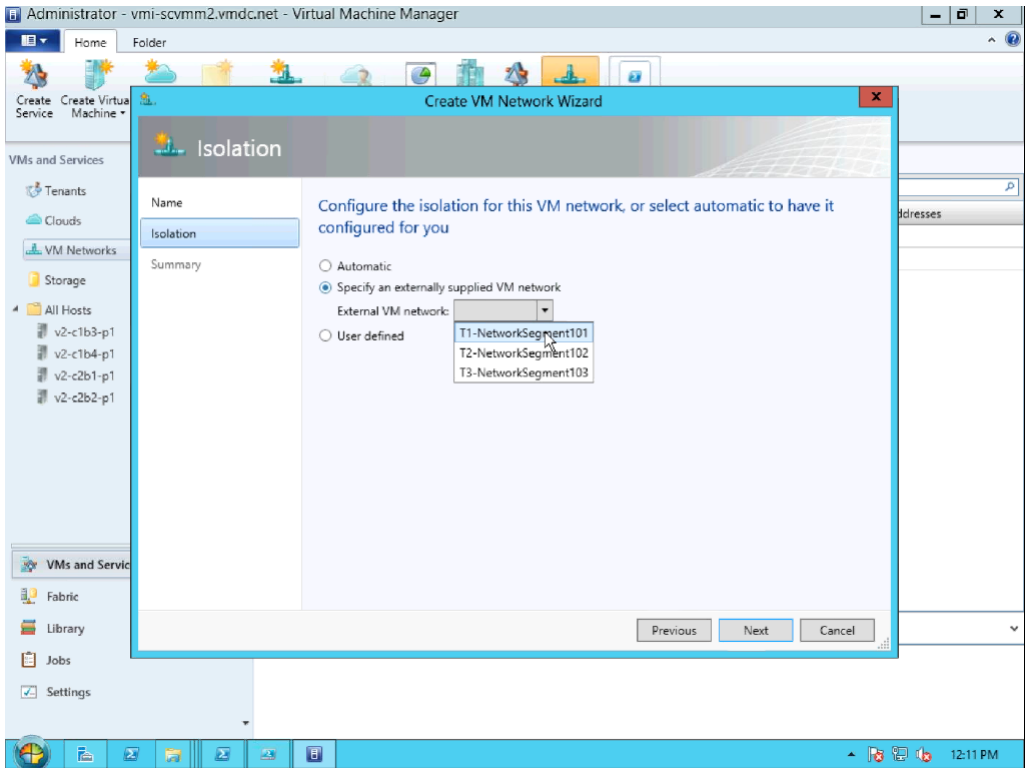
c. Create the VM network name and select the logical network.

Figure 3-42 Create VM Network Name



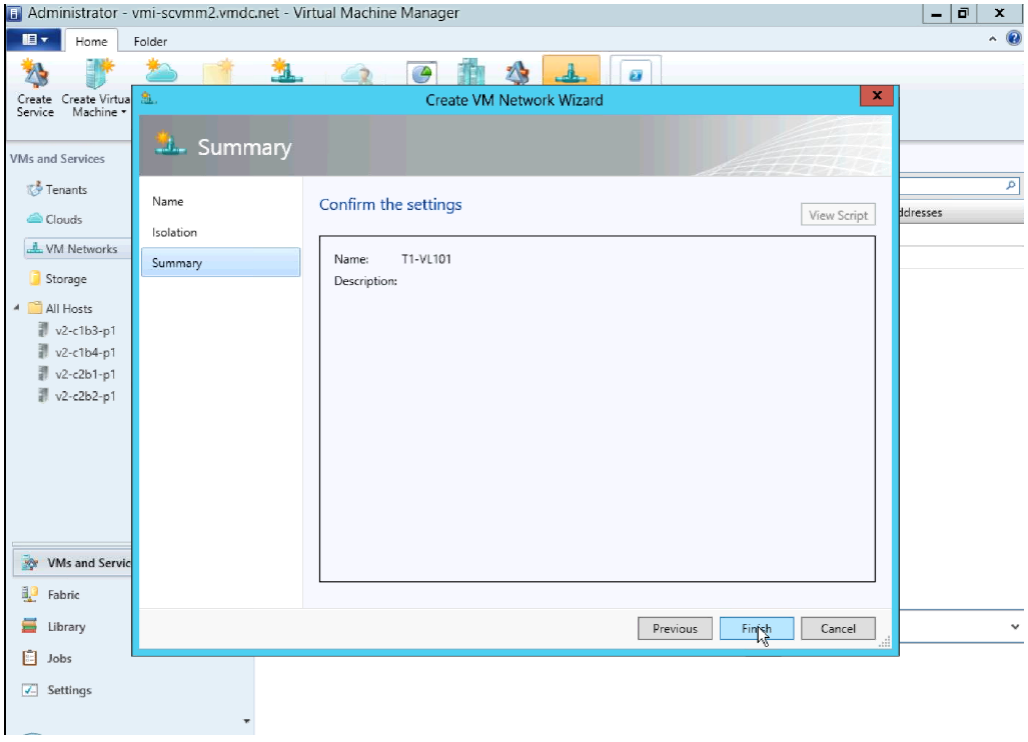
d. Select the network segment.

Figure 3-43 Select Network Segment



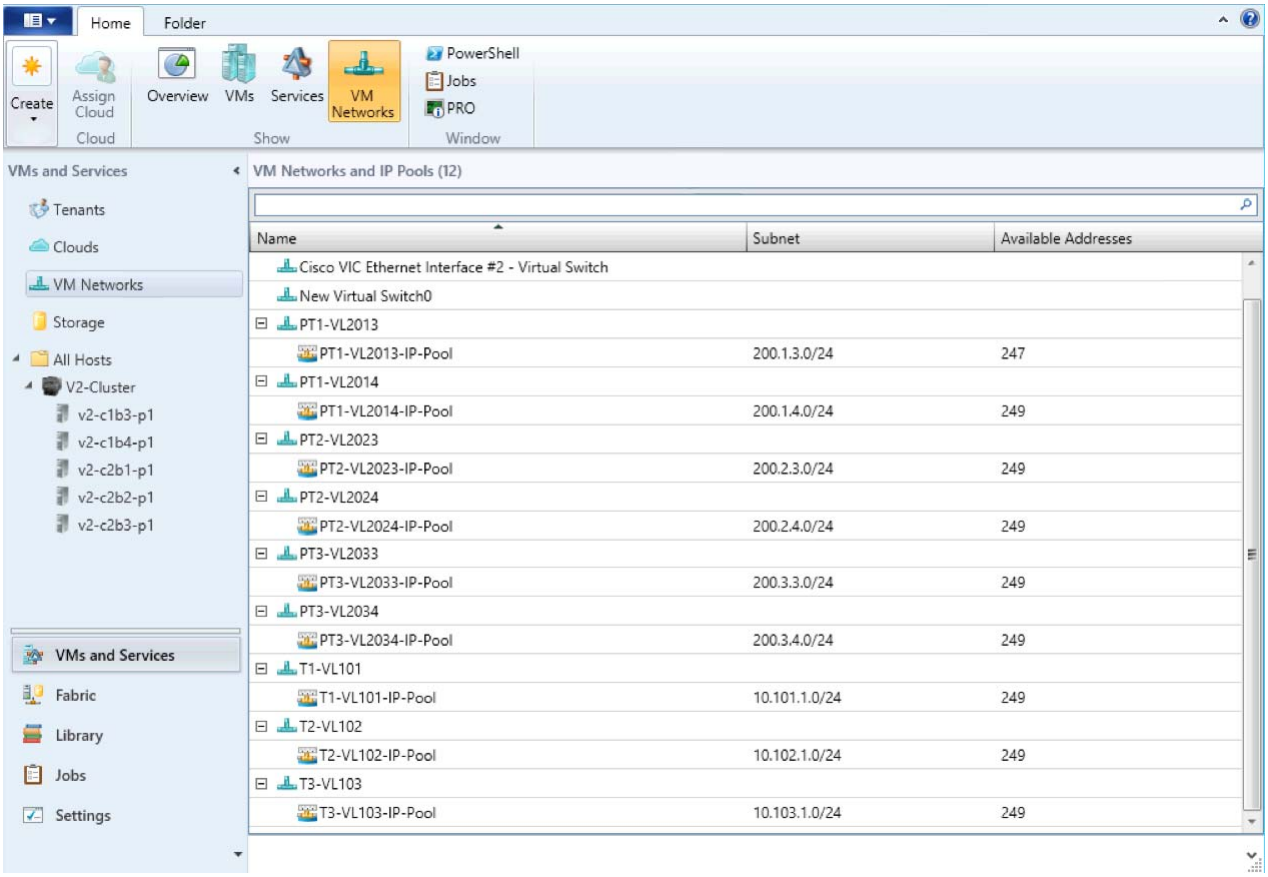
e. Confirm the VM network settings.

Figure 3-44 Confirm VM Network Settings



f. Follow the same steps to create the remaining VM Networks.

Figure 3-45 All VM Networks



g. Verify the network segment are now a “member-of” the correct VM Networks. This line of the configuration is automatically added to the CLI as noted Step 5Create Network Segments., page 3-4.

```
nsm network segment T1-NetworkSegment101
  member-of vmnetwork T1-NetworkSegment101
  member-of network segment pool T1
  switchport access vlan 101
  ip pool import template T1-VL101-IP-Pool
  publish network segment
  switchport mode access
```

At this point, the logical switch, including VSM and VEMs, is installed. VMs can now be added to the logical switch.

Deployment Guidelines

1. **Manually refresh the VSEM**. Hyper-V performs a periodic refresh every 30 minutes; changes in the Nexus 1000V are not automatically updated in Hyper-V. Manually refresh the VSEM to force updates to show up in SCVMM.

2. **Manually remove NetSwitchTeam.** If a host is deleted from SCVMM, NetSwitchTeam is not removed from the host.

   If hosts are removed and added again, the hosts is not added to the logical switch because NetSwitchTeam still exists on the hosts.

   This error is seen in the Jobs section:

   Error (25238)

   Creating the adapter team failed with error An internal error has occurred trying to contact the v2-c1b4-p1.vmdc.net server.

   WinRM: URL: [http://v2-c1b4-p1.vmdc.net:5985], Verb: [GET], Resource: [http://schemas.microsoft.com/wbem/wsman/1/wmi/root/scvmm/ErrorInfo?ID=1001]

   Check that WS-Management service is installed and running on server v2-c1b4-p1.vmdc.net. For more information use the command "winrm helpmsg hresult". If v2-c1b4-p1.vmdc.net is a host/library/update server or a PXE server role then ensure that VMM agent is installed and running. Recommended Action

   ensure the team is functioning correctly and retry the operation

   To clear this condition, open Windows PowerShell and do the following:

```
PS C:\Users\Administrator.VMDC> Get-NetSwitchTeam *
Name    : V2-HyperV-VSM-P12b352411-1eff-4e95-bc84-9f0fb5a339a4
Members : {Ethernet 5, Ethernet 4}

PS C:\Users\Administrator.VMDC> Get-NetSwitchTeam | Remove-NetSwitchTeam
```

   After the obsolete NetSwitchTeam is removed, the host can be added to the Logical switch.

3. **Verify that hosts ports show up in VSM**. In UCSM, each host had two MGMT and two DATA vNICs. The DATA vNICs were used for NetSwitchTeam. On one or two occasions, when a host was added to the Nexus 1000V logical switch, only one interface showed up in the VSM for that VEM, even though both interfaces were selected. The procedure to add the host to the Nexus 1000V had to be repeated, and the interface that did not show up had to be added to the newly created Nexus 1000V connection.

   This can be verified by logging into the VSM and looking at the output **from show interface brief**. Look for the VEM and the ports. A **show port-channel summary** should shows those ports added to the port-channel.

4. **Close and reopen SCVMM**. On occasion, odd behavior was seen, such as hosts not responding to messages. Connecting to hosts using Remote Desktop Protocol (RDP) showed that the hosts were in the correct state. Closing and reopening the SCVMM app cleared this state. This is most likely a winrm issue that needs further investigation when it happens again.

5. **Create a Gold Template for SCVMM**. After three to four weeks, SCVMM became unstable. A new SCVMM was created, and a Gold Template was generated from that VM, in case the instability recurs.

6. Refer to Cisco Nexus 1000V for Microsoft Hyper-V Installation Guide, Release 5.2(1)SM1(5.1) for information about creating the Nexus 1000V logical switch in Hyper-V SCVMM.

Adding VMs to Nexus V Switch for Hyper-V Logical Switch

This section shows the process for adding Virtual Machines to the Nexus 1000V Switch for Microsoft Hyper-V Logical switch.

Step 1 Go to the **VM Properties** page.

Right-click the VM and select **Properties**.

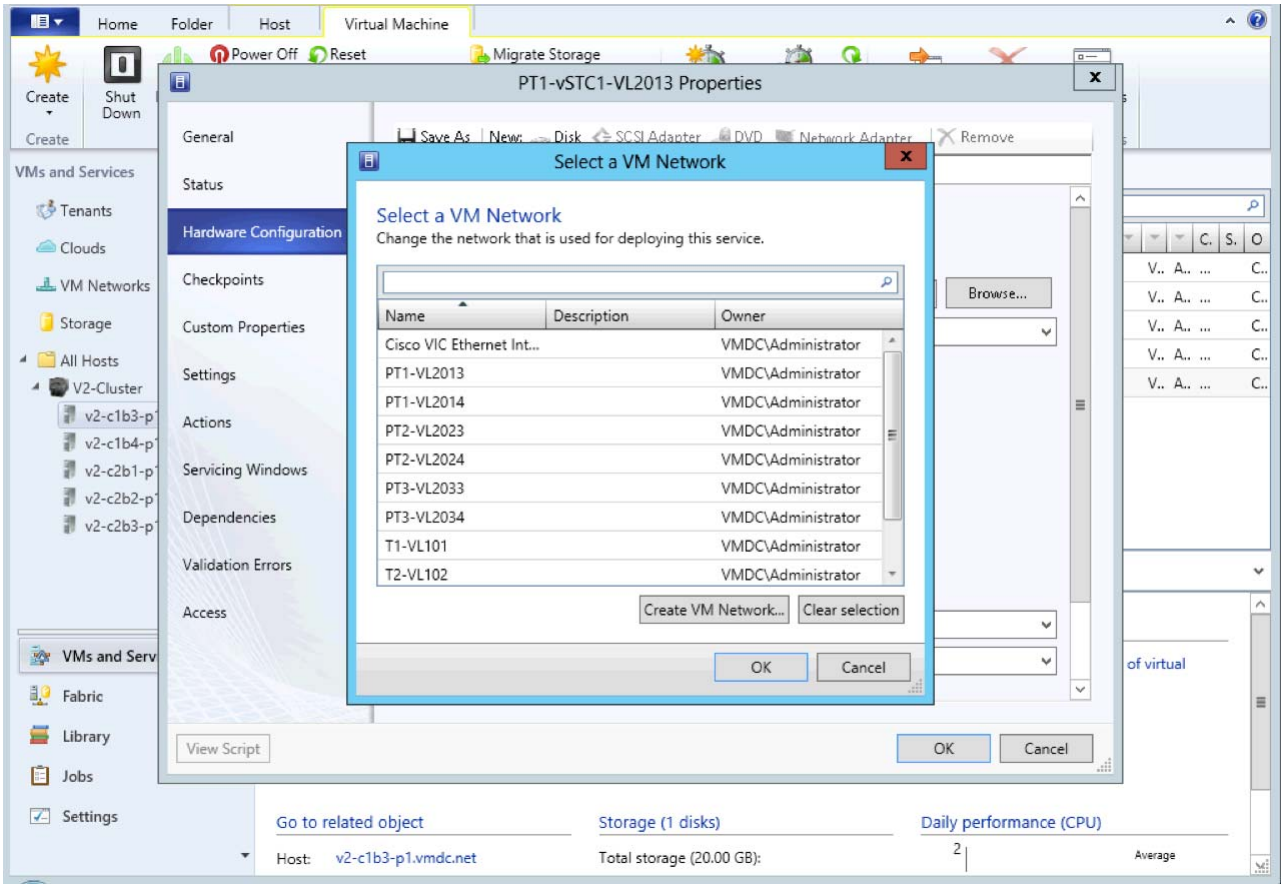
Step 2 Select **Hardware Configuration** and select the adapter to add to the logical switch.

There are two adapters in the test VMs. One connects to the Microsoft external switch for Management and the other connects to the Nexus 1000V.

Step 3 Select the VM network.

On the network adapter properties page, click **Browse** to see a list of available VM networks.

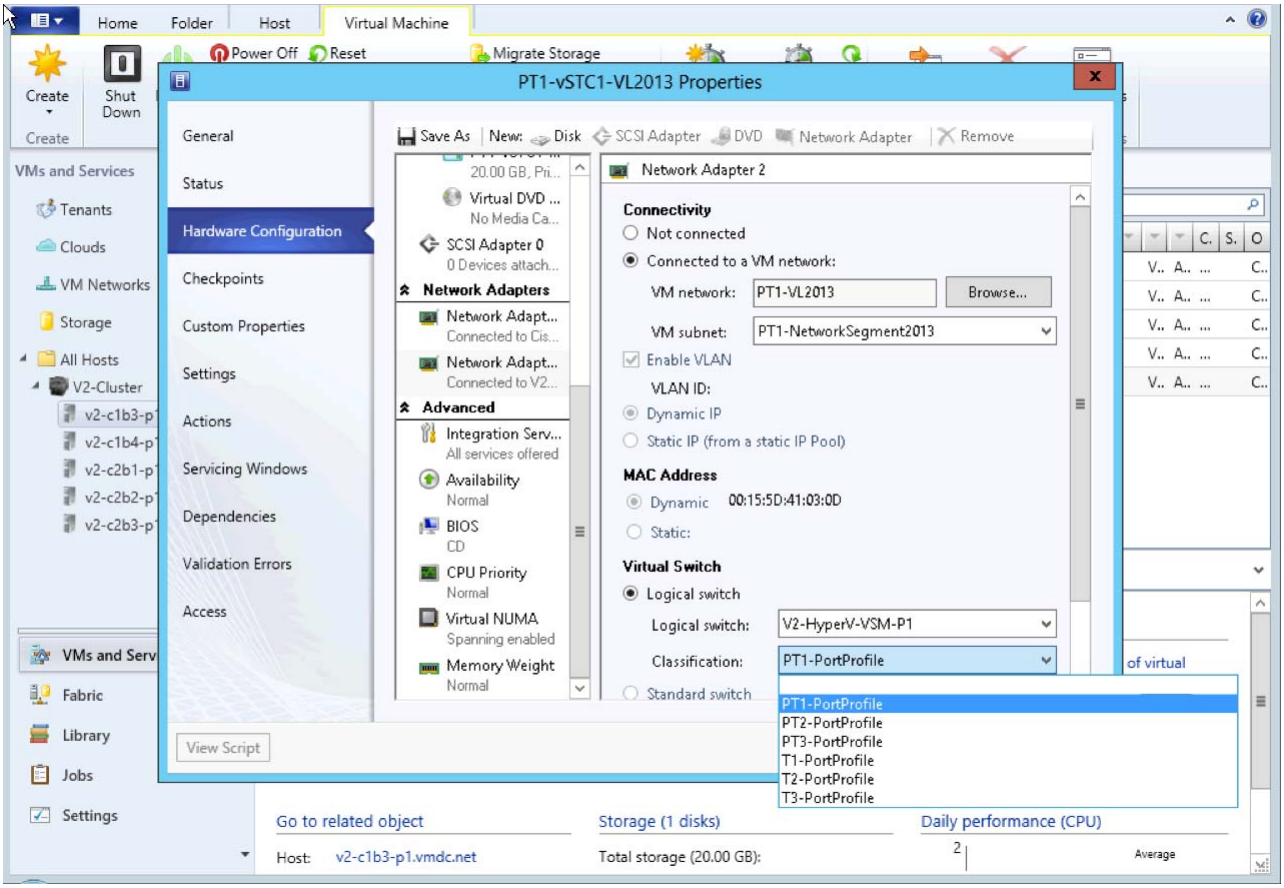
Figure 3-46 Select a VM Network



Step 4 Select the classification.

After selecting the VM network, click the Classification drop-down and select the classification profile.

Figure 3-47 Select Classification



Step 5 After selecting the classification, click **OK**.

Step 6 Verify the Virtual Machine has been deployed by issuing a “show interface virtual” from the CLI of the VSM:

```
V2-HyperV-VSM-P1# show interface virtual

--------------------------------------------------------------------------------
Port        Adapter        Owner                     Mod Host
--------------------------------------------------------------------------------
Veth1       Net Adapter    PT1-vSTC1-VL2013          3   V2-C1B3-P1
Veth2       Net Adapter    PT1-vSTC1-VL2014          3   V2-C1B3-P1
Veth3       Net Adapter    PT3-vSTC1-VL2033          3   V2-C1B3-P1
Veth4       Net Adapter    T1-vSTC1-VL101            3   V2-C1B3-P1
Veth5       Net Adapter    PT2-vSTC1-VL2023          4   V2-C1B4-P1
Veth6       Net Adapter    PT2-vSTC1-VL2024          4   V2-C1B4-P1
Veth7       Net Adapter    PT3-vSTC1-VL2034          4   V2-C1B4-P1
Veth8       Net Adapter    T2-vSTC1-VL102            4   V2-C1B4-P1
Veth9       Net Adapter    PT1-vSTC2-VL2013          5   V2-C2B1-P1
Veth10      Net Adapter    PT1-vSTC2-VL2014          5   V2-C2B1-P1
Veth11      Net Adapter    PT3-vSTC2-VL2033          5   V2-C2B1-P1
Veth12      Net Adapter    T3-vSTC1-VL103            5   V2-C2B1-P1
Veth13      Net Adapter    PT2-vSTC2-VL2023          6   V2-C2B2-P1
Veth14      Net Adapter    PT2-vSTC2-VL2024          6   V2-C2B2-P1
Veth15      Net Adapter    PT3-vSTC2-VL2034          6   V2-C2B2-P1
Veth16     Net Adapter   LM-Windows Server 2012 -01          4   V2-C1B4-P1

Veth17      Net Adapter    LM-Win2008-02             4   V2-C1B4-P1
```

Deployment Guidelines

1. **Select the correct interfaces when adding network adapters**. In UCSM, each host has two MGMT and two DATA vNICs. From the Windows OS perspective, four VIC interfaces are presented. Ensure that the correct interfaces are selected when adding the hosts to virtual switches. Check the MAC addresses.
2. Refer to **Connecting VMs to Logical Switch** in Cisco Nexus 1000v for Microsoft Hyper-V Installation Guide, Release 5.2(1)SM1(5.1) for more information.

CHAPTER 4

SCOM 2012 with UCS Management Pack

Microsoft System Center Operations Manager (SCOM) 2012 is a key component of Microsoft Private Cloud, and provides basic orchestration and monitoring for Private Cloud components. Cisco provides a plug-in for SCOM that enables users to monitor UCS. In order to minimize downtime, users can create e-mail alerts that report Private Cloud failures.

Installation and Configuration

Like SCVMM, SCOM a part of the Microsoft Private Cloud Suite. Users can install SCOM on the same server as the SCVMM, or on a standalone SCOM server. This decision depends upon resource restrictions and the preference of the System Administrator.

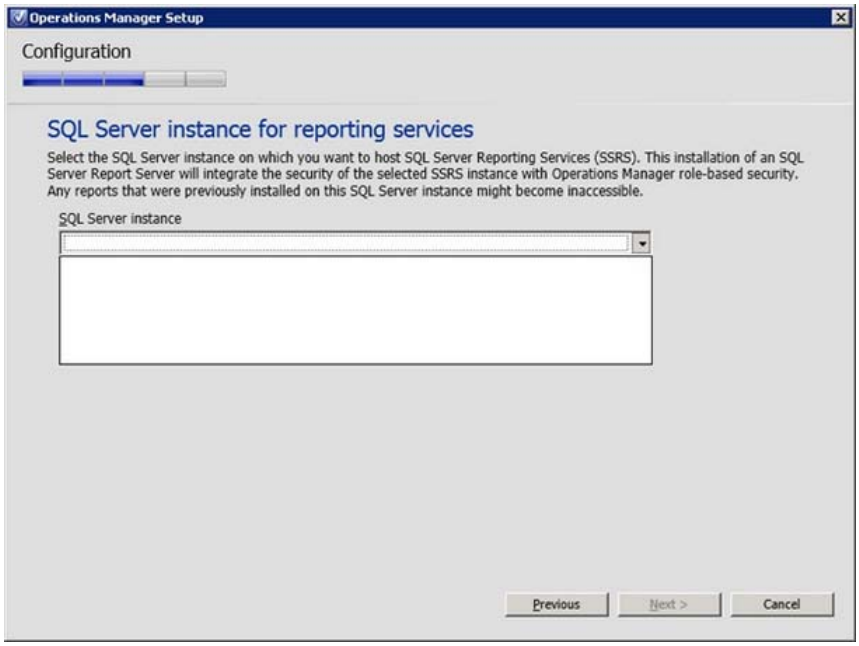
Before installation, ensure that the Windows Server 2012 server that SCOM will reside on can communicate with the SQL Server. No other adjustment to SQL is necessary. During SCOM installation, SQL automatically creates the necessary database and files.

Refer to the Microsoft System Center site for more installation details.

Deployment Guidelines

Since SQL 2012 resides on a standalone server separate from SCOM, the installation program might not be able to detect the SQL Server instance when attempted to install SQL Server Reporting Services (SSRS).

Figure 4-1 SQL Server Instance



This is normal, because SCOM expects a local installation of SQL Server Express. However, because the full version of SQL Server 2012 already exists in the ecosphere with backup and redundancy, the local installation of SQL Server Express was unnecessary. To work around this issue, perform the following step:

Ensure that both SQL Server and SCOM Server are in the same domain.

1. Install SCOM without the reporting server.
2. Install reporting services directly onto the SQL Server.
3. On the SCOM Server, open and close the Operation Management Console and reporting service should now be available.

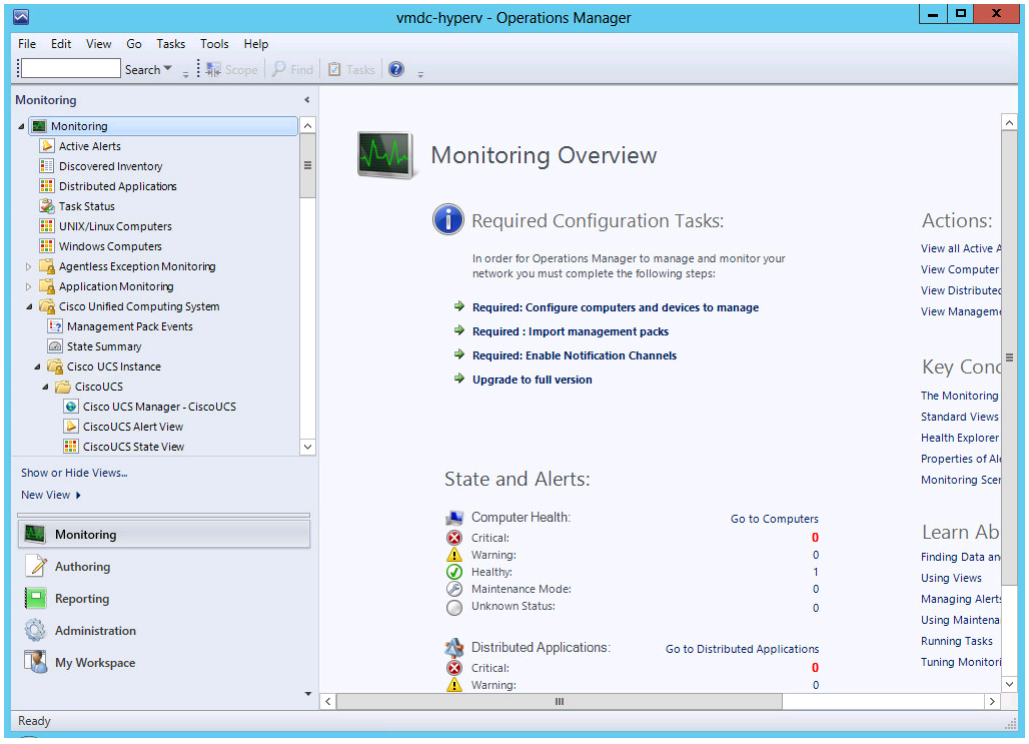
Cisco UCS Management Pack for SCOM

After the SCOM installation finishes, users can install a Cisco plug-in, UCS Management Pack, which is downloaded in the form of a Windows Installer (*.msi) file. This plug-in enables users to monitor various UCS components.

Before beginning the installation, download the UCS Management Pack.

The UCS Management Pack file, Cisco.UCS.MP.xxxx.vx.xx-x64.msi, should be saved on the desktop of the SCOM server. When the download finishes, double-click the file to install the program. When the installation finishes, a “Cisco Unified Computing System” folder should appear in SCOM.

Figure 4-2 Cisco Folder SCOM



For detailed information about installing and deploying UCS Management Pack, refer to the Quick Start Guide.

Monitors and Alerts

In SCOM, users can view Private Cloud status and configuration information. Users can view the Cisco UCS folder for UCS status and configuration information. In order to minimize downtime, users can create e-mail alerts that report UCS failures.

Figure 4-3 SCOM UCS Diagram

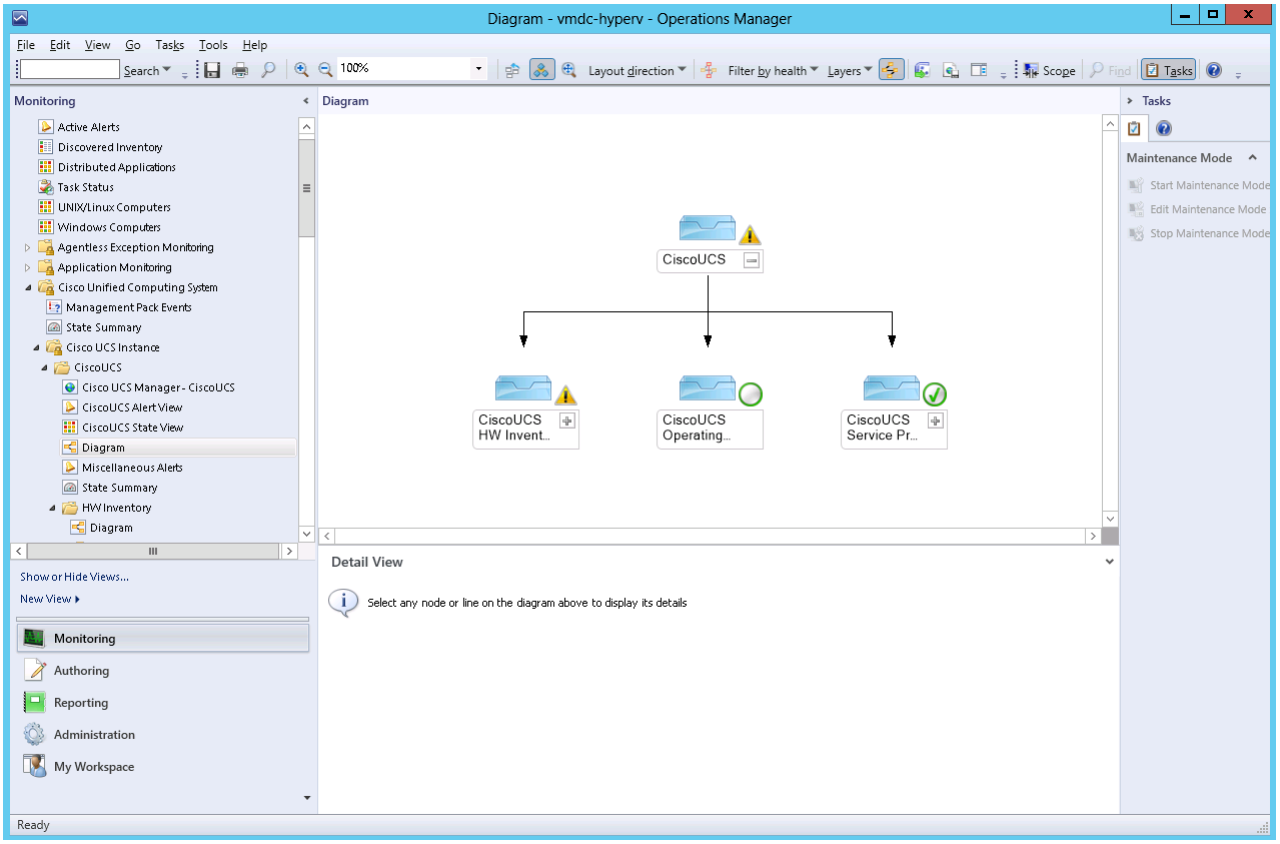
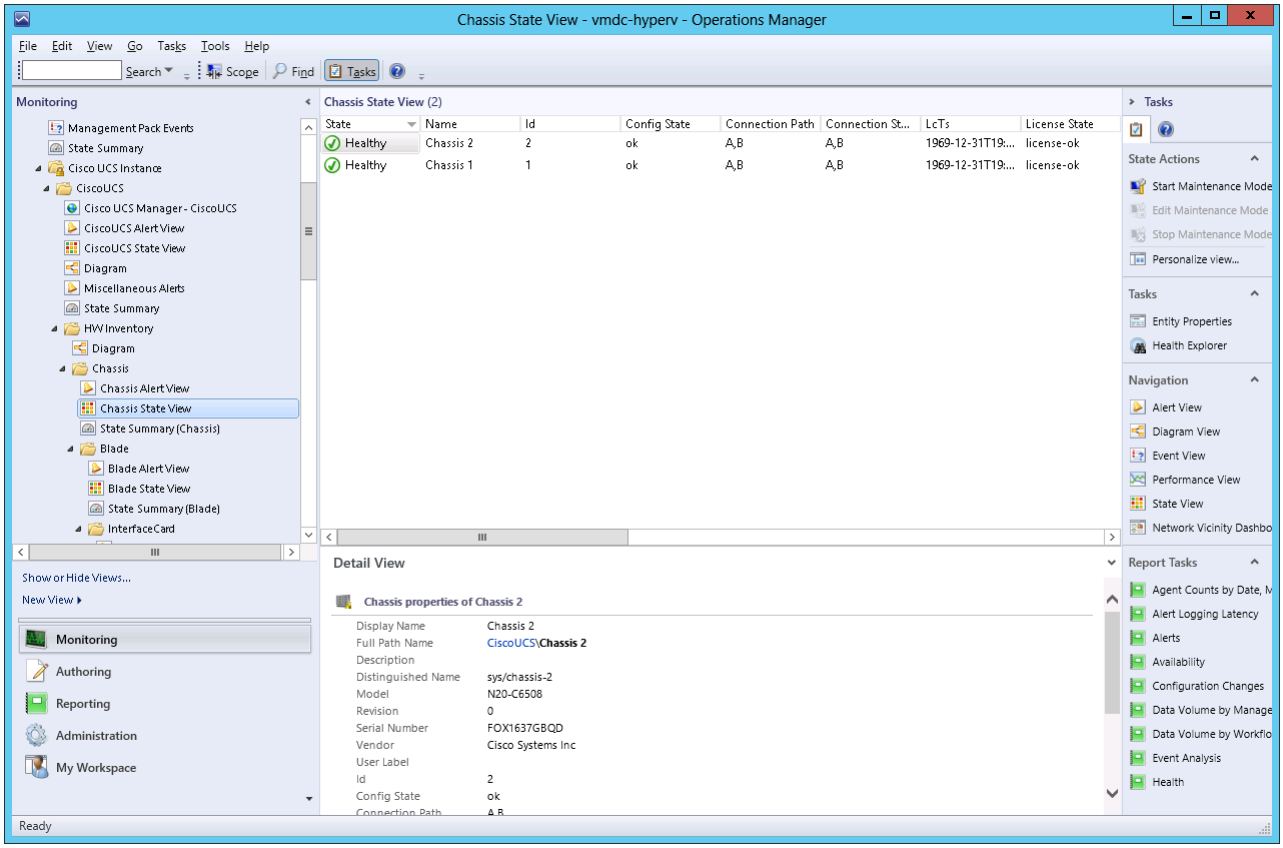


Figure 4-4 Chassis State View



Summary

Cisco Unified Computing System is a versatile computing platform capable of effectively supporting Microsoft Hyper-V and CloudOS. With the addition of Cisco Nexus 1000v, the virtual network becomes scalable and easy to manage. Utilizing the design and methodology of the Virtual Multiservice Data Center (VMDC), customers can build a highly secure, scalable, and self-serviceable private cloud to satisfy their infrastructure needs.